Algèbre II
Anneaux, modules, théorie de Galois

Jean-François Dat

2017-2018

Résumé

Ce cours introduit les techniques algébriques fondamentales utilisées en théorie des nombres et en géométrie algébrique. Une grande partie concernera la théorie générale des anneaux (commutatifs) et de leurs modules, et une autre partie la théorie des extensions de corps.

Sommaire

1 Algèbre commutative

1.1 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.

1.1.1 *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 de Gauss (ou 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].

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 :

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

Surtout, le résultat d'Euclide permet de résoudre certaines équations "diophantiennes", c'est-à-dire des équations polynomiales 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 peut montrer 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. 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

1.1.2 *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 :

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

1.1.3 *Eléments irréductibles, anneaux factoriels.*

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 de Gauss* 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 $u \in A^\times$.*

Nous reverrons plus en détail cette notion, mais on peut remarquer que dans un anneau factoriel, on a une 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.*

Exemple. – 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 $\mathbb{Z}[i]^\times = \{z \in \mathbb{Z}[i], z\bar{z} = 1\} = \{\pm 1, \pm i\}$. 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 [2].

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 $(x, y) = (0, 1)$.

Exercice. – L'anneau $\mathbb{Z}[\sqrt{-2}]$ et l'équation $x^2 + 2 = y^3$. Adapter les arguments précédents pour montrer que $\mathbb{Z}[\sqrt{-2}]$ est euclidien, puis que l'ensemble des solutions entières de l'équation $x^2 + 2 = y^3$ est $\{(5, 3), (-5, 3)\}$.

1.1.4 *Des anneaux d'entiers algébriques non factoriels.*

Exemple. – L'anneau $\mathbb{Z}[\sqrt{-3}]$ et l'équation $x^2 + 3 = y^3$. Essayons la même stratégie que précédemment. 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

2. Montrer que c'est encore équivalent au fait que -1 n'est pas un carré modulo p

anneau n'est pas factoriel [3]. 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 [4]. 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 $x \neq 0$ modulo 3. 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 $x \neq 0$ modulo 3. 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

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

3. 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 $\{z, |z| < 1\}$.

4. 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.

1.1.5 *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. Il est utile de se rappeler que pour deux éléments $a, b \in A$, on a $a|b \Leftrightarrow (a) \supset (b)$, ainsi que $(a) = A \Leftrightarrow a \in A^\times$.

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 de Gauss, 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.*

Voici une manière un peu plus précise de formuler ce résultat. Pour un idéal non nul I et un idéal premier non nul $\mathfrak{p}$, posons $v_\mathfrak{p}(I) := \mathrm{Max}\{m \in \mathbb{N}, \mathfrak{p}^m \supset I\}$, que l'on appelle encore "valuation $\mathfrak{p}$-adique" de I. Alors Dedekind prouve que $v_\mathfrak{p}(I)$ est bien défini, non nul pour un nombre fini de $\mathfrak{p}$ lorsqu'on fixe I, et qu'on a l'égalité d'idéaux $I = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(I)}$.

Par exemple on a les égalités d'idéaux suivantes :

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

Exercice. – Prouver les égalités ci-dessus et montrer 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 non principaux.

On remarque 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.

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 si (x, y) est une solution, alors $x + \sqrt{-5}$ 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 contenir $\sqrt{-5}$, auquel cas $\mathfrak{p} = (\sqrt{-5})$ (vérifier que ce dernier est bien premier). Mais si $\sqrt{-5}$ divisait $x + \sqrt{-5}$, alors 5 diviserait x, donc aussi y et on obtiendrait l'égalité $5 \equiv 0[25]$ qui est absurde. De plus, si $(2, 1+\sqrt{-5})$ contenait $(x+\sqrt{-5})$ alors 2 diviserait y, donc x serait 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.

1.1.6 *Groupe des classes d'un anneau d'entiers.* 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 (toujours supposé intégralement clos). 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 $\mathfrak{p}\mathfrak{q} = (a)$ 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 avancé ou M2 introductif.

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 $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}]) = \mathbb{Z}/2\mathbb{Z}$ (voir ci-dessous).

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.

Remarque culturelle. (sur la "géométrie des nombres") – Voici les ingrédients pour prouver que le groupe $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}])$ est d'ordre 2. Soit J un idéal non nul de $\mathbb{Z}[\sqrt{-5}]$. C'est un sous-groupe abélien de rang 2 de $\mathbb{Z}[\sqrt{-5}]$ et on peut donc définir son indice $i(J) := |\mathbb{Z}[\sqrt{-5}]/J| \in \mathbb{N}$. On peut aussi considérer J comme un réseau de $\mathbb{C}$, *i.e.* un sous-groupe abélien de type fini et $\mathbb{R}$-générateur. On peut alors définir son "covolume" $\mathrm{Covol}(J)$ comme le volume d'un parallélogramme fondamental de ce réseau. On a alors (exercice) $\mathrm{Covol}(J) = i(J)\mathrm{Covol}(\mathbb{Z}[\sqrt{-5}]) = i(J)\sqrt{5}$. On peut montrer (exercice) qu'une boule fermée centrée en 0 de rayon r contient un élément de J dès lors que son volume πr^2 dépasse $4\mathrm{Covol}(J)$. On peut donc trouver un élément $\alpha \in J$ tel que $|\alpha|^2 \leqslant \frac{4}{\pi}\sqrt{5} \cdot i(J)$. Noter que $|\alpha|^2 = i((\alpha))$. Ecrivons alors $(\alpha) = IJ$, grâce au théorème de factorisation de Dedekind. Il vient $i(I) = i(\alpha)i(J)^{-1} \leqslant \frac{4}{\pi}\sqrt{5} < 3$, et donc $i(I) = 1$ ou 2. Si $i(I) = 1$ on a $I = A$. Si $i(I) = 2$ alors I est premier (car l'indice est multiplicatif) et contient (2), donc $I = (2, 1 + \sqrt{-5})$. Ainsi J est équivalent, dans $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}])$, à A ou à $(2, 1 + \sqrt{-5})$, et on a donc $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}]) = \mathbb{Z}/2\mathbb{Z}$.

Remarque culturelle. (sur les "courbes elliptiques") – Les équations $x^2 + N = y^3$ que nous avons étudiées ici définissent chacune une "courbe elliptique", dont nous avons étudié les points entiers rationnels. L'ensemble des solutions complexes d'une telle équation est naturellement muni d'une structure de groupe abélien (il faut rajouter un point à l'infini) et l'ensemble des solutions rationnelles en est un sous-groupe. Un théorème célèbre de Mordell affirme que ce sous-groupe est de type fini. Dans les cas que nous avons regardés ci-dessus il était même fini (*i.e.* de rang nul). Mais pour $N = 25, 20$ ou -10 il est infini et de rang 1, pour $N = -63$ il est même de rang 2.

1.1.7 *Une pathologie.* Les exemples ci-dessus avaient pour but de montrer comment certains concepts de la théorie des anneaux (irréductibilité, factorialité, clôture intégrale, idéaux) sont nés parce qu'ils se sont révélés utiles pour résoudre des problèmes de théorie des nombres d'apparence plus élémentaire. D'où l'intérêt de développer une théorie systématique des anneaux commutatifs comme nous allons le faire dans ce cours. Cependant, loin des jolies propriétés des anneaux de nombres, nous allons aussi rencontrer beaucoup de pathologies. Voici par exemple un exemple d'anneau pourtant naturel qui ne possède *aucun* élément irréductible !

Exemple. – Soit $\overline{\mathbb{Z}} \subset \mathbb{C}$ l'ensemble de tous les entiers algébriques. C'est un sous-anneau de $\mathbb{C}$ (exercice : le prouver). Notons que ce n'est pas un corps : par exemple $1/n$ pour $n > 1$ entier n'est jamais entier algébrique (le vérifier). Soit $z \in \overline{\mathbb{Z}}$ non nul et non inversible, et soit $\sqrt{z}$ une racine carrée de z dans $\mathbb{C}$ (qui est algébriquement clos !). C'est encore un élément de $\overline{\mathbb{Z}}$, non nul et non inversible dans $\overline{\mathbb{Z}}$ (justifier). Mais alors l'égalité $z = \sqrt{z} \cdot \sqrt{z}$ montre que z n'est pas irréductible. Ainsi $\overline{\mathbb{Z}}$ ne possède aucun élément irréductible.

Nous montrerons plus tard que pour les anneaux *noethériens*, cette pathologie n'apparait pas ; tout élément non nul et non inversible y est produit d'irréductibles.

1.1.8 *Anneaux de la géométrie algébrique classique.* Une autre source de motivation pour la théorie des anneaux est la *géométrie algébrique.* 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 polynomiales (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 données "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 le sous-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. Une notion naturelle "naïve" est celle d'*application polynomiale*.

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* polynomiale *si elle est la restriction d'une application polynomiale $\tilde{\varphi} : \mathbb{C}^n \longrightarrow \mathbb{C}^{n'}$, 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 polynomiale* sur V est une application polynomiale $V \longrightarrow \mathbb{C}$ en le sens précédent. L'ensemble $\mathcal{O}(V \subset \mathbb{C}^n)$ des fonctions polynomiales sur V est manifestement une $\mathbb{C}$-algèbre (via l'addition et la multiplication point par point des fonctions). Notons-le abusivement $\mathcal{O}(V)$ pour simplifier. Si $\varphi : V \longrightarrow V'$ est une application polynomiale, il découle de ces définitions que la composition des fonctions $f' \mapsto \varphi \circ f$ induit un morphisme de $\mathbb{C}$-algèbres

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

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 $\mathcal{O}(V') \longrightarrow \mathcal{O}(V)$.*

Ce résultat suggère qu'étudier les ensembles algébriques et les applications polynomiales 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 polynomiales sur un ensemble algébrique. Par définition $\mathcal{O}(\mathbb{C}^n)$ est engendrée, en tant que $\mathbb{C}$-algèbre par les fonctions coordonnées $z_1, \cdots, z_n$. Toujours par définition, pour $V \subset \mathbb{C}^n$, l'application de restriction des fonctions

$$\mathcal{O}(\mathbb{C}^n) \longrightarrow \mathcal{O}(V), f \mapsto f_{|V}$$

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 polynomiales $\mathcal{O}(V)$. 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 polynomiales $f \in \mathcal{O}(V)$ 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 $\mathcal{O}(V)$.*

Remarque. – On ne peut pas retrouver la topologie usuelle de V, mais on peut retrouver la topologie de Zariski de V, dont les fermés sont justement les sous-ensembles algébriques (exercice : montrer que $E_{I_1} \cup E_{I_2} = E_{I_1 \cap I_2}$ et que $\bigcap_i E_{I_i} = E_{\sum_i I_i}$). On a en effet la version un peu plus forte du Nullstellensatz :

THÉORÈME. – *Les applications $I \mapsto E_I$ et $E \mapsto I_E$ définissent des bijections réciproques entre l'ensemble des sous-ensembles algébriques de V et celui des idéaux* radiciels *de $\mathcal{O}(V)$.*

Un idéal I d'un anneau (commutatif) A est dit *radiciel* si $\forall f \in A, f^k \in I \Rightarrow f \in I$.

On peut donc retrouver V muni de sa topologie de Zariski comme l'ensemble $\mathrm{Max}(\mathcal{O}(V))$ muni de la topologie (aussi appelée "de Zariski") dont les fermés sont les ensemble $M(I) = \{\mathfrak{m}, \mathfrak{m} \supset I\}$.

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 polynomiales est intégralement clos est une variété lisse.

1.1.9 *La géométrie algébrique moderne.* La dualité entre sous-ensembles algébriques de $\mathbb{C}^n$ et $\mathbb{C}$-algèbres réduites de type fini est le 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.

1.2 Généralités sur les anneaux commutatifs

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

1.2.1 *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.

1.2.2 *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.

1.2.3 *(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 $\varphi(aa') = \varphi(a)\varphi(a')$.

— $\varphi(1) = 1$.

Il découle de cette définition que l'image d'un morphisme d'anneau $A \longrightarrow A'$ est un sous-anneau de 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. □

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 $\varphi \circ \psi = \psi'$.*

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".

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). Ainsi, tout anneau est, de manière unique, une $\mathbb{Z}$-algèbre.

1.2.4 *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 $(1, 0) \cdot (0, 1) = (0, 0)$.

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

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

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

En revanche, l'application $\varphi : \ A \longrightarrow A \times A$, $a \mapsto (a, 0)$ est bien additive et multiplicative mais envoie 1 sur $(1, 0)$: ce n'est pas un morphisme d'anneaux.

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

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

est un isomorphisme d'anneaux de $\mathbb{Z}/nm\mathbb{Z}$ sur le produit de $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$.

1.2.5 *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 $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Exercice. (interprétation géométrique) – Soit X un espace topologique et $A = \mathcal{C}(X, \mathbb{C})$ la $\mathbb{C}$-algèbre de ses fonctions continues. Montrer que X est connexe si et seulement si les seuls idempotents de A sont 1 et 0.

Remarque. – Il est aussi vrai qu'un sous-ensemble algébrique V est connexe (pour sa topologie de Zariski définie plus loin, ou pour la topologie usuelle induite de $\mathbb{C}^n$) si et seulement si les seuls idempotents de son algèbre de fonctions $\mathcal{O}(V)$ sont 0 et 1. Néanmoins, la preuve de la réciproque requiert la conséquence suivante du Nullstellensatz : si I est un idéal propre de $\mathcal{O}(V)$, alors $V(I) \neq \emptyset$.

DÉFINITION. – *Deux idempotents* e_1, e_2 *sont dits* orthogonaux *si* $e_1e_2 = e_2e_1 = 0$. *Un idempotent est dit* primitif *s'il n'est pas somme de deux idempotents orthogonaux non nuls.*

On montrera plus tard en TD que les *composantes connexes* d'un sous-ensemble algébrique sont en bijection avec les *idempotents primitifs* de son algèbre $\mathcal{O}(V)$.

1.2.6 *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.

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.

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 polynomiale $X_1 : \mathbb{C}^2 \longrightarrow \mathbb{C}, (z_1, z_2) \mapsto z_1$ induit une fonction polynomiale 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.

Interprétation géométrique. Plus généralement, soit $V \subset \mathbb{C}^n$ un sous-ensemble algébrique. On dit que V est *irréductible* s'il n'est pas réunion de deux sous-ensembles algébriques stricts. Certains auteurs appellent *sous-variété algébrique* un sous-ensemble algébrique irréductible (d'autres appellent sous-variété tout sous-ensemble algébrique...).

PROPOSITION. – *V est irréductible si et seulement si $\mathcal{O}(V)$ est intègre.*

Démonstration. Supposons V irréductible et soient $f_1, f_2 \in \mathcal{O}(V)$ deux fonctions polynomiales telles que $f_1 f_2 = 0$. Alors V est réunion $V = V(f_1) \cup V(f_2)$ des deux sous-ensembles algébriques (*i.e.* fermés de Zariski) $V(f_i) = \{z \in V, f_i(z) = 0\}$, $i = 1, 2$. Donc, par irréductibilité, il existe i tel que $V(f_i) = V$. On a donc $f_i = 0$ et il s'ensuit que $\mathcal{O}(V)$ est intègre.

Réciproquement, supposons que V est union $V = V_1 \cup V_2$ de deux sous-ensembles algébriques stricts. Ainsi V_1 est de la forme $V(f_1, \cdots, f_r)$ avec $f_i \in \mathcal{O}(V)$. Choisissons alors $z_2 \in V_2 \setminus V_1$; par définition, il existe i tel que $f_i(z_2) \neq 0$. De même, on peut trouver un élément $z_1 \in V_1$ et une fonction polynomiale $g \in \mathcal{O}(V)$ qui s'annule sur V_2 et pas sur z_1. Alors la fonction produit gf_i est partout nulle, i.e. $gf_i = 0$ dans $\mathcal{O}(V)$, ce qui montre que $\mathcal{O}(V)$ n'est pas intègre. $\square$

1.2.7 *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.

Remarque. – La notion de nilpotence n'est pas une "pathologie qu'on préfère éviter" et trouve des applications intéressantes en géométrie algébrique à la Grothendieck. Pour en donner un aperçu, on peut remarquer que si $\mathfrak{m} = (X_1, \cdots, X_n)$ désigne l'idéal maximal de $A = \mathbb{C}[X_1, \cdots, X_n]$ en $(0, \cdots, 0)$, alors l'image d'un polynôme $f \in A$ dans le quotient[5] $A/\mathfrak{m} = \mathbb{C}$ est la "valeur en 0" tandis que celle dans le quotient $A/\mathfrak{m}^2 = (A/\mathfrak{m}) \oplus (\mathfrak{m}/\mathfrak{m}^2)$

5. cette remarque suppose de savoir ce qu'est un anneau quotient, notion qui sera vue ou revue un peu plus loin

donne aussi la différentielle en 0 si on identifie $\mathfrak{m}/\mathfrak{m}^2 \simeq \mathbb{C}\bar{X}_1 \oplus \cdots \oplus \mathbb{C}\bar{X}_n$ à l'espace cotangent (au sens usuel de la géométrie différentielle) via $\bar{X}_i \mapsto dx_i$. (À méditer ! !)

1.2.8 *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. Laissée au lecteur. □

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 $I = N\mathbb{Z}$.

1.2.9 *Idéal engendré par un sous-ensemble.* 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 $x = a_1e_1 + \cdots + a_re_r$ 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 en général cet idéal $(x_1, \cdots, x_n)$. On dit qu'un idéal 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*).

1.2.10 *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 $IJ \subset I \cap J$.

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 $\mathfrak{p}^2 = (2)$.

Application à la topologie de Zariski de $\mathbb{C}^n$. Nous montrerons plus tard que tout idéal I de $\mathbb{C}[X_1, \cdots, X_n]$ est de type fini. Il s'ensuit que les sous-ensembles algébriques de $\mathbb{C}^n$ sont exactement les sous-ensembles de la forme $V(I) = \{z \in \mathbb{C}^n, \forall f \in I, f(z) = 0\}$. Mais alors, on vérifie facilement que $V(IJ) = V(I) \cup V(J)$ et $V(\sum_{k\in E} I_k) = \bigcap_{k\in E} V(I_k)$. Puisqu'on a aussi $V(\{0\}) = \mathbb{C}^n$ et $V((1)) = \emptyset$, on en déduit que les $V(I)$ sont les fermés d'une topologie, dite topologie de Zariski, sur $\mathbb{C}^n$. Cette topologie est beaucoup plus grossière que la topologie usuelle, et en particulier n'est pas Hausdorff.

1.2.11 *Idéaux premiers et maximaux.* On dit d'un idéal I dans un anneau commutatif A qu'il est :

— *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 $\forall x \in A$, $(\exists k \in \mathbb{N}^*, x^k \in I) \Rightarrow x \in I$.

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 $\mathcal{O}(\mathbb{C}^n)$.

Topologie de Zariski "abstraite". On note généralement $\mathrm{Spec}(A)$ l'ensemble des idéaux premiers de A. Il est muni d'une topologie dont les fermés sont les

$$V(I) := \{\mathfrak{p} \in \mathrm{Spec}(A),\ \mathfrak{p} \supset I\}$$

pour I idéal de A. En effet, on a $V(A) = \emptyset$, $V(\{0\}) = \mathrm{Spec}(A)$, on vérifie sans peine que $V(\sum_{k\in E} I_k) = \bigcap_{k\in E} V(I_k)$ et on vérifie aussi que $V(IJ) = V(I) \cup V(J)$ en utilisant la propriété d'être premier. Cette topologie n'est pas Hausdorff.

L'ensemble $\mathrm{Max}(A)$ hérite de la topologie induite par celle de $\mathrm{Spec}(A)$, qui peut aussi se définir directement de manière analogue. On montre (exercice) que $\mathrm{Max}(A)$ est l'ensemble des points "fermés" de $\mathrm{Spec}(A)$ (i.e. dont le singleton associé est fermé). On peut faire le lien avec la topologie de Zariski "concrète" sur $\mathbb{C}^n$ de la manière suivante. A tout $z \in \mathbb{C}^n$ on associe un idéal $\mathfrak{m}_z = \{f \in \mathcal{O}(\mathbb{C}^n), f(z) = 0\}$. Cet idéal est maximal (exercice) et on a $I \subset \mathfrak{m}_z \Leftrightarrow (\forall f \in I, f(z) = 0)$. Ainsi l'application $\mathbb{C}^n \xrightarrow{\iota} \mathrm{Max}(\mathcal{O}(\mathbb{C}^n))$ ainsi obtenue est injective et continue. Le Nullstellensatz, que l'on démontrera plus tard, affirme qu'elle est bijective et il s'ensuit aisément que c'est un homéomorphisme.

Exercice. – Soit $\varphi : A \longrightarrow B$ un morphisme d'anneaux et I un idéal de B. Montrer que I premier $\Rightarrow \varphi^{-1}(I)$ premier. Montrer que l'application $\varphi^{-1} : \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ ainsi obtenue est continue pour les topologies de Zariski.

Trouver un exemple où I est maximal et $\varphi^{-1}(I)$ ne l'est pas. Ce défaut de fonctorialité de Max explique que l'on préfère souvent travailler avec Spec. Néanmoins, nous verrons que si A et B sont des algèbres de type fini sur un corps, alors l'image réciproque d'un idéal maximal est un idéal maximal. Nous verrons aussi (peut-être) que dans ce cas, $\mathrm{Max}(A)$ est dense dans $\mathrm{Spec}(A)$ et qu'il n'y a donc pas grande différence à travailler avec l'un ou l'autre.

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 qui affirme la chose suivante : *si dans un ensemble ordonné $(E, \leqslant)$, toute chaîne (= sous-ensemble totalement ordonné) 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 et qui est propre puisqu'il ne contient pas 1. 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. $\square$

1.2.12 *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

$$x \equiv y \pmod{I} \text{ si et seulement si } x - y \in I.$$

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 $\pi_I(x)$, $\overline{x}$, $x+I$, $x \pmod{I}$, 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 $x \equiv x' \pmod{I}$ et $y \equiv y' \pmod{I}$, on a $(x+y) \equiv (x'+y') \pmod{I}$ et $xy \equiv x'y' \pmod{I}$. 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 $\overline{1}$. $\square$

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). $\square$

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 $I' \mapsto \pi_I(I')$. Montrer que $\pi_I^{-1}(\sqrt{0}) = \sqrt{I}$. Montrer que cette bijection induit un homéomorphisme de $\mathrm{Spec}(A/I)$ sur le fermé $V(I)$ de $\mathrm{Spec}(A)$.

1.2.13 *Propriété universelle des quotients.* Lorsqu'on travaille avec des anneaux quotients, on utilise très rarement la définition en termes d'ensemble de classes d'équivalence. Il est beaucoup plus efficace d'utiliser la "propriété universelle" suivante.

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.*

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\pi_I"'] & A' . \\ A/I \arrow[ur, dashed, "\overline{\varphi}"'] & \end{tikzcd}$$

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 $\overline{x} = \overline{0} = 0$. $\square$

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"[6]. 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" $(A, I) - \mathrm{Alg}$ des A-algèbres (B, ψ) telles que $\psi(I) = 0$ avec pour morphismes les morphismes de A-algèbres. La proposition nous dit que cette paire possède la propriété suivante : *pour toute A-algèbre (A', φ) telle que $\varphi(I) = 0$, il existe un unique morphisme de A-algèbres $A/I \longrightarrow A'$.*[7] 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.[8]

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 polynomiales $\mathcal{O}(V)$, l'application de restriction des fonctions $\mathcal{O}(\mathbb{C}^n) \longrightarrow \mathcal{O}(V)$

6. Le mot "catégorie" a en fait un sens mathématique précis. Informellement, une catégorie $\mathcal{C}$ est formée d'une classe d'objets $\mathrm{Ob}(\mathcal{C})$ et d'une notion de morphismes entre ces objets, composables comme on s'y attend. Plus précisément, on se donne pour chaque paire d'objets A, B un ensemble $\mathcal{C}(A, B)$ de "morphismes" de A vers B, et pour chaque triplet A, B, C d'objets, une loi de composition *associative* $\mathcal{C}(A, B) \times \mathcal{C}(B, C) \longrightarrow \mathcal{C}(A, C)$ pour laquelle il existe dans chaque $\mathcal{C}(A, A)$ un élément neutre (à droite et à gauche) généralement noté id_A. Exemples : la catégorie des ensembles munis des applications, la catégorie des espaces topologiques munis des applications continues, la catégorie des groupes abéliens munis des morphismes de groupes, la catégorie des anneaux munis des morphismes d'anneaux, la catégorie des A-algèbres munies des morphismes de A-algèbres, etc. Dans une catégorie, un *isomorphisme* est un morphisme qui admet un inverse à droite et à gauche.

7. En d'autres termes, l'objet $(A/I, \pi_I)$ de $(A, I) - \mathrm{Alg}$ admet un unique morphisme vers tout autre objet de $(A, I) - \mathrm{Alg}$. On dit que c'est un *objet initial* de la catégorie $(A, I) - \mathrm{Alg}$. Autres exemples : $\mathbb{Z}$ est un objet initial dans la catégorie des anneaux. L'espace vectoriel nul est un objet initial de la catégorie des espaces vectoriels sur $\mathbb{C}$. L'ensemble vide est un objet initial de la catégorie des ensembles.

8. Ce raisonnement très général montre que dans une catégorie, un objet initial est "unique à isomorphisme unique près", au sens où deux objets initiaux sont isomorphes d'une seule manière.

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 $\mathbb{C}[X_1, \cdots, X_n]$.

1.2.14 *Morphismes entre quotients.* Soit maintenant $J \supset I$ un idéal de A contenant I. La propriété 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 $\mathrm{Ker}(\overline{\pi}_J) = \pi_I(\pi_I^{-1}(\mathrm{Ker}(\overline{\pi}_J)) = \pi_I(J)$. $\square$

Exemple. – On retrouve le fait "bien connu" que pour $m|n$ l'application $a \mapsto a \pmod m$ se factorise par un morphisme $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ via l'application $a \mapsto a \pmod n$ 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

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

1.2.15 *Théorème des restes chinois.* Soient I, J deux idéaux de A. Le noyau du morphisme $A \longrightarrow A/I \times A/J$, $a \mapsto (a \pmod I, a \pmod J)$ est visiblement égal à $I \cap J$ donc, par la propriété universelle des quotients, ce morphisme se factorise via $\pi_{I\cap J}$ par un morphisme *injectif*

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

PROPOSITION. – *Le morphisme $(\overline{\pi}_I, \overline{\pi}_J)$ est surjectif (et donc bijectif) si et seulement si $I + J = A$. Dans ce cas, on a aussi $IJ = I \cap J$ et on obtient donc un isomorphisme*

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

Démonstration. 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 $(c \pmod I, c \pmod J) = (a \pmod I, b \pmod J)$.

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.

Enfin, il nous reste à vérifier que $IJ = I \cap J$. On a toujours l'inclusion $IJ \subset I \cap J$, donc montrons l'inclusion réciproque. Ecrivons $1 = i + j$ et soit $a \in I \cap J$. Alors $a = ai + aj$ et $ai, aj \in IJ$, donc $a \in IJ$. □

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 : $\mathbb{Z}/nm\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Exemple. – Si I et J sont deux idéaux maximaux distincts, la condition $I + J = A$ est vérifiée.

1.3 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.

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

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

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.

1.3.2 *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.

Remarque. – Les A-modules munis des morphismes de A-modules forment une catégorie que l'on note souvent $A - \mathrm{Mod}$. De même on a une catégorie $B - \mathrm{Mod}$ de B-modules. Nous venons d'associer à tout A-module M un B-module $\varphi^* M$ et à toute paire de A-modules M, N une application $\varphi^* : \mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_B(M, N)$ (qui est ici une inclusion) qui est évidemment compatible avec la composition des morphismes de chaque côté. Ceci est un exemple de *foncteur*[9] entre deux catégories.

9. Plus généralement, un foncteur $F : \mathcal{C} \longrightarrow \mathcal{C}'$ entre deux catégories est la donnée d'une "application" $\mathrm{Ob}(\mathcal{C}) \longrightarrow \mathrm{Ob}(\mathcal{C}')$ et d'applications $F : \mathcal{C}(A, B) \longrightarrow \mathcal{C}'(FA, FB)$ compatibles à la composition et aux éléments neutres.

1.3.3 *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.

1.3.4 *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 $m \pmod N$ 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*

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

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 $\operatorname{Ker}(\overline{\pi}_P) = \pi_N(\operatorname{Ker}(\pi_P)) = \pi_N(P) = P/N$, 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 $\operatorname{Ker}(\rho) = N \cap P$, 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. □

1.3.5 *Suites exactes, complexes.* Soit A un anneau. Considérons une suite

$$\cdots \xrightarrow{d_{i-2}} M_{i-1} \xrightarrow{d_{i-1}} M_i \xrightarrow{d_i} M_{i+1} \xrightarrow{d_{i+1}} \cdots$$

de morphismes de A-modules. On dit que cette suite est un *complexe* si on a $d_{i+1} \circ d_i = 0$ pour tout $i \in \mathbb{Z}$. On dit que cette suite (ou ce complexe) est *exacte* si on a $\mathrm{Ker}(d_{i+1}) = \mathrm{Im}(d_i)$ pour tout $i \in \mathbb{N}$. Par exemple, la suite

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} P \longrightarrow 0$$

est exacte si et seulement si ι est injective, π est surjective, et $\mathrm{Ker}\,\pi = \mathrm{Im}\,\iota$. Dans ce cas, ι identifie N à un *sous-module* de M, et π identifie P au quotient de M par ce sous-module. On parle alors de *suite exacte courte.*

Exercice. – Soit $\varphi : M \longrightarrow N$ un morphisme de A-modules. On pose $\mathrm{Coker}(\varphi) := N/\mathrm{Im}(\varphi)$ et on note $\pi_\varphi : N \longrightarrow \mathrm{Coker}(\varphi)$ la projection canonique. La paire $(\mathrm{Coker}(\varphi), \pi_\varphi)$ est appelée *conoyau* de φ.

i) Montrer que le conoyau est universel parmi les paires (P, ψ) constituées d'un A-module P muni d'un morphisme $\psi : N \longrightarrow P$ tel que $\psi \circ \varphi = 0$.

ii) Montrer que la suite suivante est exacte.

$$0 \longrightarrow \mathrm{Ker}(\varphi) \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\pi_\varphi} \mathrm{Coker}(\varphi) \longrightarrow 0$$

1.3.6 *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*

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

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

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

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). $\square$

Remarque. (Produits et coproduits dans les catégories) – Supposons donnée une famille $(X_i)_{i\in I}$ d'objets dans une catégorie $\mathcal{C}$. On appelle *produit* de cette famille une paire $(X, (\pi_i)_{i\in I})$ formée d'un objet de $\mathcal{C}$ et d'une famille de morphismes $\pi_i \in \mathcal{C}(X, X_i)$ telle que pour tout objet Y de $\mathcal{C}$, l'application

$$\mathcal{C}(Y, X) \longrightarrow \prod_{i\in I} \mathcal{C}(Y, X_i),\ \varphi \mapsto (\pi_i \circ \varphi)_{i\in I}$$

est bijective. Si une telle paire existe, elle est unique à isomorphisme unique près : en effet, c'est un objet initial de la catégorie dont les objets sont les paires $(Y, (\psi_i)_{i\in I})$ avec pour morphismes les morphismes $\psi \in \mathcal{C}(Y, Y')$ tels que $\psi_i = \psi \circ \psi_i'$. On note en général l'objet produit $\prod_{i \in I} X_i$. Dans les exemples "classiques" (modules, anneaux, espaces topologiques), les produits existent et l'ensemble sous-jacent est le produit cartésien des sous-ensembles sous-jacents (on dit pompeusement que "les produits commutent aux foncteurs d'oubli vers la catégorie des ensembles"...).

De manière "duale"[10], on appelle *coproduit* de la famille $(X_i)_{i \in I}$ une paire $(X, (\iota_i)_{i \in I})$ formée d'un objet de $\mathcal{C}$ et d'une famille de morphismes $\iota_i \in \mathcal{C}(X_i, X)$ telle que pour tout objet Y de $\mathcal{C}$, l'application

$$\mathcal{C}(X, Y) \longrightarrow \prod_{i \in I} \mathcal{C}(X_i, Y), \ \varphi \mapsto (\varphi \circ \iota_i)_{i \in I}$$

est bijective. À défaut de meilleure notation, on note généralement le coproduit $\coprod_{i \in I} X_i$. C'est d'ailleurs la notation usuelle pour la *réunion disjointe* d'ensembles, qui n'est autre qu'un coproduit dans la catégorie des ensembles. On remarquera que les coproduits existent dans les catégories de modules, mais "ne commutent pas au foncteur d'oubli vers la catégorie des ensembles" : l'ensemble sous-jacent d'une somme directe n'est pas la réunion disjointe des ensembles sous-jacents.

Remarque. (Foncteurs représentables) – Un foncteur $F : \mathcal{C} \longrightarrow \mathcal{E}ns$ est dit *représentable* s'il est "isomorphe" (on dit aussi "équivalent") à un foncteur de la forme $Y \mapsto \mathcal{C}(X, Y)$. Plus précisément, un *représentant* de F est un couple (X, α) avec X dans $\mathrm{Ob}(\mathcal{C})$ et $\alpha \in F(X)$ tel que pour tout objet Y dans $\mathrm{Ob}(\mathcal{C})$ l'application $\mathcal{C}(X, Y) \longrightarrow F(Y)$, $\varphi \mapsto F(\varphi)(\alpha)$ soit une bijection. Un représentant, s'il existe, est unique à isomorphisme unique près. Par exemple, un coproduit $(X, (\iota_i)_{i \in I}$ de la famille $(X_i)_{i \in I})$ représente le foncteur $Y \mapsto \prod_{i \in I} \mathcal{C}(X_i, Y)$.

1.3.7 *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

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

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

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

10. On remarquera qu'à toute catégorie $\mathcal{C}$ on peut associer sa catégorie "opposée" $\mathcal{C}^{\mathrm{opp}}$ dont les objets sont les mêmes et les flèches données par $\mathcal{C}^{\mathrm{opp}}(A, B) := \mathcal{C}(B, A)$. Le passage à la catégorie opposée échange formellement les notions de produits et coproduits.

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.

1.3.8 *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[11]

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

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 $\Psi(\sum_{i\in I} a_i e_i) = \sum_{i\in I} a_i m_i$. $\square$

11. Autrement dit, le couple $(A, (e_i)_{i\in I})$ représente le foncteur $M \mapsto M^I$.

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.*

Exemple. – Quelques modules non libres :
— Si I est un idéal propre et non nul de A, alors le A-module $M := A/I$ n'est pas libre. En fait, M ne possède aucune famille libre, puisque l'action de tout $i \in I \setminus \{0\}$ annule M.
— Soit $A = \mathbb{C}[X, Y]$ et $M = (X, Y)$ (idéal engendré par X et Y). Puisque $M \subset A$, l'exemple précédent nous dit que les seules familles libres de M sont les singletons $\{f(X, Y)\}$ où $f(X, Y)$ est un polynôme non nul de terme constant nul. Mais on voit aisément qu'un singleton n'est jamais générateur de M.

Les modules libres partagent quelques propriétés agréables des espaces vectoriels sur un corps. Par exemple, si M est libre de base $(e_i)_{i=1,\cdots,n}$ et N est libre de base $(f_j)_{i=1,\cdots,m}$, et φ un morphisme de A-module $N \longrightarrow M$, on peut écrire $\varphi(f_j) = \sum_{i=1}^n a_{ij} e_i$. On obtient ainsi une bijection (et même un isomorphisme de A-modules)

$$\mathrm{Hom}_A(N, M) \xrightarrow{\sim} \mathcal{M}_{n,m}(A)$$

avec les matrices $n \times m$ à coefficients dans A. Lorsque $N = M$, il s'agit même d'un isomorphisme d'anneaux.

Il y a cependant des différences notables. En voici quelques exemples :
— Un endomorphisme injectif d'un module libre de rang fini n'est pas nécessairement surjectif. Exemple : $A = \mathbb{Z} = M$ et φ l'endomorphisme $m \mapsto 2m$ de M.
— On ne peut pas nécessairement extraire une base d'une famille génératrice. Exemple $A = \mathbb{Z} = M$ et famille $\{2, 3\}$.

— Une famille libre ne peut pas nécessairement être complétée en une base. Même exemple avec comme famille libre $\{2\}$.
— Un sous-module d'un module libre de rang n n'est pas nécessairement libre, ni engendré par une famille de cardinal inférieur à n. Exemple $A = \mathbb{C}[X, Y]$, $n = 1$ et $M = AX + AY$.

Une bonne nouvelle tout de même :

Proposition. – *Soit M un A-module libre de type fini. Alors toutes ses bases sont finies et ont même cardinal. On l'appelle le* rang de M. *De plus, le cardinal d'une famille libre (resp. génératrice) est inférieur (resp. supérieur) au rang de M.*

Démonstration. Supposons d'abord que M admette une base finie $E = (e_1, \cdots, e_n)$ et soit $F = (f_1, \cdots, f_m)$ une famille d'éléments de M. Nous allons montrer que si F est génératrice alors $m \geqslant n$. Par symétrie il en découlera que si F est une base, alors $n = m$.

Pour montrer $m \geqslant n$, nous allons nous ramener au cas connu où l'anneau de base est un corps. Ecrivons $f_j = \sum_{i,j} a_{ij} e_i$. La matrice $P = (a_{ij})_{i,j} \in \mathcal{M}_{n \times m}(A)$ est la matrice d'un morphisme $A^m \xrightarrow{\psi} A^n$, et F est génératrice si et seulement si ψ est surjectif. Choisissons maintenant un idéal maximal $\mathfrak{m}$ de A et notons $\pi : A \longrightarrow A/\mathfrak{m}$ le morphisme de passage au quotient. La matrice $(\pi(a_{ij}))_{i,j} \in \mathcal{M}_{n \times m}(A/\mathfrak{m})$ est la matrice d'un morphisme $\overline{\psi}$: $(A/\mathfrak{m})^m \longrightarrow (A/\mathfrak{m})^n$ qui s'inscrit dans un diagramme commutatif

$$\begin{tikzcd} A^m \arrow[r, "\psi"] \arrow[d, "\pi^m"'] & A^n \arrow[d, "\pi^n"] \\ (A/\mathfrak{m})^m \arrow[r, "\overline{\psi}"] & (A/\mathfrak{m})^n \end{tikzcd}$$

(rappelons que la commutativité du diagramme signifie que $\pi^n \circ \psi = \overline{\psi} \circ \pi^m$). Puisque π^n est surjective, on voit que (ψ surjective) $\Rightarrow$ ($\pi^n \circ \psi$ surjective) $\Leftrightarrow$ ($\overline{\psi} \circ \pi^m$ surjective) $\Rightarrow$ ($\overline{\psi}$ surjective. Mais puisque $A/\mathfrak{m}$ est un corps, on sait que $\overline{\psi}$ surjective $\Rightarrow m \geqslant n$.

Montrons maintenant que si $m > n$, la famille F est liée. Soit r le plus grand entier tel que P admette un mineur de taille $r \times r$ non nul. Si $r = 0$, tous les f_i sont nuls et F est évidemment liée, donc on supposera $r \geqslant 1$. On a aussi $r \leqslant n < m$. Quitte à renuméroter les familles, nous pouvons supposer que le mineur $\mu_1 := \det((a_{ij})_{1 \leqslant i \leqslant r, 2 \leqslant j \leqslant r+1})$ est non nul. Pour $k = 2, \cdots, r+1$, notons alors μ_k le mineur $\det((a_{ij})_{1 \leqslant i \leqslant r, 1 \leqslant j \leqslant r+1, j \neq k}$. Alors pour tout $i = 1, \cdots, n$, la somme $\sum_{k=1}^{r+1} (-1)^{k+1} a_{ik} \mu_k$ est un mineur de taille $r + 1$ de P ou le déterminant d'une matrice ayant deux lignes égales. Elle est donc nulle. Comme E est une base, il s'ensuit que $\sum_{k=1}^{r+1} (-1)^{k+1} \mu_k f_k = 0$, et comme $\mu_1 \neq 0$, on voit que la famille F est liée.

Enfin, il reste à nous débarrasser de l'hypothèse initiale que M admet une base *finie*. Cette hypothèse n'est pas dans l'énoncé de la proposition, qui suppose simplement que $M \simeq A^{(I)}$ pour un ensemble I. Supposons donc I infini, et que M admette par ailleurs une famille génératrice finie, disons de cardinal m. On doit trouver une contradiction. Pour cela, soit $J \subset I$ un ensemble de cardinal $n > m$. On dispose d'un morphisme canonique $A^{(I)} \xrightarrow{\rho} A^J$ qui projette sur les composantes indexées par J. Ce morphisme est surjectif, donc la famille $\rho(F)$ engendre $A^J = A^n$, ce qui contredit la discussion précédente puisque $m < n$ $\square$

1.3.9 *Limites projectives.* Les produits et coproduits sont des cas particuliers d'une construction plus générale où l'on part d'un ensemble d'indices *ordonné* $(I, \leqslant)$. Un *système projectif* d'ensembles indexé par I est une famille $(E_i)_{i\in I}$ d'ensembles munis d'applications $f_{ij} : E_i \longrightarrow E_j$ pour chaque couple $i \geqslant j$ et telles que $f_{jk} \circ f_{ij} = f_{ik}$ et $f_{ii} = \mathrm{id}_{E_i}$. On définit la "limite projective" (ou simplement "limite") du système projectif comme le sous-ensemble suivant du produit $\prod_{i\in I} E_i$:

$$\varprojlim_{i\in I} E_i := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} E_i,\ \forall i \geqslant j, x_j = f_{ij}(x_i) \right\}$$

Supposons maintenant que les E_i sont des groupes/anneaux/modules [12], alors le produit $\prod_{i\in I} E_i$ est naturellement un groupe/anneau/module et son sous-ensemble $\varprojlim_{i\in I} E_i$ est un sous- groupe/anneau/module. On l'appelle toujours "limite (projective)" du système projectif $(E_i)_{i\in I}$ et on vérifie sans peine qu'on a une bijection $\varphi \mapsto (\pi_i \circ \varphi)_{i\in I}$

$$\mathrm{Hom}(E, \varprojlim_i E_i) \longrightarrow \varprojlim_i \mathrm{Hom}(E, E_i)$$

où le Hom est à prendre au sens des groupes/anneaux/modules et la limite projective à droite est celle du système projectif d'ensembles $(\mathrm{Hom}(E, E_i))_{i\in I}$ muni des transitions $\mathrm{Hom}(E, E_i) \longrightarrow \mathrm{Hom}(E, E_j)$, $\varphi_i \mapsto f_{ij} \circ \varphi_i$ pour $i \geqslant j$. Encore mieux, si les E_i sont des ensembles/groupes/anneaux topologiques [13] et les f_{ij} sont continues, alors $\varprojlim_i E_i$ est fermé dans $\prod_i E_i$ muni de la topologie produit, ce qui en fait un ensemble/groupe/anneau topologique.

Remarque. – Plus généralement, un système projectif indexé par I dans une catégorie $\mathcal{C}$ est une famille $(X_i)_{i\in I}$ munie de morphismes $f_{ij} \in \mathcal{C}(X_i, X_j)$ pour $i \geqslant j$. Une paire $(X, (\pi_i)_{i\in I}))$ formée d'un objet X de $\mathcal{C}$ et d'une famille de morphismes $\pi_i \in \mathcal{C}(X, X_i)$ est appelée *limite (projective)* du système $(X_i)_{i\in I}$ si pour tout objet Y l'application $f \mapsto (\pi_i \circ f)_{i\in I}$ induit une bijection

$$\mathcal{C}(Y, X) \xrightarrow{\sim} \varprojlim_{i\in I} \mathcal{C}(Y, X_i),$$

où le membre de droite est la limite du système projectif d'ensembles $(\mathcal{C}(Y, X_i))_{i\in I}$ dont les applications de transition sont données par $\varphi_i \mapsto f_{ij} \circ \varphi_i : \mathcal{C}(Y, X_i) \longrightarrow \mathcal{C}(Y, X_j)$. Une telle paire, si elle existe, est unique à "isomorphisme unique près".

Exemple. (L'anneau des entiers p-adiques) – Soit p un nombre premier, et considérons le système projectif $(\mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{N}}$ indexé par l'ensemble $I = \mathbb{N}$ muni de l'ordre usuel, et où

12. rayer les mentions inutiles
13. ce qui signifie qu'ils sont munis d'une topologie pour laquelle les lois de compositions et passage à l'inverse sont continues

les applications “de transition” sont les projections $f_{nm} : \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^m\mathbb{Z}$ pour $m \leqslant n$. La limite projective

$$\mathbb{Z}_p := \lim_{\longleftarrow\, n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$$

est appelée “anneau des entiers p-adiques” et a une importance fondamentale en théorie des nombres. Notons $\iota : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ le morphisme d'anneaux canonique, qui est donné explicitement par $\iota(a) = (a \bmod p^n)_{n\in\mathbb{N}}$. Notons aussi $\pi_n : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ la projection sur le facteur $\mathbb{Z}/p^n\mathbb{Z}$ et posons $\nu(a) := \mathrm{Max}\{n \in \mathbb{N}, \pi_n(a) = 0\}$ qui est bien défini dès que $a \neq 0$. Voici d'abord quelques propriétés *algébriques* de $\mathbb{Z}_p$.

Proposition. – *i) On a* $\mathrm{Ker}(\pi_n) = \{a \in \mathbb{Z}_p, \nu(a) \geqslant n\} = \iota(p)^n\mathbb{Z}_p$.

ii) Le morphisme ι est injectif et induit par passage aux quotients des isomorphismes $\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}_p/\iota(p)^n\mathbb{Z}_p$ pour tout n.

iii) $\mathbb{Z}_p$ est intègre et $\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p, \nu(a) = 0\}$. Ses idéaux sont les $\iota(p)^n\mathbb{Z}_p$, $n \in \mathbb{N}$. En particulier, $\mathbb{Z}_p$ est principal et possède un unique[14] *idéal maximal, à savoir $\iota(p)\mathbb{Z}_p$.*

Démonstration. i) La première égalité est claire. Puisque $\pi_n(\iota(p)^n) = 0$, on a évidemment l'inclusion $\mathrm{Ker}(\pi_n) \supset \iota(p)^n\mathbb{Z}_p$. Pour l'autre inclusion, considérons un élément $a = (\bar{a}_m)_{m\in\mathbb{N}}$ dans le noyau $\mathrm{Ker}(\pi_n)$ (ici $a_m \in \mathbb{Z}$ et $\bar{a}_m = a_m(\mathrm{mod} p^m)$). Alors p^n divise a_n et donc divise chaque a_{n+m} pour $m \geqslant 0$. Poson $b_m := a_{m+n}/p^n$, alors la famille $b = (\bar{b}_m)_{m\in\mathbb{N}}$ est un élément de $\mathbb{Z}_p$ tel que $p^n b = a$.

ii) Soit $a \in \mathbb{Z}$. Son image $\iota(a) = (a(\mathrm{mod} p^n))_{n\in\mathbb{N}}$ dans $\mathbb{Z}_p$ est nulle si et seulement si p^n divise a pour tout n, donc si et seulement si $a = 0$. Ainsi $\iota : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ est injectif. Considérons la composée $\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\bar{\iota}} \mathbb{Z}_p/\iota(p)^n\mathbb{Z}_p \xrightarrow{\bar{\pi}_n} \mathbb{Z}/p^n\mathbb{Z}$ dans laquelle $\bar{\iota}$ et $\bar{\pi}_n$ sont induites par ι et π_n par passage au quotient. Cette composée doit être l'identité car c'est le seul endomorphisme d'anneau de $\mathbb{Z}/n\mathbb{Z}$, et on vient de voir que $\bar{\pi}_n$ est injective. Il s'ensuit que ces deux morphismes sont des isomorphismes réciproques.

iii) Donnons-nous deux éléments $a = (\bar{a}_n)_{n\in\mathbb{N}}$ et $b = (\bar{b}_n)_{n\in\mathbb{N}}$. Supposons a non nul. Il existe donc un n tel que p^n ne divise pas a_n, et par conséquent ne divise pas non plus a_m pour tout $m \geqslant n$. Supposons maintenant $ab = 0$. Alors pour tout m on a $p^m | a_m b_m$. Par notre choix de n, il s'ensuit que p^{m-n} divise b_m pour tout $m \geqslant n$. Fixons alors $m \geqslant n$. On a $p^m | b_{m+n}$ et $b_{m+n} \equiv b_m[p^m]$, donc $p^m | b_m$ et $\bar{b}_m = 0$. Ceci s'applique pour tout $m \geqslant n$ donc $b = 0$, et $\mathbb{Z}_p$ est bien intègre.

Si $a \in \mathbb{Z}_p^\times$, on doit avoir $\pi_1(a) \in (\mathbb{Z}/p\mathbb{Z})^\times$, donc $\nu(a) = 0$. Réciproquement, soit $a = (\bar{a}_n)_{n\in\mathbb{N}}$ tel que $\nu(a) = 0$. Cela signifie que p ne divise pas a_1 et donc ne divise aucun a_n. Il existe donc des entiers u_n, v_n tels que $u_n a_n + p^n v_n = 1$. Pour $m \geqslant n$, on a alors $p^n | (u_m a_m - u_n a_n)$. Comme on a aussi $p^n | (a_m - a_n)$, il suit $p^n | (u_m a_n - u_n a_n) = (u_m - u_n)a_n$, puis $p^n | (u_m - u_n)$. Ainsi la suite $(\bar{u}_n)_{n\in\mathbb{N}}$ définit un élément u de $\mathbb{Z}_p$, et puisque $\bar{u}_n\bar{a}_n = 1$ dans $\mathbb{Z}/p^n\mathbb{Z}$ pour tout n, on a bien $au = 1$.

Soit I un idéal non nul de $\mathbb{Z}_p$, et soit $\nu(I) := \mathrm{Min}\{\nu(a), a \in I\}$. D'après le i), on a $p^{\nu(I)} | a$ pour tout $a \in I$, c'est-à-dire $I \subset p^{\nu(I)}\mathbb{Z}_p$. De plus, soit $a \in I$ tel que $\nu(a) = \nu(I)$.

14. on dit que c'est un anneau *local*

Ecrivons $a = p^n a'$ pour un (unique) $a' \in \mathbb{Z}_p$. Alors $\nu(a') = 0$, donc $a' \in \mathbb{Z}_p^\times$, et il s'ensuit que $p^{\nu(I)} \in I$ puis finalement que $p^{\nu(I)}\mathbb{Z}_p = I$. $\square$

Remarque. – On voit sur les définitions que $\nu(\iota(n)) = \nu_p(n)$ (valuation p-adique). Le iii) implique donc que pour tout entier n premier à p, l'élément $\iota(n)$ est inversible dans $\mathbb{Z}_p$.

Exercice. – Montrer que la multiplication par $\iota(p)^n$ induit des isomorphismes de modules $\mathbb{Z}_p/\iota(p)\mathbb{Z}_p \xrightarrow{\sim} \iota(p)^n\mathbb{Z}_p/\iota(p)^{n+1}\mathbb{Z}_p$.

On oubliera dorénavant souvent le ι dans les notations et on identifiera $\mathbb{Z}$ à un sous-anneau de $\mathbb{Z}_p$. Nous munissons maintenant $\mathbb{Z}_p$ de la topologie produit en considèrant chaque $\mathbb{Z}/p^n\mathbb{Z}$ comme un anneau topologique discret. Voici quelques propriétés *topologiques* de $\mathbb{Z}_p$.

Proposition. – *i) $\mathbb{Z}_p$ est un anneau compact et "totalement discontinu"[15], dont la topologie est engendrée par les ouverts de la forme*

$$a + p^n\mathbb{Z}_p = \{z \in \mathbb{Z}_p, \nu(z-a) \geqslant n\},$$

où $a \in \mathbb{Z}_p$ et $n \in \mathbb{N}$. C'est aussi la topologie métrique associée à la distance[16] $|a-b| := p^{-\nu(a-b)}$.

ii) Le morphisme ι est injectif et fait de $\mathbb{Z}_p$ le complété de $\mathbb{Z}$ pour la topologie engendrée par les ensembles de la forme $a + p^n\mathbb{Z}$ (appelée topologie p-adique), qui est aussi la topologie métrique associée à la distance p-adique $|a-b|_p := p^{-\nu_p(a-b)}$.

iii) Toute série $\sum_{n\in\mathbb{N}} a_n p^n$ avec $a_n \in \mathbb{Z}$ est convergente dans $\mathbb{Z}_p$, et tout élément a de $\mathbb{Z}_p$ s'écrit de manière unique comme limite d'une série

$$a = \sum_{n\in\mathbb{N}} a_n p^n \text{ avec } a_n \in \{0, \cdots, p-1\}, \forall n \in \mathbb{N}.$$

Démonstration. i) Rappelons qu'un produit de compacts, muni de la topologie produit, est compact. De plus, un produit d'ensembles discrets, muni de la topologie produit, est totalement discontinu (exercice... indication :remarquer que le complémentaire d'un ouvert standard d'un tel produit est encore ouvert). Ainsi $\mathbb{Z}_p$, qui est fermé dans $\prod_n \mathbb{Z}/p^n\mathbb{Z}$, est aussi compact et totalement discontinu. Par définition, la topologie dont on a muni $\mathbb{Z}_p$ est engendrée par les ensembles de la forme $\pi_n^{-1}(U)$ où U est un ouvert de $\mathbb{Z}/p^n\mathbb{Z}$. Ce dernier étant discret on peut se restreindre aux singletons $U = \{\bar{a}\}$ avec $a \in \mathbb{Z}$. Il nous faut donc vérifier que dans ce cas $\pi_n^{-1}(U) = \iota(a) + p^n\mathbb{Z}_p$. Quitte à translater par $\iota(a)$, cela équivaut à montrer que $\mathrm{Ker}(\pi_n) = p^n\mathbb{Z}_p$, ce que l'on a fait au i) de la proposition précédente. La dernière assertion est une simple réinterprétation de l'égalité $p^n\mathbb{Z}_p = \{z \in \mathbb{Z}_p, \nu(z) \geqslant n\}$.

ii) D'après le i), la topologie induite sur $\mathbb{Z}$ est bien de la forme décrite, et on constate qu'elle est donnée par la distance mentionnée. Comme $\mathbb{Z}_p$ est compact et donc complet, il reste à voir que $\mathbb{Z}$ est dense dans $\mathbb{Z}_p$. Or si $a = (\bar{a}_n)_{n\in\mathbb{N}}$ est un élément de $\mathbb{Z}_p$, la suite $(a_n)_{n\in\mathbb{N}}$

15. cela signifie que ses sous-ensembles connexes maximaux sont les singletons

16. Cette distance vérifie l'inégalité triangulaire "ultramétrique" suivante : $|a-b| \leqslant \max(|a-c|, |c-b|)$, laquelle vient en l'occurence de l'inégalité $\nu(a-b) \geqslant \min(\nu(a-c), \nu(c-b))$.

(ou plutôt $\iota(a_n)_{n\in\mathbb{N}}$ pour être précis) tend vers a puisque $\iota(a_n) - a \in \mathrm{Ker}(\pi_n) = p^n\mathbb{Z}_p$, et la suite décroissantes d'ouverts $a + p^n\mathbb{Z}_p$ est une base de voisinages de a dans $\mathbb{Z}_p$.

iii) Remarquons d'abord qu'une série de la forme $\sum_n a_n p^n$ avec $a_n \in \mathbb{Z}$ a toujours une unique limite dans $\mathbb{Z}_p$ puisque ses sommes partielles forment une suite de Cauchy.

Soit $a \in \mathbb{Z}_p$ et $(\alpha_n)_{n\in\mathbb{N}} \in \mathbb{N}^{\mathbb{N}}$ une suite telle que $a = (\bar{\alpha}_n)_{n\in\mathbb{N}}$. Soit $\alpha_n = \sum_m a_m(\alpha_n)p^m$ le développement de α_n en base p (avec donc $a_m(\alpha_n) \in \{0, \cdots, p-1\}$). Posons $a_m := a_m(\alpha_{m+1})$. Alors pour tout $n \geqslant m+1$, on a $\alpha_n \equiv \alpha_{m+1}[p^{m+1}]$, donc $a_m(\alpha_n) = a_m$. Il s'ensuit que $p^n|(\alpha_n - \sum_{m=1}^{n-1} a_m p^m)$ et donc aussi que $\nu(a - \sum_{m=1}^{n-1} a_m p^m) \geqslant n$, ce qui montre que la série $\sum_n a_n p^n$ converge vers a.

Pour l'unicité, supposons $a = \sum_n a_n p^n = \sum_n a'_n p^n$ avec $a_n, a'_n \in \{0, \cdots, p-1\}$, et notons $s_n := \sum_{m=1}^{n-1} a_m p^m$, $s'_n := \sum_{m=1}^{n-1} a'_m p^m$ les sommes partielles. Alors $s_n, s'_n \in \{0, \cdots, p^n - 1\}$ et $\pi_n(s_n) = \pi_n(s'_n)$ dans $\mathbb{Z}/p^n\mathbb{Z}$. Donc $s_n = s'_n$ pour tout n, et il s'ensuit que $a_n = a'_n$ pour tout n. □

Remarque. – On peut donc penser à un nombre p-adique comme à un développement en base p avec éventuellement une infinité de chiffres. La somme et le produit donnés par les algorithmes usuels (avec retenues) sur les développements en base p d'entiers passent à la limite pour donner la somme et le produit dans $\mathbb{Z}_p$.

Exercice. – Ecrire le développement en base p de l'inverse de $1 + p$ dans $\mathbb{Z}_p$.

Remarque. – Plus généralement, si A est un anneau et I un idéal, la limite projective

$$\widehat{A}_I := \lim_{\longleftarrow n} A/I^n$$

est appelée "complété I-adique de A". Le morphisme $A \longrightarrow \widehat{A}_I$ (donné par la propriété universelle de la limite projective) fait de $\widehat{A}_I$ le séparé-complété de A pour la topologie engendrée par les ensembles de la forme $a + I^n$, $a \in A$, $n \in \mathbb{N}$.

Voici un exemple de limite projective d'un genre un peu différent.

Exemple. – Considérons l'ensemble I des parties non vides de $\{1, 2\}$ ordonné par contenance. Un système projectif d'ensembles indexé par I est donc la donnée d'un diagramme

$$\begin{tikzcd} & E_1 \arrow[d, "f_1"] \\ E_2 \arrow[r, "f_2"] & E_{1,2} \end{tikzcd}$$

La limite projective s'identifie alors au "produit fibré" $E_1 \times_{E_{12}} E_2 := \{(e_1, e_2) \in E_1 \times E_2,\ f_1(e_1) = f_2(e_2)\}$. Lorsque E_1, E_2 sont des sous-ensembles de E et f_1, f_2 les inclusions associées, alors ce produit fibré n'est autre que l'intersection $E_1 \cap E_2$.

D'autres exemples apparaitront au fil du cours, comme par exemple le groupe de Galois absolu de $\mathbb{Q}$, qui est limite projective de groupes finis. Si on aime l'analyse fonctionnelle, on pourra s'émouvoir d'apprendre qu'un espace de Fréchet est une limite projective d'espaces de Banach dans la catégorie des espaces vectoriels topologiques.

Remarque. – La notion de limite admet encore une généralisation naturelle où l'on remplace $(I, \leqslant)$ par une "petite catégorie" $\mathcal{I}$ (i.e. dont les objets forment un ensemble I), et on remplace la notion de "système projectif indexé par $(I, \leqslant)$" par celle de "diagramme indexé par $\mathcal{I}$" qui par définition est simplement un foncteur $\mathcal{X} : \mathcal{I} \longrightarrow \mathcal{C}$, et qui n'est finalement qu'une famille $(\mathcal{X}(i))_{i\in I}$ d'objets munie d'une famille de morphismes $\mathcal{X}(i) \xrightarrow{\mathcal{X}(f)} \mathcal{X}(j)$ pour chaque $f \in \mathcal{I}(i,j)$ satisfaisant $\mathcal{X}(f\circ g) = \mathcal{X}(f)\circ\mathcal{X}(g)$ et $\mathcal{X}(\mathrm{id}_i) = \mathrm{id}_{\mathcal{X}(i)}$. Lorsque $\mathcal{C}$ est la catégorie des ensembles, on définit la limite d'un diagramme par

$$\varprojlim(\mathcal{X}) := \left\{(x_i)_{i\in I} \in \prod_{i\in I} X_i,\ \forall i,j\in I, \forall f \in \mathcal{C}(X_i, X_j), f(x_i) = x_j\right\}$$

Puis, pour une catégorie $\mathcal{C}$ quelconque, on définit une limite d'un diagramme à valeurs dans $\mathcal{C}$ comme une paire $(X, (\pi_i \in \mathcal{C}(X, \mathcal{X}(i)))_{i\in I})$ telle que l'application $\varphi \mapsto (\pi_i \circ \varphi)_{i\in I}$ soit une bijection $\mathcal{C}(Y,X) \xrightarrow{\sim} \varprojlim(\mathcal{C}(Y,\mathcal{X}))$ pour tout Y, où $\mathcal{C}(Y,\mathcal{X})$ désigne le diagramme d'ensembles $i \mapsto \mathcal{C}(Y,\mathcal{X}(i))$, $f \in \mathcal{I}(i,j) \mapsto [\mathcal{C}(Y,\mathcal{X}(i)) \xrightarrow{\phi\mapsto\mathcal{X}(f)\circ\phi} \mathcal{C}(Y,\mathcal{X}(j))]$.

Beaucoup de constructions sont des cas particuliers de limites en ce sens étendu.

Exemple. – Soit G un groupe fini, et $\mathcal{G}$ la catégorie avec un seul objet $\bullet$ et morphismes $\mathcal{C}(\bullet,\bullet) = G$ (avec la loi de composition de G). Soit par ailleurs $\mathrm{Vec}_{\mathbb{C}}$ la catégorie des espaces vectoriels de dimension finie sur $\mathbb{C}$. Alors un foncteur $\mathcal{G} \longrightarrow \mathrm{Vec}_{\mathbb{C}}$ est donné par une représentation linéaire de G sur un espace vectoriel V. La limite projective associée n'est autre que le sous-espace V^G des invariants sous G.

1.3.10 *Limites inductives.* Soit à nouveau $(I, \leqslant)$ un ensemble ordonné. Un *système inductif indexé par* I dans une catégorie $\mathcal{C}$ est un système projectif indexé par I dans la catégorie opposée $\mathcal{C}^{\mathrm{opp}}$. C'est donc une famille $(X_i)_{i\in I}$ d'objets de $\mathcal{C}$ munie de morphismes $X_i \xrightarrow{f_{ij}} X_j$ pour $i \leqslant j$ qui se composent bien. On appelle alors *colimite* ou *limite inductive* d'un tel système toute paire $(X, (\iota_i)_{i\in I})$ qui est une limite projective dans $\mathcal{C}^{\mathrm{opp}}$. Ainsi, pour tout objet Y, l'application $f \mapsto (f\circ\iota_i)_{i\in I}$ doit induire une bijection

$$\mathcal{C}(X,Y) \xrightarrow{\sim} \varprojlim_{i\in I} \mathcal{C}(X_i, Y),$$

où le membre de droite est la limite du système projectif $(\mathcal{C}(X_i,Y))_{i\in I}$ dont les applications de transition sont données par $\varphi_i \mapsto \varphi_i \circ f_{ji} : \mathcal{C}(X_i, Y) \longrightarrow \mathcal{C}(X_j, Y)$ pour $i \geqslant j$.

Exemple. – Tout système inductif d'ensembles admet une limite inductive, donnée par l'ensemble quotient suivant (exercice)

$$\varinjlim_{i\in I} E_i := \coprod_{i\in I} E_i/\sim$$

où la relation d'équivalence est déterminée par $x_j = f_{ij}(x_i) \Rightarrow x_i \sim x_j$ pour tous $i \leqslant j$.

Exemple. – Tout système inductif de modules admet aussi une limite inductive donnée par le quotient de $\bigoplus_{i\in I} M_i$ par le sous-module engendré par les $\iota_i(x_i) - \iota_j(f_{ij}(x_i))$ pour $i \leqslant j$ et $x_i \in M_i$ (exercice).

Remarque. – Remarquons que si les M_i sont des sous-modules d'un module M tels que $i \leqslant j \Rightarrow M_i \subset M_j$ alors le système inductif obtenu (avec applications de transition données par les inclusions) a pour limite la somme $\sum_{i\in I} M_i$ calculée dans M. Ainsi, lorsqu'on a plus généralement un système inductif à transitions injectives de modules qui ne sont pas nécessairement contenus dans un module ambiant, on peut penser à la limite inductive comme une manière "externe" de faire exister cette somme. C'est selon ce principe qu'on construira les clôtures algébriques plus tard.

Exemple. – La notion de germe d'une fonction (polynomiale, holomorphe, etc.) en un point z de $\mathbb{C}^n$ est en général définie comme une classe d'équivalence de paires (U, f) formée d'un voisinage ouvert de z et d'une fonction (polynomiale, holomorphe) sur U. Soit alors I l'ensemble des voisinages ouverts de z, ordonné par contenance. On constate ainsi que le $\mathbb{C}$-ev des germes de fonctions holomorphes (par exemple) en z est la limite inductive du système inductif des $\mathbb{C}$-espaces vectoriels $\mathcal{O}(U)$ des fonctions holomorphes sur $U \in I$ avec morphismes de transition $\mathcal{O}(U) \longrightarrow \mathcal{O}(V)$ donnés par restriction des fonctions $f \mapsto f_{|V}$ pour $U \supset V$.

Remarque. – Comme précédemment, on peut remplacer systèmes inductifs par diagrammes indexés par une petite catégorie. La colimite (ou limite inductive) se définit comme ci-dessus. Dans l'exemple de la catégorie $\mathcal{G}$ associée à un groupe fini G et d'un diagramme $\mathcal{G} \longrightarrow \mathrm{Vec}_{\mathbb{C}}$ donné par une représentation V de G, la colimite est l'espace quotient V_G de V par le sous-espace engendré par les $v - gv$, $v \in V$ et $g \in G$ (appelé coinvariants de G).

1.3.11 *Modules et anneaux noethériens.* Les modules de type fini ont les propriétés suivantes :

— M de type fini et $N \subset M \Rightarrow M/N$ de type fini (exercice).
— N de type fini et M/N de type fini $\Rightarrow M$ de type fini. En effet, si N est engendré par $m_1, \cdots m_r \in M$ et si M/N est engendré par des éléments $\overline{m}_{r+1}, \cdots, \overline{m}_{r+s}$ (avec $m_{r+1}, \cdots, m_{r+s} \in M$), alors M est engendré par $m_1, \cdots m_{r+s}$ (exercice).

Par contre, un sous-module d'un module de type fini n'est pas nécessairement de type fini ! Voici deux exemples :

Exemple. – $M = A = \mathbb{Z}[X_i, i \in \mathbb{N}]$, (l'anneau des polynômes en une infinité de variables, cf plus bas) et N l'idéal formé de tous les polynômes de terme constant nul. Toute famille finie de N est contenue dans l'idéal engendré par $X_1, \cdots, X_n$ pour n assez grand, et cet idéal ne contient pas X_{n+1}. Donc N n'est pas de type fini.

Exemple. – $M = A = \overline{\mathbb{Z}}$ et N l'idéal engendré par la suite $(x_n)_{n\in\mathbb{N}}$ où $x_0 = 2$ et x_n est une racine carrée de x_{n-1}. À nouveau, toute sous-module de type fini de N est contenu dans le sous-anneau engendré par $x_1, \cdots, x_n$ pour n assez grand, et ce dernier ne contient pas x_{n+1}.

Pour éviter ces pathologies, on introduit la notion de module et anneau noethérien (en l'honneur d'Emmy Noether qui a inventé ces notions)

Proposition. – *Soit M un A-module. Les propriétés suivantes sont équivalentes :*

i) tout sous-A-module de M est de type fini.

ii) toute suite croissante de sous-A-modules devient stationnaire à partir d'un certain rang.

iii) tout ensemble non vide de sous-A-module de M admet un élément maximal pour l'inclusion.

Démonstration. *i)* $\Rightarrow$ *ii)*. Soit $(M_n)_{n\in\mathbb{N}}$ une suite croissante de sous-modules. Alors la réunion $M = \bigcup_{n\in\mathbb{N}} M_n$ est aussi un sous-module (le vérifier !). Sous la propriété i), il est engendré par une famille finie d'éléments, laquelle est contenue dans un M_n pour n assez grand. Il s'ensuit que $M = M_n$ et que $M_N = M_n$ pour tout $N \geqslant n$.

ii) $\Rightarrow$ *iii)*. Montrons la contraposée. Supposons qu'il existe un ensemble de sous-A-modules de M sans élément maximal. On peut alors construire par récurrence une suite strictement croissante, et donc qui ne devient jamais stationnaire.

iii) $\Rightarrow$ *i)*. Soit M' un sous-module de M. Considérons l'ensemble des sous-modules de type fini de M', qui est non vide puisqu'il contient $\{0\}$. Sous la propriété iii), il admet un élément maximal N. Soit alors m' un élément quelconque de M'. Le sous-module $N + (m')$ de M' est de type fini, donc contenu dans N par maximalité de ce dernier. Donc $m' \in N$ et $M' = N$ est de type fini. □

Définition. – *Un A-module M satisfaisant les conditions équivalentes de la proposition sera dit* noethérien. *L'anneau A est dit lui-même* noethérien*, s'il est noethérien en tant que A-module.*

Ainsi, un anneau est noethérien si tous ses idéaux sont de type fini. En particulier, un anneau *principal* (i.e. dont tous les idéaux sont principaux) est noethérien.

Proposition. – *i) Soit M un A-module et N un sous-module. Alors M est noethérien si et seulement si N et M/N le sont.*

ii) Une somme directe finie de modules est noethérienne si et seulement si chacun des facteur est noethérien.

iii) Sur un anneau noethérien, tout module de type fini est noethérien.

iv) Soit $B \xrightarrow{\varphi} A$ *un morphisme d'anneaux. Si M est de type fini, resp. noethérien, en tant que B-module, alors il l'est aussi en tant que A-module.*

Démonstration. i) Supposons M noethérien. Alors tout sous-module de N est un sous-module de M donc est de type fini, et N est noethérien. De plus, tout sous-module $\overline{P}$ de M/N est l'image par la projection $M \longrightarrow M/N$ d'un sous-module P de M (contenant N), lequel est engendré par une famille finie $m_1, \cdots, m_r$. Donc $\overline{P}$ est engendré par $\overline{m}_1, \cdots, \overline{m}_r$ et M/N est noethérien.

Supposons maintenant que N et M/N sont noethériens et soit P un sous-module de M. Alors $P\cap N$, qui est un sous-module de N est de type fini. Par ailleurs, le quotient $P/(P\cap N)$ est canoniquement isomorphe au quotient $(N + P)/N$ (2ème théorème d'isomorphisme), lequel est un sous-module de M/N (cf Exercice du paragraphe 1.3.4) donc est de type fini. Il s'ensuit que P est lui-même de type fini : si $P \cap N$ est engendré par $p_1, \cdots, p_r$ et $P/(N \cap P)$ est engendré par $\overline{p}_{r+1}, \cdots, \overline{p}_s$, alors P est engendré par $p_1, \cdots, p_s$ où $p_{r+1}, \cdots p_s$ sont des relèvements quelconques de $\overline{p}_{r+1}, \cdots, \overline{p}_s$ dans P.

ii) c'est un cas particulier de i) lorsque il y a 2 facteurs puisque, si $M = M_1 \oplus M_2$, la projection sur M_2 induit un isomorphisme $M/M_1 \xrightarrow{\sim} M_2$. On passe à n facteurs par une récurrence immédiate.

iii) Supposons que M est engendré par $m_1, \cdots, m_r$. À cette famille correspond un morphisme surjectif $A^r \longrightarrow M$ (qui envoie e_i sur m_i). Ainsi M est un quotient de A^r qui, par le point ii), est noethérien, donc M est noethérien par le point i).

iv) Pour "de type fini", il suffit de remarquer que toute famille génératrice pour B l'est a fortiori pour A. Pour "noethérien", il suffit de remarquer que toute suite croissante de sous-A-modules de M est aussi une suite croissante de sous-B-modules. □

Corollaire. – *Tout anneau quotient d'un anneau noethérien est noethérien.*

Démonstration. Supposons $A = B/J$ avec B noethérien. Le B-module B/J est de type fini (et même monogène) donc noethérien, et donc noethérien aussi en tant que A-module d'après le iv) de la proposition précédente. Donc l'anneau A est noethérien. □

Une vertu des anneaux noethériens est qu'ils possèdent suffisamment d'éléments irréducibles (contrairement à l'anneau $\overline{\mathbb{Z}}$ qui n'en possède aucun, par exemple).

Théorème. – *Soit A un anneau intègre et noethérien. Tout élément non nul et non inversible est produit d'éléments irréductibles.*

Démonstration. Considérons l'ensemble $\mathcal{I}$ de tous les idéaux principaux (a) engendrés par un élément non nul et non inversible qui *n'est pas produit d'éléments irréductible*. Si cet ensemble $\mathcal{I}$ est non vide, il possède un élément maximal (a) car A est supposé noethérien. Puisque a n'est pas irréducible, on peut l'écrire $a = bc$ avec b, c non inversibles. Alors (b) et (c) contiennent *strictement* (a). En effet, si on avait par exemple $(b) = (a)$, ie $b = ad$ pour un $d \in A$, on aurait $a = acd$ et donc $cd = 1$ (A est intègre), contredisant la non-inversibilité de c. Maintenant, puisque a n'est pas produit d'irréductibles, il en va de même pour b ou pour c, mais cela contredit le choix de (a) comme élément maximal de $\mathcal{I}$. □

Remarque. – Il n'est peut-être pas inutile d'expliciter le lien entre éléments irréductibles et idéaux principaux dans un anneau *intègre*. Remarquons d'abord qu'un élément $a \in A$ est irréductible si et seulement si l'idéal principal (a) est *maximal parmi les idéaux propres principaux de A*. En effet, supposons $a = bc$ avec b non inversible. Alors (b) est un idéal principal propre contenant (a), et on voit que $(b) = (a)$ si et seulement si c est inversible (remarquer que $b = ad \Rightarrow a = acd \Rightarrow 1 = cd$ car A est supposé intègre). En fait, l'application $a \mapsto (a)$ induit, dans tout anneau *intègre*, une bijection

$$\begin{gathered}\{\text{ éléments irréductibles modulo équivalence }\}\\ \longleftrightarrow \{\text{ idéaux principaux, maximaux } \textit{parmi} \text{ les idéaux principaux propres}\}.\end{gathered}$$

1.4 Anneaux de polynômes

1.4.1 *L'algèbre d'un monoïde : construction et propriété universelle.* Soit A un anneau commutatif et soit $(\mathcal{N}, +, \nu_0)$ un monoïde associatif d'élément neutre ν_0. Nous allons profiter de la loi de $\mathcal{N}$ pour munir le A-module libre $A^{(\mathcal{N})}$ d'une structure de A-algèbre. Pour cela, considérons la base canonique $(e_\nu)_{\nu\in\mathcal{N}}$ de $A^{(\mathcal{N})}$, de sorte que tout élément de $A^{(\mathcal{N})}$ s'écrit de manière unique $(a_\nu)_{\nu\in\mathcal{N}} = \sum_{\nu\in\mathcal{N}} a_\nu e_\nu$.

Proposition. – *Il existe une unique structure de A-algèbre sur $A^{(\mathcal{N})}$ telle que*

$$e_\nu \cdot e_{\nu'} = e_{\nu+\nu'} \text{ pour tous } \nu, \nu' \in \mathcal{N}.$$

Démonstration. Supposons qu'une telle multiplication existe. Alors par A-linéarité on doit avoir

$$(a_\nu)_{\nu\in\mathcal{N}} \cdot (b_\nu)_{\nu\in\mathcal{N}} = (c_\nu)_{\nu\in\mathcal{N}} \quad \text{avec} \quad c_\nu = \sum_{\mu+\rho=\nu} a_\mu b_\rho,$$

ce qui montre l'unicité.

Pour l'existence, remarquons d'abord qu'on peut définir c_ν par la somme ci-dessus car celle-ci est finie puisqu'on est dans $A^{(\mathcal{N})}$ et pas dans $A^{\mathcal{N}}$. Un calcul immédiat montre alors l'associativité et la A-bilinéarité. L'élément neutre est e_{ν_0} et la structure de A-algèbre est donnée par le morphisme $A \longrightarrow A^{(\mathbb{N})}$, $a \mapsto ae_{\nu_0}$. □

Remarque. – Malgré notre notation + pour la loi de $\mathcal{N}$, la construction marche très bien si $\mathcal{N}$ n'est pas commutatif. Dans ce cas, $A^{(\mathcal{N})}$ n'est pas commutatif non plus.

Définition. – *La A-algèbre ainsi définie est appelée* A-algèbre du monoïde $\mathcal{N}$ *et se note généralement $A[\mathcal{N}]$. Lorsque $\mathcal{N}$ est un groupe, on parle aussi de* A-algèbre de groupe.

L'algèbre $\mathcal{A}[\mathcal{N}]$ munie de sa base $(e_\nu)_{\nu\in\mathcal{N}}$ peut aussi être caractérisée par une propriété universelle, qui comme souvent est la meilleure manière de l'utiliser.

Proposition. – *Soit B une A-algèbre munie d'un morphisme de monoïdes $\nu \mapsto b_\nu$, $(\mathcal{N}, +, \nu_0) \longrightarrow (B, \cdot, 1)$. Alors il existe un unique morphisme de A-algèbres $\varphi : A[\mathcal{N}] \longrightarrow B$ tel que $\varphi(e_\nu) = b_\nu$ pour tout $\nu \in \mathcal{N}$. En d'autres termes, pour toute A-algèbre B, l'application $\varphi \mapsto (\nu \mapsto \varphi(e_\nu))$ est une bijection*

$$\mathrm{Hom}_{A-\mathrm{alg}}(A[\mathcal{N}], B) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{mono}}(\mathcal{N}, (B, \cdot)).$$

Rappelons que “$\nu \mapsto b_\nu$ est un morphisme de monoïdes” signifie qu'on a dans B les égalités $b_\nu b_{\nu'} = b_{\nu+\nu'}$ pour tous $\nu, \nu' \in \mathcal{N}$ et $b_{\nu_0} = 1$.

Démonstration. Puisque la famille $(e_\nu)_{\nu\in\mathcal{N}}$ est une base de $A[\mathcal{N}]$, la propriété universelle des A-modules libres nous assure l'existence d'un *unique* morphisme de A-modules $\varphi : A[\mathcal{N}] \longrightarrow B$ qui envoie e_ν sur b_ν. On en déduit a fortiori l'unicité d'un morphisme comme dans l'énoncé. Pour l'existence, il faut voir que ce morphisme φ est bien compatible à la multiplication. C'est clair sur la base $(e_\nu)_{\nu\in\mathcal{N}}$ puisque $\varphi(e_\nu e_{\nu'}) = \varphi(e_{\nu+\nu'}) = b_{\nu+\nu'} = b_\nu b_{\nu'}$. Par linéarité, c'est vrai partout. □

Les exemples qui nous intéressent dans ce cours sont développés ci-dessous. Auparavant, voici un exemple parlant pour ceux qui connaissent les représentations de groupes.

Exemple. – Supposons que $\mathcal{N}$ est un groupe, que nous noterons G pour des raisons psychologiques, et considérons la $\mathbb{C}$-algèbre $\mathbb{C}[G]$ du groupe G. On se rappelle qu'un module sur $\mathbb{C}[G]$ est un groupe abélien V muni d'un morphisme d'anneaux $\mathbb{C}[G] \longrightarrow \mathrm{End}_{\mathbb{Z}}(V)$. C'est donc aussi un $\mathbb{C}$-espace vectoriel V muni d'un morphisme de $\mathbb{C}$-algèbres $\mathbb{C}[G] \longrightarrow \mathrm{End}_{\mathbb{C}}(V)$. Par la propriété universelle, se donner un tel morphisme revient à se donner un morphisme de groupes $G \longrightarrow \mathrm{Aut}_{\mathbb{C}}(V) = \mathrm{GL}(V)$, c'est-à-dire une représentation complexe de G. Ainsi la catégorie des représentations de G n'est autre que celle des $\mathbb{C}[G]$-modules.

1.4.2 *Polynômes en* 1 *variable.* C'est le cas particulier où $(\mathcal{N}, +, \nu_0) = (\mathbb{N}, +, 0)$. Notons alors X l'élément $e_1 = (0, 1, 0, 0, \cdots)$ de $A[\mathbb{N}] = A^{(\mathbb{N})}$. Par définition on a $X^n = e_n$, donc la famille $\{1, X, X^2, \cdots\}$ est la base canonique de $A^{(\mathbb{N})}$. Tout élément s'écrit donc de manière unique $(a_n)_{n\in\mathbb{N}} = \sum_{n\in\mathbb{N}} a_n X^n$ avec $a_n = 0$ pour $n >> 0$, et la multiplication s'écrit

$$\left(\sum_n a_n X^n\right) \cdot \left(\sum_n b_n X^n\right) = \sum_n \left(\sum_{p+q=n} a_p b_q\right) X^n.$$

Définition. – *La A-algèbre $A[\mathbb{N}]$ se note $A[X]$ et est appelée* A-algèbre des polynômes en l'indéterminée X *sur A. Ses éléments sont appelés* polynômes (en l'indéterminée X) à coefficients dans A.

La A-algèbre des polynômes $A[X]$ munie de son élément X est caractérisée par la propriété universelle suivante :

Proposition. – *Pour toute A-algèbre B (commutative ou non) et tout élément $b \in B$, il existe un unique morphisme de A-algèbres $\varphi : A[X] \longrightarrow B$ tel que $\varphi(X) = b$. En d'autres termes, pour toute A-algèbre B, l'application $\varphi \mapsto \varphi(X)$ est une bijection*

$$\mathrm{Hom}_{A-\mathrm{alg}}(A[X], B) \xrightarrow{\sim} B.$$

Sa bijection réciproque associe à un élement $b \in B$ le morphisme d'"évaluation en b", i.e. le morphisme $A[X] \longrightarrow B$ qui envoie $f = \sum_n a_n X^n$ sur $f(b) := \sum_n a_n b^n$.

Démonstration. C'est une reformulation de la propriété universelle de l'algèbre $A[\mathbb{N}]$, une fois qu'on a remarqué qu'un morphisme de monoïde $\mathbb{N} \longrightarrow (B, \cdot)$ est entièrement déterminé par l'image de $1 \in \mathbb{N}$. □

On peut résumer informellement la proposition ci-dessus ainsi : *Se donner un morphisme de A-algèbres $A[X] \longrightarrow B$ revient à se donner l'image $b \in B$ de X.*

Corollaire. – *Soit M un A-module et χ un endomorphisme du A-module M. Il existe une unique structure de $A[X]$-module sur M qui étend celle de A-module et telle que X agisse par χ. Ainsi, la donnée d'un $A[X]$-module est équivalente à celle d'un couple formé d'un A-module et d'un endomorphisme de celui-ci.*

Démonstration. En effet, si $A \xrightarrow{\rho} \mathrm{End}_{\mathbb{Z}}(M)$ est le morphisme d'anneau qui définit la structure de A-module sur M, alors d'après la proposition précédente, il existe un unique morphisme de A-algèbres $A[X] \xrightarrow{\tilde{\rho}} \mathrm{End}_{\mathbb{Z}}(M)$ qui prolonge ρ et envoie X sur χ. Celui-ci définit la structure de $A[X]$-module annoncée. □

La propriété universelle de $A[X]$ et celle des quotients impliquent une propriété universelle pour une A-algèbre de la forme $A[X]/(f)$ où $f \in A[X]$.

COROLLAIRE. – *Soit $f \in A[X]$, et notons $\bar{X}$ l'image de X dans $A[X]/(f)$. Alors pour toute A-algèbre B, l'application $\varphi \mapsto \varphi(\bar{X})$ induit une bijection*

$$\mathrm{Hom}_{A-\mathrm{alg}}(A[X]/(f), B) \xrightarrow{\sim} \{b \in B, f(b) = 0\}.$$

On peut grossièrement paraphraser cet énoncé en disant que "se donner un morphisme de A-algèbres $A[X]/(f) \longrightarrow B$ revient à se donner une racine de f dans B".

Démonstration. Tout d'abord, l'application de l'énoncé est bien définie car $f(\varphi(\bar{X})) = \varphi(f(\bar{X})) = \varphi(\overline{f(X)}) = \varphi(\bar{f}) = \varphi(0) = 0$.

Construisons maintenant la bijection réciproque. Partons de $b \in B$ tel que $f(b) = 0$. La proposition précédente nous fournit un unique morphisme $\tilde{\varphi} : A[X] \longrightarrow B$ tel que $\tilde{\varphi}(X) = b$. On a alors $\tilde{\varphi}(f) = f(b) = 0$, donc $f \in \mathrm{Ker}(\tilde{\varphi})$ et la propriété universelle des quotients nous dit que $\tilde{\varphi}$ se factorise par un morphisme $\varphi : A[X]/(f) \longrightarrow B$ tel que $\varphi(\bar{X}) = \tilde{\varphi}(X) = b$.

Par construction, ces deux applications sont inverses l'une de l'autre. □

Exemples. – se donner un morphisme d'anneaux $\mathbb{Z}[X]/(X^n) \longrightarrow B$ revient à se donner un élément nilpotent d'indice $\leqslant n$ de B. Se donner un morphisme d'anneaux $\mathbb{Z}[X]/(X^n - 1) \longrightarrow B$ revient à se donner une racine n-ème de l'unité de B.

Voici un autre corollaire utile de la propriété universelle (que l'on pourrait aussi voir plus laborieusement sur la construction).

COROLLAIRE. – *Soit I un idéal de A. Notons $\varphi : A[X] \longrightarrow A/I[X]$ l'unique morphisme de A-algèbres qui envoie X sur X. Alors φ induit un isomorphisme*

$$\bar{\varphi} : A[X]/IA[X] \xrightarrow{\sim} A/I[X].$$

Démonstration. Puisque $\varphi(I) = 0$, l'idéal $IA[X]$ de $A[X]$ est contenu dans $\mathrm{Ker}(\varphi)$ et donc φ passe bien au quotient pour donner $\bar{\varphi}$ comme dans l'énoncé. Dans l'autre sens, partons du morphisme $A \longrightarrow A[X]$ et composons-le avec la projection $A[X] \longrightarrow A[X]/IA[X]$. Le morphisme ψ obtenu est nul sur I donc se factorise par un morphisme de A-algèbres $\bar{\psi} : A/I \longrightarrow A[X]/IA[X]$. La propriété universelle de $A/I[X]$ nous fournit alors un unique morphisme $\tilde{\psi} : A/I[X] \longrightarrow A[X]/IA[X]$. La composée $\bar{\varphi} \circ \tilde{\psi}$ est l'unique endomorphisme de la A/I-algèbre $A/I[X]$ qui envoie X sur X, donc c'est l'identité. De même pour l'autre composée, de sorte que les morphismes $\bar{\varphi}$ et $\tilde{\psi}$ sont inverses l'un de l'autre. □

1.4.3 *Transfert de propriétés.* Nous allons voir que certaines propriétés d'un anneau A se transfèrent à l'anneau $A[X]$. Rappelons d'abord quelques définitions.

DÉFINITION. – *Soit* $f = \sum_n a_n X^n$ *un polynôme* non nul.

i) Son degré $\deg(f)$ *est le plus grand indice* n *tel que* $a_n \neq 0$.

ii) Son coefficient dominant *est* $a_{\deg(f)}$.

iii) On dit que f *est* unitaire *si* $a_{\deg(f)} = 1$.

PROPOSITION. – *Soit* $f = \sum_n a_n X^n$ *et* $g = \sum_n b_n X^n$ *dans* $A[X]$ *supposés non nuls. Ecrivons* $fg = \sum_n c_n X^n$. *Alors on a* $\deg(fg) \leqslant \deg(f)+\deg(g)$ *avec égalité si et seulement si* $a_{\deg(f)}b_{\deg(g)} \neq 0$. *Dans ce cas, on a* $c_{\deg(fg)} = a_{\deg(f)}b_{\deg(g)}$.

Démonstration. La définition du produit montre que $fg = a_{\deg(f)}b_{\deg(g)}X^{\deg(f)+\deg(g)}+$ (termes de degré plus petit). □

Remarque. – Pour que l'égalité sur le degré d'un produit soit vraie sans restriction sur les facteurs, on déclarera que le degré du polynôme nul est $-\infty$, et que ce symbole vérifie les relations d'ordre $-\infty < 0$ et d'addition $\forall n \in \mathbb{N}$, $-\infty + n = -\infty$.

Exercice. – Donner un exemple de polynômes où $\deg(fg) < \deg(f) + \deg(g)$.

COROLLAIRE. – *Si* A *est intègre, alors* $A[X]$ *est intègre aussi, et* $A[X]^\times = A^\times$.

Démonstration. L'égalité $\deg(fg) = \deg(f) + \deg(g)$ implique que $f, g \neq 0 \Rightarrow fg \neq 0$, ie que $A[X]$ est intègre. Enfin, si $fg = 1$ et puisque $\deg(1) = 0$, on doit avoir $\deg(f) = \deg(g) = 0$, donc $f, g \in A$ et finalement $f, g \in A^\times$. □

Exemple. – Parfois $A[X]^\times$ peut être strictement plus gros que $A^\times$. Soit $A = \mathbb{Z}/p^2\mathbb{Z}$. Alors le polynôme $1 + \overline{p}X$ est inversible dans $A[X]$, d'inverse $1 - \overline{p}X$. En effet, on a $(1 + \overline{p}X)(1 - \overline{p}X) = 1 - \overline{p}^2 X = 1$.

PROPOSITION. (Division euclidienne) – *Soit* $f \in A[X]$ *un polynôme* unitaire *(et donc non nul). Alors pour tout* $g \in A[X]$ *non nul, il existe un unique couple* $(q, r) \in A[X]^2$ *tel que* $\deg(r) < \deg(f)$ *et* $g = qf + r$

Démonstration. Existence. On procède par récurrence sur $\delta := \deg(g) - \deg(f)$. Notons que si $\delta < 0$, on peut prendre $q = 0$ et $r = g$. D'un autre côté, si $\delta \geqslant 0$, on peut considérer $g' := g - b_{\deg(g)}X^\delta f$, où $b_{\deg(g)}$ est le coefficient dominant de g. Alors clairement $\delta' = \deg(g') - \deg(f) < \delta$, et par récurrence il existe q', r' tels que $g' = q'f + r'$. On a donc $g = (q' + b_{\deg(g)}X^\delta)f + r'$ comme voulu.

Unicité. Si $qf + r = q'f + r'$, on a $(q - q')f = r' - r$. Supposons que $r' \neq r$. Alors on a $\deg(r' - r) < \deg(f)$ et $\deg(qf - qf') = \deg(q - q') + \deg(f)$ car f est unitaire, ce qui est impossible. On a donc $r = r'$, puis $qf = qf'$ et enfin $q = q'$ car f n'est pas diviseur de zero, étant unitaire. □

COROLLAIRE. – *Soit* $f \in A[X]$ *unitaire de degré* d. *Alors le quotient* $A[X]/(f)$ *est un* A*-module libre de base* $\{\overline{1}, \overline{X}, \cdots, \overline{X}^{d-1}\}$, *où* $\overline{X}$ *désigne l'image de* X *dans* $A/(f)$.

Démonstration. Soit $g \in A[X]$. Ecrivons $g = qf + r$ avec $\deg(r) < \deg(f)$. On a donc $r = \sum_{i=0}^{d-1} c_i X^i$ pour des c_i dans A. Alors l'image $\overline{g}$ de g dans $A[X]/(f)$ est donnée par $\overline{g} = \overline{r} = \sum_{i=0}^{d-1} c_i \overline{X}^i$, ce qui montre que la famille de l'énoncé est bien génératrice. Par ailleurs, supposons que $\sum_{i=1}^{d} c_i \overline{X}^i = 0$. Alors $r := \sum_{i=1}^{d} c_i X^i \in (f)$ et par l'unicité de la division euclidienne, on a $r = 0$, donc $c_i = 0$ pour tout i et la famille de l'énoncé est bien une base du A-module $A[X]/(f)$. □

Remarque. – Attention, $A[X]/(f)$ n'est bien-sûr pas libre en tant que $A[X]$-module, sauf si $f = 1$.

Théorème. (Thm de la base de Hilbert) – *Si A est noethérien, $A[X]$ est noethérien.*

Démonstration. Soit I un idéal de $A[X]$. On veut montrer qu'il est de type fini. Comme principe général, on peut remarquer que, par 1.3.7, il suffit de montrer que I/J est un idéal de type fini dans $A[X]/J$ où $J \subset I$ est un sous-idéal de type fini de notre choix.

En particulier, lorsque I contient un polynôme unitaire f, on peut prendre $J = (f)$. Le corollaire précédent nous dit que $A[X]/J$ est un A-module de type fini, donc noethérien, et I/J est donc de type fini sur A et a fortiori sur $A[X]$.

Néanmoins, I peut ne contenir aucun polynôme unitaire. Dans ce cas, considérons l'ensemble $K \subset A$ de tous les coefficients dominants de polynômes $f \in I$. Il s'agit clairement d'un idéal de A (le vérifier), et donc il est engendré sur A (qui est noethérien) par des éléments $a_1, \cdots, a_r$. Choisissons pour chaque $i = 1, \cdots, r$ un polynôme $f_i \in I$ dont le coefficient dominant est a_i, et notons $J \subset I$ l'idéal de $A[X]$ engendré par $f_1, \cdots, f_r$. Nous allons montrer que l'image I/J de I dans $A[X]/J$ est un A-module de type fini, ce qui suffit à conclure d'après le premier paragraphe.

Pour cela, soit $d = \max\{\deg(f_1), \cdots, \deg(f_r)\}$. Il suffit de montrer que

(*) *Tout polynôme $f \in I$ est congru modulo J a un polynôme de degré $< d$.*

En effet, si on admet (*), on voit que I/J est l'image de $I \cap (A + AX + \cdots + AX^{d-1})$ qui est un sous-A-module de $(A + AX + \cdots + AX^{d-1})$ donc est de type fini sur A noethérien. Donc I/J est lui même de type fini.

Montrons donc (*), par récurrence sur $\deg(f)$. La propriété étant tautologique si $\deg(f) < d$, supposons $\deg(f) \geqslant d$ et notons $\delta_i := \deg(f) - \deg(f_i) > 0$ pour $i = 1, \cdots, r$. Alors le coefficient dominant de f est de la forme $a_{\deg(f)} = c_1 a_1 + \cdots + c_r a_r$ pour $c_1, \cdots, c_r \in A$. Il s'ensuit que si on pose $f' := f - \sum_{i=1}^{r} c_i X^{\delta_i} f_i$ alors $f' \equiv f \pmod J$ et $\deg(f') < \deg(f)$. On applique l'hypothèse de récurrence à f' pour conclure. □

1.4.4 *Polynômes à plusieurs variables.* On s'intéresse ici à l'algèbre du monoïde $\mathcal{N} = \mathbb{N}^n$. Un élément $\nu \in \mathbb{N}^n$ est donc un n-uplet $(\nu_1, \cdots, \nu_n)$ d'entiers positifs et la somme est définie terme à terme par $\nu + \nu' = (\nu_1 + \nu_1', \cdots, \nu_n + n_n')$. Posons alors, dans $A[\mathbb{N}^n]$,

$$X_i := e_{(0,\cdots,1,\cdots,0)}, \text{ où le 1 est en } i\text{-ème position.}$$

On a donc, pour tout $\nu = (\nu_1, \cdots, \nu_n)$ l'égalité

$$e_\nu = X_1^{\nu_1} X_2^{\nu_2} \cdots X_n^{\nu_n}.$$

Ainsi la famille $(X_1^{\nu_1} \cdots X_n^{\nu_n})_{(\nu_1,\cdots,\nu_n)\in\mathbb{N}^n}$ est la base canonique de $A[\mathbb{N}^n]$, autrement dit tout élément f de $A[\mathbb{N}^n]$ s'écrit de manière unique sous la forme

$$f = \sum_{(\nu_1,\cdots,\nu_n)} a_{\nu_1,\cdots,\nu_n} X_1^{\nu_1} \cdots X_n^{\nu_n}.$$

Pour simplifier les notations, il est d'usage de noter $X^\nu := X_1^{\nu_1} \cdots X_n^{\nu_n}$, et donc $f = \sum_{\nu\in\mathbb{N}^n} a_\nu X^\nu$. La multiplication est alors donnée par

$$\left(\sum_{\nu\in\mathbb{N}^n} a_\nu X^\nu\right) \cdot \left(\sum_{\nu\in\mathbb{N}^n} b_\nu X^\nu\right) = \sum_\nu \left(\sum_{\mu+\rho=\nu} a_\mu b_\rho\right) X^\nu$$

Définition. – *L'algèbre $A[\mathbb{N}^n]$ se note aussi $A[X_1, \cdots, X_n]$ et s'appelle aussi "algèbre des polynômes en les n indéterminées $X_1, \cdots, X_n$". Ses éléments sont appelés* polynômes en les X_i *et les élements $X^\nu = X_1^{\nu_1} X_2^{\nu_2} \cdots X_n^{\nu_n}$ sont les* monômes.

Ainsi les monômes forment une base de $A[X_1, \cdots, X_n]$ et tout polynôme est combinaison A-linéaire de monômes. Le *degré total* du monôme X^ν est par définition l'entier $|\nu| = \nu_1 + \cdots + \nu_n$. Le *degré total* d'un polynôme $f = \sum_\nu a_\nu X^\nu$ est le plus grand des degrés des monômes X^ν tels que $a_\nu \neq 0$.

La propriété universelle satisfaite par $A[\mathbb{N}^n]$ s'exprime plus aisément en termes des X_i :

Proposition. – *Pour toute A-algèbre B munie d'éléments $b_1, \cdots, b_n$, il existe un unique morphisme de A-algèbres $\varphi : A[X_1, \cdots, X_n] \longrightarrow B$ tel que $\varphi(X_i) = b_i$ pour tout i. En d'autres termes, pour toute A-algèbre B, l'application $\varphi \mapsto (\varphi(X_1), \cdots, \varphi(X_n))$ est une bijection*

$$\mathrm{Hom}_{A-\mathrm{alg}}(A[X_1, \cdots, X_n], B) \xrightarrow{\sim} B^n.$$

Sa bijection réciproque associe à un élement $(b_1, \cdots, b_n) \in B^n$ le morphisme d'"évaluation en $(b_1, \cdots, b_n)$", i.e. le morphisme $A[X_1, \cdots, X_n] \longrightarrow B$ qui envoie $f = \sum_\nu a_\nu X^\nu$ sur $f(b_1, \cdots, b_n) := \sum_\nu a_\nu b_1^{\nu_1} \cdots b_n^{\nu_n}$.

Démonstration. On peut le montrer directement. Mais il est plus naturel de le déduire de la propriété universelle de $A[\mathbb{N}^n]$ en remarquant que se donner n éléments $b_1, \cdots, b_n$ est équivalent à se donner un morphisme de monoïdes $(\mathbb{N}^n, +, 0) \longrightarrow (B, \cdot, 1)$, $\nu \mapsto b_\nu$ via la relation $b_\nu = b_1^{\nu_1} b_2^{\nu_2} \cdots b_n^{\nu_n}$. □

On peut paraphraser la proposition en disant informellement que *se donner un morphisme $A[X_1, \cdots, X_n] \longrightarrow B$ revient à se donner les images $b_1, \cdots, b_n$ des X_i.*

Corollaire. – *Soient $f_1, \cdots, f_r$ des polynômes dans $A[X_1, \cdots, X_n]$. L'application de la proposition précédente induit par restriction une bijection*

$$\mathrm{Hom}_{A-\mathrm{alg}}(A[X_1, \cdots, X_n]/(f_1, \cdots, f_r), B) \xrightarrow{\sim} \{(b_1, \cdots, b_n) \in B^n,\ f_i(b_1, \cdots, b_n) = 0, \forall i\}.$$

Démonstration. Par la propriété universelle des quotients, le terme de gauche s'identifie au sous-ensemble $\{\varphi \in \mathrm{Hom}_{A-\mathrm{alg}}(A[X_1,\cdots,X_n],B),\ \varphi(f_1)=\cdots=\varphi(f_r)=0\}$ de l'ensemble de gauche dans la proposition précédente. Comme on a dans B l'égalité $\varphi(f_i) = f_i(\varphi(X_1),\cdots,\varphi(X_n))$, ce sous-ensemble est bien envoyé sur le terme de droite par la bijection de la proposition. □

On peut à nouveau paraphraser ceci en : se donner un morphisme de A-algèbres $A[X_1,\cdots,X_n]/(f_1,\cdots,f_r) \longrightarrow B$ équivaut à se donner un n-uplet $(b_1,\cdots,b_n)\in B^n$ tel que $f_1(b_1,\cdots,b_n)=\cdots=f_r(b_1,\cdots,b_n)=0$.

On aurait pu aussi construire inductivement les polynômes en plusieurs variables en considérant $A[X_1,\cdots,X_{n-1}][X_n]$. C'est aussi une A-algèbre munie d'un n-uplet d'éléments $X_1,\cdots,X_n$. Comme on peut s'y attendre on obtient le même objet.

COROLLAIRE. – *Il y a un unique isomorphisme de A-algèbres $A[X_1,\cdots,X_n] \xrightarrow{\sim} A[X_1,\cdots,X_{n-1}][X_n]$ tel que $X_i\mapsto X_i$.*

Démonstration. Il suffit de montrer que la A-algèbre $A[X_1,\cdots,X_{n-1}][X_n]$ satisfait la même propriété universelle que $A[X_1,\cdots,X_n]$. Soit donc B une A-algèbre munie de n éléments $b_1,\cdots,b_n$. La propriété universelle de $A[X_1,\cdots,X_{n-1}]$ nous fournit un morphisme de A-algèbres $A[X_1,\cdots,X_{n-1}]$ dans B qui envoie X_i sur b_i pour $i=1,\cdots,n-1$. Cela fait de B une $A[X_1,\cdots,X_{n-1}]$-algèbre. Ensuite, la propriété universelle des polynômes en une indéterminée nous fournit un morphisme de $A[X_1,\cdots,X_{n-1}]$-algèbres

$$\varphi:\ A[X_1,\cdots,X_{n-1}][X_n]\longrightarrow B$$

qui envoie X_n sur b_n. Ainsi, φ est aussi un morphisme de A-algèbres qui envoie X_i sur b_i pour tout i. Montrons qu'un tel morphisme est unique. Si φ' est un autre tel morphisme, on a $\varphi_{|A[X_1,\cdots,X_{n-1}]}=\varphi'_{|A[X_1,\cdots,X_{n-1}]}$ par pté universelle de $A[X_1,\cdots,X_{n-1}]$, puis $\varphi=\varphi'$ par pté universelle des polynômes en une variable. □

COROLLAIRE. – *Si A est intègre, resp. noethérien, alors $A[X_1,\cdots,X_n]$ est intègre, resp. noethérien.*

Démonstration. Grâce au corollaire précédent on est ramené par récurrence au cas d'1 indéterminée que nous avons déjà traité. □

Remarque. – Dans $\mathbb{C}[X,Y]$, l'idéal $(X,Y)^n$ est engendré par les monômes X^kY^{n-k}, $k=0,\cdots,n$. Par un argument de degré, on voit que tout système de générateurs de cet idéal devra contenir une base de l'espace des polynômes homogènes de degré n, et donc $n+1$ est le cardinal minimal d'un tel système. Ceci montre que dans un anneau noethérien, le nombre d'éléments nécessaires pour engendrer un idéal peut être arbitrairement grand.

Application. – Soit $\mathcal{F}(\mathbb{C}^n)$ la $\mathbb{C}$-algèbre de toutes les fonctions $\mathbb{C}^n\longrightarrow\mathbb{C}$. Parmi ces fonctions il y a les fonctions coordonnées $z_1,\cdots,z_n$. On définit la $\mathbb{C}$-algèbre $\mathcal{O}(\mathbb{C}^n)$ des fonctions polynomiales sur $\mathbb{C}^n$ comme l'image du morphisme de $\mathbb{C}$-algèbres $\mathbb{C}[X_1,\cdots,X_n]\longrightarrow \mathcal{F}(\mathbb{C}^n)$ qui envoie X_i sur z_i. En d'autres termes, une fonction est polynomiale si elle est de la forme $(z_1, \cdots, z_n) \mapsto f(z_1, \cdots, z_n)$ pour un polynôme $f \in \mathbb{C}[X_1, \cdots, X_n]$. Notons que ce polynôme est *uniquement déterminé* par la fonction (exercice). En d'autres termes, le morphisme $\mathbb{C}[X_1, \cdots, X_n] \longrightarrow \mathcal{F}(\mathbb{C}^n)$ est injectif et on peut identifier $\mathbb{C}[X_1, \cdots, X_n] = \mathcal{O}(\mathbb{C}^n)$. Notons que la propriété universelle fournit une bijection

$$\mathbb{C}^n \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}-\mathrm{alg}}(\mathcal{O}(\mathbb{C}^n), \mathbb{C}), \; z \mapsto (f \mapsto f(z))$$

qui permet de voir tout point de l'"espace" $\mathbb{C}^n$ comme un morphisme d'évaluation sur l'algèbre des fonctions sur cet espace.

Plus généralement, soit $V \subset \mathbb{C}^n$ un sous-ensemble algébrique de $\mathbb{C}^n$ et $\mathcal{F}(V)$ la $\mathbb{C}$-algèbre de toutes les fonctions $V \longrightarrow \mathbb{C}$. Une telle fonction est dite polynomiale si c'est la restriction d'une fonction polynomiale sur $\mathbb{C}^n$. L'application de restriction des fonctions fournit donc un morphisme surjectif

$$\mathcal{O}(\mathbb{C}^n) = \mathbb{C}[X_1, \cdots, X_n] \twoheadrightarrow \mathcal{O}(V).$$

Soit I son noyau, i.e. l'idéal des fonctions $f \in \mathcal{O}(\mathbb{C}^n)$ qui s'annulent sur V. D'après le dernier corollaire, I est de type fini, engendré par des polynômes $f_1, \cdots, f_r \in \mathbb{C}[X_1, \cdots, X_n]$. On a donc

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

[En effet, l'inclusion $V \subset V(I)$ est claire, et puisque V est algébrique donc de la forme $V(f'_1, \cdots, f'_{r'})$ pour d'autres polynômes f'_i, on a $f'_i \in I$ pour tout i, et donc $V(I) \subset V(f'_1, \cdots, f'_{r'}) = V$.] On s'aperçoit donc que la propriété universelle pour le quotient $\mathbb{C}[X_1, \cdots, X_n]/I = \mathcal{O}(V)$ fournit la bijection

$$V \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}-\mathrm{alg}}(\mathcal{O}(V), \mathbb{C}), \; z \in (f \mapsto f(z))$$

et que, à nouveau, les points de l'espace V s'interprètent comme des morphismes d'évaluation sur sa $\mathbb{C}$-algèbre de fonctions polynomiales.

Rappelons maintenant que nous avons défini une *application polynômiale* de $V \subset \mathbb{C}^n$ vers $V' \subset \mathbb{C}^{n'}$ comme une application obtenue par restriction d'une application polynômiale $\mathbb{C}^n \longrightarrow \mathbb{C}^{n'}$ à V. Si $h : V \longrightarrow V'$ est une telle application, elle induit dualement un morphisme de $\mathbb{C}$-algèbres $\mathcal{O}(V') \longrightarrow \mathcal{O}(V)$, $f' \mapsto h \circ f'$. Réciproquement tout morphisme $\varphi : \mathcal{O}(V') \longrightarrow \mathcal{O}(V)$ induit une application $\varphi^* : V = \mathrm{Hom}_{\mathbb{C}-\mathrm{alg}}(\mathcal{O}(V), \mathbb{C}) \longrightarrow \mathrm{Hom}_{\mathbb{C}-\mathrm{alg}}(\mathcal{O}(V), \mathbb{C}) = V'$. Ces deux procédés fournissent des bijections réciproques

$$\mathrm{App.Pol}(V, V') \longleftrightarrow \mathrm{Hom}_{\mathbb{C}-\mathrm{alg}}(\mathcal{O}(V'), \mathcal{O}(V))$$

qui montrent que la bonne manière "intrinsèque" de caractériser un ensemble algébrique (sans référence à un espace ambiant et un système d'équations) est d'utiliser son algèbre de fonctions polynômiales. Celle-ci est une $\mathbb{C}$-algèbre réduite de type fini (et donc noethérienne).

Réciproquement, toute $\mathbb{C}$-algèbre réduite de type fini A est l'algèbre des fonctions d'un sous-ensemble algébrique : choisi un morphisme surjectif $\mathbb{C}[X_1, \cdots, X_n] \longrightarrow A$, des générateurs $(f_1, \cdots, f_r)$ de son noyau et considérer $V(f_1, \cdots, f_r)$.

1.4.5 *Polynômes de Laurent.* On s'intéresse ici à l'algèbre du monoïde $\mathbb{Z}$ (qui est donc un groupe !). La A-algèbre $A[\mathbb{Z}]$ possède donc une base $(e_n)_{n\in\mathbb{Z}}$ telle que $e_n e_m = e_{n+m}$ pour tout $n, m \in \mathbb{Z}$. Notons alors $X := e_1$. On a $e_n = X^n$ pour tout $n \in \mathbb{Z}$, et tout élément de $A[\mathbb{Z}]$ s'écrit de manière unique $f = \sum_{n\in\mathbb{Z}} a_n X^n$.

DÉFINITION. – *L'algèbre $A[\mathbb{Z}]$ est appelée "algèbre des polynômes de Laurent". On la note généralement $A[X, X^{-1}]$, ou parfois aussi $A[X^{\pm 1}]$.*

La propriété universelle de $A[X, X^{-1}]$ s'exprime ainsi :

PROPOSITION. – *Pour toute A-algèbre B munie d'un élément* inversible *b, il existe un unique morphisme de A-algèbres $\varphi : A[X, X^{-1}] \longrightarrow B$ tel que $\varphi(X) = b$. En d'autres termes, pour toute A-algèbre B, l'application $\varphi \mapsto \varphi(X)$ induit une bijection*

$$\mathrm{Hom}_{A-\mathrm{alg}}(A[X, X^{-1}], B) \xrightarrow{\sim} B^\times.$$

On peut paraphraser en disant que *se donner un morphisme $A[X, X^{-1}] \longrightarrow B$ revient à se donner un élément inversible de B, à savoir l'image de X.*

PROPOSITION. – *Si A est intègre, resp. noethérien, alors $A[X, X^{-1}]$ est intègre, resp. noethérien.*

Démonstration. Supposons A intègre. L'anneau des polynômes "ordinaires" $A[X]$ est contenu dans $A[X, X^{-1}]$ et on sait qu'il est intègre. Soient alors $f, g \in A[X, X^{-1}]$ tels que $fg = 0$. Il existe un entier $n \in \mathbb{N}$ tel que $fX^n \in A[X]$ et $gX^n \in A[X]$. Alors l'égalité $(fX^n)(gX^n) = 0$ qui a lieu dans $A[X]$ implique que $fX^n = 0$ ou $gX^n = 0$. Puisque X est inversible dans $A[X, X^{-1}]$ on a $f = 0$ ou $g = 0$. Il s'ensuit que $A[X, X^{-1}]$ est intègre.

Supposons maintenant A noethérien. Nous allons présenter $A[X, X^{-1}]$ comme un quotient d'un anneau que l'on sait être noethérien. Pour cela considérons l'unique morphisme $A[X, Y] \longrightarrow A[X, X^{-1}]$ qui envoie X sur X et Y sur X^{-1} (donné par la pté universelle). Il envoie aussi X^n sur X^n et Y^n sur X^{-n} et on voit ainsi qu'il est surjectif, puisque son image contient une base de $A[X, X^{-1}]$. On a vu que $A[X, Y]$ est noethérien, on en déduit que $A[X, X^{-1}]$ l'est aussi. □

Exercice. – Montrer que le noyau du morphisme $A[X, Y] \longrightarrow A[X, X^{-1}]$ qui envoie X sur X et Y sur X^{-1} est l'idéal engendré par $XY - 1$, de sorte que

$$A[X, X^{-1}] = A[X, Y]/(XY - 1).$$

1.4.6 *Polynômes de Laurent à n indéterminées.* C'est l'exemple $\mathcal{N} = \mathbb{Z}^n$. L'algèbre $A[\mathbb{Z}^n]$ contient la sous-algèbre $A[\mathbb{N}^n]$ donc les éléments $X_1, \cdots, X_n$ définis précédemment. On voit alors que les monômes de Laurent $X_1^{\nu_1} \cdots X_n^{\nu_n}$ pour $\nu = (\nu_1, \cdots, \nu_n) \in \mathbb{Z}^n$ forment une A-base de $A[\mathbb{Z}^n]$. On note aussi cet anneau $A[X_1^{\pm 1}, \cdots, X_n^{\pm 1}]$. Se donner un morphisme $A[X_1^{\pm 1}, \cdots, X_n^{\pm 1}] \longrightarrow B$ équivaut à se donner un n-uplet $(b_1, \cdots, b_n)$ d'élements *inversibles* de B. Ceci nous permet de voir, comme dans le cas des polynômes ordinaires, que $A[X_1^{\pm 1}, \cdots, X_n^{\pm 1}] \simeq A[X_1^{\pm 1}, \cdots, X_{n-1}^{\pm 1}][X_n^{\pm 1}]$. Par récurrence on en déduit que si A est intègre, resp. noethérien, alors $A[X_1^{\pm 1}, \cdots, X_n^{\pm 1}]$ l'est aussi.

Remarque. – Il n'est pas vrai en général que A intègre implique $A[\mathcal{N}]$ intègre. Par exemple pour $\mathcal{N} = \mathbb{Z}/2\mathbb{Z}$, on a $A[\mathbb{Z}/2\mathbb{Z}] \simeq A[X]/(X^2-1)$ (exercice) dans lequel $(X-1)(X+1) = 0$ mais $X-1$ et $X+1$ sont non nuls. Quant à la propriété "A noethérien implique $A[\mathcal{N}]$ noethérien", l'exemple des polynômes à une infinité de variables $A[\mathbb{N}^{\mathbb{N}}] = A[X_1, X_2, \cdots]$ montre qu'elle n'est pas toujours vraie. Elle est néanmoins vraie si le monoïde $\mathcal{N}$ est engendré par un nombre fini d'éléments (exercice).

1.5 Anneaux factoriels, principaux, euclidiens

Dans cette section, tous les anneaux considérés seront intègres (et commutatifs), sauf mention du contraire.

1.5.1 *Généralités sur les anneaux factoriels.* Soit A un anneau intègre. Rappelons quelques définitions et propriétés déjà rencontrées :
- un élément $p \in A$ non nul et non inversible est dit *irréductible* si pour tous $a, b \in A$, $(p = ab) \Rightarrow (a \in A^\times$ ou $b \in A^\times)$.
- deux éléments irréductibles $p, p' \in A$ sont dits *équivalents* (ou "associés") s'il existe un inversible $u \in A^\times$ tel que $p' = up$, ce qui équivaut à l'égalité d'idéaux $(p) = (p')$ (on utilise l'intégrité de A ici).
- un élément $x \in A$ non nul et non inversible est irréductible si et seulement si l'idéal (x) est maximal parmi les idéaux principaux propres.
- si l'idéal (x) est premier, alors x est irréductible.

Ceci étant, rappelons la définition suivante.

DÉFINITION. – *L'anneau intègre A est dit* factoriel *(en anglais :* Unique Factorisation Domain *ou UFD) lorsqu'il satisfait les deux propriétés suivantes :*

(Ex) : tout élément $x \in A$ non nul et non inversible est produit $x = p_1 \cdots p_r$ d'éléments irréductibles.

(Un) : deux factorisations $x = p_1 \cdots p_r = p'_1 \cdots p'_{r'}$ comme dans (Ex) sont équivalentes *au sens où $r = r'$ et il existe une permutation σ de $\{1, \cdots, r\}$ telle que p_i et $p'_{\sigma(i)}$ soient équivalents (ie $(p_i) = (p'_{\sigma(i)})$).*

On a vu que les anneaux noethériens satisfont (Ex), mais il y a aussi des anneaux non noethériens qui satisfont (Ex), par exemple $\mathbb{C}[\mathbb{N}^{\mathbb{N}}] = \mathbb{C}[X_1, \cdots, X_n, \cdots]$. On a aussi rencontré des anneaux noethériens, comme $\mathbb{Z}[\sqrt{-5}]$, qui ne satisfont pas (Un). Voici un autre exemple dans lequel, même la longueur d'une décomposition en produit d'irréductibles n'est pas unique : dans $\mathbb{Z}[\sqrt{-23}]$, les nombres 3 et $(2 \pm \sqrt{-23})$ sont irréductibles et on a pourtant l'égalité $(2 + \sqrt{-23})(2 - \sqrt{-23}) = 3^3$.

Remarque. (Pathologies dans un anneau non intègre) – Considérons $A = \mathbb{C}[X, Y]/(XY)$. L'élement $\bar{X}$ engendre un idéal premier (car le quotient $\mathbb{C}[X, Y]/(XY, X) = \mathbb{C}[Y]$ est intègre) et pourtant l'égalité $\bar{X}(1 + \bar{Y}) = \bar{X}$ montre que $\bar{X}$ n'est pas un élément irréductible ! (noter que $1 + \bar{Y}$ n'est pas inversible puisque $(XY, 1 + Y) = (X, Y + 1)$ est un idéal propre dans $\mathbb{C}[X, Y]$). Pire : bien que A soit noethérien, $\bar{X}$ n'est pas produit d'irréductibles. En effet si $\bar{X} = p_1 \cdots p_r$ et si on écrit chaque p_i sous la forme $p_i = \bar{X} f_i(\bar{X}) + g_i(\bar{Y})$, alors on constate que l'un des g_i doit être nul. Mais alors l'égalité $(1 + \bar{Y})p_i = p_i$ montre à nouveau que p_i n'est pas irréductible.

Lemme. – *Soit A un anneau intègre satisfaisant (Ex). Alors les assertions suivantes sont équivalentes :*

i) A satisfait (Un)

ii) A satisfait le lemme d'Euclide *: (p irréductible et $p|ab$) $\Rightarrow$ ($p|a$ ou $p|b$).*

iii) A satisfait le lemme de Gauss *: ($a|bc$ et a, b sont sans facteur commun) $\Rightarrow$ $a|c$.*

iv) pour tout élément irréducible p, l'idéal (p) est premier.

Démonstration. *iii)* $\Rightarrow$ *ii)* est tautologique puisque le lemme d'Euclide est un cas particulier du lemme de Gauss.

Montrons *ii)* $\Rightarrow$ *i)*. Plus précisément, montrons par récurrence sur r qu'une égalité de produits d'irréductibles $p_1 \cdots p_r = p'_1 \cdots p'_{r'}$ implique $r = r'$ et l'existence d'une permutation σ de $\{1, \cdots, r\}$ telle que $(p_i) = (p'_{\sigma(i)})$. Traitons d'abord le cas $r = 1$. Dans ce cas, le lemme d'Euclide nous dit que p_1 divise l'un des p'_i, disons p'_1 quitte à permuter. Mais alors, si $r' > 1$ on a $p'_2 \cdots p'_{r'} \in A^\times$, ce qui est absurde. Donc $r' = 1$. Supposons maintenant $r > 1$. Comme précédemment, p_r divise l'un des p'_i et on peut supposer qu'il divise $p'_{r'}$ quitte à permuter. On a donc $p'_r = u.p_r$ pour un inversible $u \in A^\times$ et on se retrouve avec une égalité $p_1 \cdots p_{r-1} = p'_1 \cdots p'_{r'-2}(p'_{r'-1}u)$ justiciable de l'hypothèse de récurrence. Celle-ci affirme donc $r = r'$ et fournit une permutation σ' d'où l'on déduit la permutation cherchée σ en tenant compte de la première permutation effectuée pour avoir $p_r | p'_{r'}$.

Montrons *i)* $\Rightarrow$ *iii)*. Choisissons une factorisation $b = p_1 \cdots p_s$, puis une factorisation $c = p_{s+1} \cdots p_r$. Alors la propriété (Un) implique qu'il existe un sous-ensemble $I \subset \{1, \cdots, r\}$ et une unité $u \in A^\times$ tels que $a = u \prod_{i \in I} p_i$. Puisque a et b sont sans facteur commun, on a $I \cap \{1, \cdots, s\} = \emptyset$, et donc $I \subset \{s+1, \cdots, r\}$, et finalement $a|c$.

Enfin, *ii)* et *iv)* sont tautologiquement équivalents. En effet, dire que (p) est premier signifie $ab \in (p) \Rightarrow (a \in (p)$ ou $b \in (p))$. Or, pour tout $x \in A$ on a $x \in (p) \Leftrightarrow p|x$. □

1.5.2 *Valuations.*

Lemme. – *Soit A un anneau intègre noethérien et p un élément irréductible.*

i) Pour tout élément non nul $a \in A$ l'ensemble E des $n \in \mathbb{N}$ tel que $p^n | a$ est fini.

ii) Le plus grand élément $\nu_p(a)$ de E est l'unique entier n pour lequel on peut écrire $a = p^n a'$ avec a' non divisible par p.

iii) On a : (p) premier $\Leftrightarrow \forall a, b \in A \setminus \{0\}$, $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

Démonstration. i) Supposons que l'ensemble considéré E ne soit pas borné, c'est à dire que $\forall n \in \mathbb{N}$ on a $p^n | a$. Ecrivons alors $a = p^n a_n$ et remarquons que puisque A est intègre, on a pour $m > n$, $p^m a_m = p^n a_n$ donc $p^{m-n} a_m = a_n$ et a_m divise a_n. Comme a_n ne divise pas a_m, il s'ensuit que la suite d'idéaux (a_n), $n \in \mathbb{N}$ est strictement croissante, contredisant la noethériannité de A.

ii) Puisque $p^{\nu_p(a)}|a$ on peut factoriser $a = p^{\nu_p(a)}a'$ et, par maximalité de $\nu_p(a)$, p ne divise pas a'. Supposons qu'on ait une autre factorisation $a = p^n a''$ avec a'' non divisible par p. Alors par définition $n \leqslant \nu_p(a)$. Comme A est intègre on obtient $p^{\nu_p(a)-n}a' = a''$ et donc $\nu_p(a) - n = 0$, ainsi que $a' = a''$.

iii) Supposons (p) premier, et fixons $a, b \neq 0$. Ecrivons $a = p^{\nu_p(a)}a'$ et $b = p^{\nu_p(b)}b'$. On a donc $ab = p^{\nu_p(a)+\nu_p(b)}a'b'$. Mais puisque p ne divise ni a' ni b', i.e. $a', b' \notin (p)$, on a $a'b' \notin (p)$ (puisque (p) est premier), et donc p ne divise pas $a'b'$. Le ii) implique alors l'égalité voulue $\nu_p(a) + \nu_p(b) = \nu_p(ab)$.

Réciproquement, supposons cette égalité vraie pour tous a, b non nuls. Alors $ab \in (p) \Leftrightarrow p|ab \Rightarrow \nu_p(ab) > 0 \Rightarrow (\nu_p(a) > 0$ ou $\nu_p(b) > 0) \Rightarrow (p|a$ ou $p|b) \Leftrightarrow (a \in (p)$ ou $b \in (p))$. Donc (p) est premier.

□

Définition. – *Sous les hypothèses du lemme, on appelle* valuation p-adique *de a et on note $\nu_p(a)$ le plus grand entier naturel n tel que $p^n|a$.*

Si a est inversible, on a donc $\nu_p(a) = 0$ pour tout p. Il est d'usage de prolonger cette définition en posant $\nu_p(0) = \infty$.

Remarque. – On trouve aussi la notation $\mathrm{ord}_p(a)$, pour "ordre de a en p". Celle-ci vient de l'interprétation géométrique suivante : dans $\mathbb{C}[X]$ vu comme espace des fonctions polynomiales sur $\mathbb{C}$, et pour tout $z \in \mathbb{C}$, le polynôme $X - z$ est évidemment irréductible et l'entier $\nu_{X-z}(f) = \mathrm{ord}_{X-z}(f)$ est l'ordre d'annulation de la fonction f en z.

Proposition. – *Soit A un anneau factoriel.*

i) Soit p un élément irréductible. On a : $\forall a, b \in A$, $\nu_p(ab) = \nu_p(a) + \nu_p(b)$

ii) Soient $a, b \in A$. On a : $(a|b) \Leftrightarrow (\forall p \in A$ irréductible, $\nu_p(a) \leqslant \nu_p(b))$.

iii) Soit p un élément irréductible et $a \in A$ de factorisation $a = p_1 \cdots p_r$. Alors $\nu_p(a)$ est le nombre de facteurs p_i équivalents à p.

iv) Soit P un ensemble de représentants des classes d'équivalence d'éléments irréductibles de A. Pour tout $a \in A$ non nul, l'ensemble $\{p \in P, \nu_p(a) \neq 0\}$ est fini et il existe $u \in A^\times$ tel que $a = u\prod_{p\in P} p^{\nu_p(a)}$.

Démonstration. i)Lorsque $ab \neq 0$, cela vient du iii) du lemme précédent. Lorsque $ab = 0$, l'égalité reste vraie avec la convention que $\infty + \infty = \infty$

ii) L'implication $\Rightarrow$ découle de i). Pour l'implication $\Leftarrow$ on procède par récurrence sur le nombre $r(a)$ de facteurs irréductibles de a. Si $r(a) = 0$ alors a est inversible et on a bien $a|b$. Si $r(a) > 0$ choisissons un diviseur irréductible q de a. On a $\nu_q(b) \geqslant \nu_q(a) > 0$ donc q divise aussi b. Posons $a = qa'$ et $b = qb'$. On a $\nu_q(b') = \nu_q(b) - 1 \geqslant \nu_q(a) - 1 = \nu_q(a')$ et pour tout $p \neq q$ on a $\nu_p(b') = \nu_p(b) \geqslant \nu_p(a) = \nu_p(a')$. Comme $r(a') < r(a)$, on peut donc appliquer HR à a', b', ce qui nous donne $a'|b'$, puis $a|b$.

iii) On utilise i) pour avoir $\nu_p(a) = \sum_{i=1}^r \nu_p(p_i)$. Or on a

$$\nu_p(p_i) = \begin{cases} 1 & \text{si } p \text{ est équivalent à } p_i \\ 0 & \text{sinon.} \end{cases}$$

iv) Factorisons $a = p_1 \cdots p_r$. D'après iii) on a $\nu_p(a) \neq 0$ si et seulement si p est équivalent à l'un des p_i d'où la finitude [17] de $\{p \in P, \nu_p(a) \neq 0\}$ et donc celle du produit $\prod_{p\in P} p^{\nu_p(a)}$. De plus, toujours le point iii) nous dit que $\nu_p(a)$ est le cardinal de l'ensemble $I_p := \{i \in \{1, \cdots, r\}, p_i \in A^\times p\}$. On a donc $\prod_{i\in I_p} p_i \in A^\times p^{\nu_p(a)}$. Comme les I_p non vides forment une partition de $\{1, \cdots, r\}$, on en déduit que $a \in A^\times \prod_{p\in P} p^{\nu_p(a)}$ comme voulu. □

Remarque. – Dans un anneau intègre noethérien *non factoriel*, toutes ces propriétés peuvent être mises en défaut. Prenons l'exemple de $\mathbb{Z}[\sqrt{-5}]$ et de la factorisation $2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. On peut montrer (exercice ou voir TD) que $2, 3, 1+\sqrt{-5}$ et $1-\sqrt{-5}$ sont des éléments irréductibles 2 à 2 non équivalents. Il s'ensuit que :

— en prenant $p = 2$, $a = 1+\sqrt{-5}$ et $b = 1-\sqrt{-5}$ on a un contre-exemple à la pté i).
— en prenant $a = 2(1+\sqrt{-5})$ et $b = 6$ on a un contre-exemple à l'implication $\Leftarrow$ de ii).
— En prenant $p = 2$, $a = 6$ et la factorisation $6 = (1+\sqrt{-5})(1-\sqrt{-5})$ on obtient un contre-exemple à iii)
— En prenant $a = 6$, le produit $\prod_{p\in P} p^{\nu_p(a)}$ est divisible par $2 \times 3 \times (1+\sqrt{-5})(1-\sqrt{-5}) = 36$ donc pas de la forme annoncée dans le iv).

Nous donnons maintenant une sorte de réciproque à la proposition ci-dessus. On appelle *valuation* d'un corps K toute application $v : K \setminus \{0\} \longrightarrow \mathbb{Z}$ telle que $v(xy) = v(x) + v(y)$ et $v(x+y) \geqslant \mathrm{Min}(v(x), v(y))$ pour tous $x, y \in K$. Ces axiomes assurent que l'ensemble $A_v := \{x \in K,\ v(x) \geqslant 0\} \cup \{0\}$ est un sous-anneau de K.

Proposition. – *Soit K un corps et V un ensemble de valuations de K tel que :*

i) $\forall x \in K, \{v \in V, v(x) \neq 0\}$ est fini.

ii) $\forall v \in V, \exists p_v \in K$ tel que $v(p_v) = 1$ et $(w \neq v \Rightarrow w(p_v) = 0)$.

Alors l'anneau $A := \bigcap_{v\in V} A_v = \{x \in K, \forall v \in V, v(x) \geqslant 0\} \cup \{0\}$ est factoriel et les p_v sont un système de représentants de ses classes d'irréductibles.

Démonstration. Après avoir remarqué que $A^\times = \{x \in K^\times, \forall v \in V, v(x) = 0\}$, montrons que les p_v sont irréductibles. En effet, si $p_v = ab$ et $a \notin A^\times$ alors $w(a) = w(b) = 0$ pour tout $w \neq v$, et $v(a) + v(b) = 1$ avec $v(a) \neq 0$, donc $v(b) = 0$ et $b \in A^\times$. Par ailleurs, si a est non nul et non inversible, il existe v tel que $v(a) > 0$, donc $p_v^{-1}a \in A$ et par conséquent $p_v | a$. Il s'ensuit que tout irréductible est associé à un p_v. L'hypothèse i) nous assure maintenant que pour $a \in A \setminus \{0\}$ le produit $\prod_{v\in V} p_v^{v(a)}$ est bien défini. Comme $a \prod_{v\in V} p_v^{-v(a)} \in A^\times$, on en déduit que A vérifie la propriété (Ex). Il nous reste à montrer que A vérifie la propriété (Un), et pour cela nous montrons que p_v satisfait le lemme d'Euclide. On a $p_v | ab \Leftrightarrow v(ab) > 0 \Rightarrow (v(a) > 0 \text{ ou } v(b) > 0) \Leftrightarrow (p_v | a \text{ ou } p_v | b)$.

□

17. on verra plus loin un exemple pas si exotique d'anneau noethérien où cette finitude n'est pas vérifiée

1.5.3 *Pgcd et ppcm dans un anneau factoriel.*

PROPOSITION. – *Soit A un anneau factoriel et $a_1, \cdots, a_n \in A$.*

i) L'idéal $I := (a_1) \cap \cdots \cap (a_n)$ est principal. Pour un élément $m \in A$, les assertions suivantes sont équivalentes :

(a) m est un générateur de I

(b) $\forall i, a_i | m$ et pour tout $x \in A$ on a : $(\forall i, a_i | x) \Rightarrow m | x$.

(c) $\forall p$ irréductible $\nu_p(m) = \max\{\nu_p(a_i), i = 1, \cdots, n\}$

ii) L'ensemble des idéaux principaux *contenant tous les a_i contient un unique élément minimal. Pour un élément $d \in A$, les assertions suivantes sont équivalentes :*

(a) d est un générateur de J

(b) $\forall i, d | a_i$ et pour tout $x \in A$ on a : $(\forall i, x | a_i) \Rightarrow x | d$.

(c) $\forall p$ irréductible $\nu_p(d) = \min\{\nu_p(a_i), i = 1, \cdots, n\}$

Ceci nous invite à la définition suivante.

DÉFINITION. – *Avec les notations de la proposition, tout générateur de I est appelé* un ppcm des a_i. *Tout générateur de J est appelé* un pgcd des a_i. *On dit que les a_i sont premiers entre eux si $J = A$.*

On prendra donc garde au fait qu'un ppcm ou un pgcd n'est défini qu'à multiplication par un inversible près.

Démonstration. Choisissons un ensemble P de représentants des classes d'équivalence d'éléments irréductibles de A.

i) Pour tout $p \in P$, posons $v_p := \max\{\nu_p(a_i), i = 1, \cdots, n\}$. Puis $m := \prod_{p \in P} p^{v_p}$, qui est bien défini par le iv) de la proposition précédente. Comme $\nu_p(m) = v_p \geqslant \nu_p(a_i)$, le ii) de la proposition précédente nous assure que chaque a_i divise m, donc $m \in I$. Par ailleurs, si $x \in I$, on a d'après ce même point ii) $\nu_p(x) \geqslant \nu_p(a_i)$ pour tout p et tout a_i, donc $\nu_p(x) \geqslant v_p$ et finalement $m | x$. Donc $I = (m)$ est principal. On en déduit aussi l'équivalence entre (a) et (c). Quant à l'équivalence entre (a) et (b), elle est tautologique puisque pour tout $x \in A$ on a équivalence (tautologique) entre $(x \in I)$ et $(\forall i, a_i | x)$.

ii)Pour tout $p \in P$, posons $u_p := \min\{\nu_p(a_i), i = 1, \cdots, n\}$. Puis $d := \prod_{p \in P} p^{u_p}$. Alors $d | a_i$ pour tout i (proposition précédente) donc (d) contient chaque (a_i). Réciproquement, si (x) contient chaque (a_i), alors x divise chaque a_i et $\nu_p(x) \leqslant \nu_p(a_i)$ pour tout i, donc $\nu_p(x) \leqslant u_p = \nu_p(d)$ et x divise d. Ainsi l'idéal (d) est le plus petit idéal principal contenant chaque (a_i). Le même argument montre l'équivalence de (a), (b) et (c). □

Remarque. (Attention) – Par définition, a et b sont premiers entre eux si A est le seul idéal principal qui contient (a, b). On prendra garde au fait que cela n'implique pas en général que $(a, b) = A$. Par exemple dans $\mathbb{C}[X, Y]$ (dont on verra plus loin qu'il est factoriel), on a $(X, Y) \subsetneq \mathbb{C}[X, Y]$.

1.5.4 *Anneaux principaux et euclidiens.* Un anneau A est dit *principal* s'il est intègre et si tous ses idéaux sont principaux. Un tel anneau est donc en particulier noethérien. Les exemples les plus célèbres sont $\mathbb{Z}$ et $K[X]$, et plus généralement les anneaux *euclidiens* (voir plus loin).

THÉORÈME. – *Soit A un anneau principal.*

i) A est factoriel.

ii) Tout idéal premier non nul est maximal.

iii) Si $a, b \in A$ sont premiers entre eux alors $(a, b) = A$.

Démonstration. iii) Puisque A est principal, l'idéal (a, b) est principal. L'hypothèse "premiers entre eux" signifie que le seul idéal principal contenant (a, b) est A. Donc $(a, b) = A$.

ii) Soit I un idéal premier non nul. Puisque A est principal, I est engendré par un élément non nul, disons $I = (x)$. Puisque I est premier, x est irréductible, et donc (x) est maximal parmi les idéaux principaux propres. Mais comme tous les idéaux sont principaux, (x) est un idéal maximal "tout court".

i) A est principal donc noethérien donc il satisfait l'existence (Ex) de factorisations. Par ailleurs, si x est irréductible, nous venons de voir que (x) est un idéal maximal, donc a fortiori premier. D'après le lemme vu plus haut, A vérifie donc (Un). $\square$

DÉFINITION. – *Un anneau intègre A est dit* euclidien *s'il admet une fonction $N : A \setminus \{0\} \longrightarrow \mathbb{N}$ vérifiant la propriété suivante : pour tous a, b non nuls, il existe $q, r \in A$ tels que $b = qa + r$ et ($N(r) < N(a)$ ou $r = 0$).*

THÉORÈME. – *Soit A un anneau euclidien. Tout idéal I non nul est engendré par tout élément $a \in I \setminus \{0\}$ tel que $N(a)$ soit minimal. En particulier, A est principal.*

Démonstration. Soient I et a comme dans l'énoncé, et soit $b \in I$. Ecrivons $b = qa + r$ avec ($N(r) < N(a)$ ou $r = 0$. Si $r \neq 0$, alors $r = b - qa \in I$ et la minimalité de $N(a)$ est contredite. Donc $r = 0$ et $b \in (a)$, et finalement $I = (a)$. $\square$

Bien-sûr, $\mathbb{Z}$ est le prototype d'anneau euclidien, avec N la fonction "valeur absolue".

Exemple. – Soit K un corps. Alors la fonction $f \mapsto N(f) = \deg(f)$ fait de $K[X]$ un anneau euclidien, donc principal, et donc factoriel. Un idéal I de $K[X]$ est engendré par tout polynôme $f \in I$ de degré minimal.

Attention, si A n'est pas un corps, $A[X]$ n'est pas euclidien (ni principal). Nous avons en effet défini la division euclidienne par un polynôme *unitaire* de $A[X]$, ce qui s'étend à un polynôme dont le coefficient dominant est inversible dans A, mais si ce coefficient dominant n'est pas inversible, il n'y a pas moyen de diviser "euclidiennement". Concrètement, soit $a \in A$ un élément non nul et non inversible, alors l'idéal (a, X) n'est pas principal.

Exemple. – Soit $A = \mathbb{Z}[i]$. Alors la fonction $z \mapsto N(z) := z\bar{z}$ en fait un anneau euclidien, donc principal (cf TD). De même pour $A = \mathbb{Z}[\sqrt{-2}]$ et pour $\mathbb{Z}[j]$.

Exercice. – On va montrer que l'anneau d'entiers $A = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ est principal, mais pas euclidien.

i) Montrer que dans un anneau euclidien, il existe un élément non inversible x tel que tout élément non nul du corps $A/(x)$ est image d'un inversible de A.

ii) Montrer que $A^\times = \{\pm 1\}$ mais que A n'a aucun morphisme d'anneaux surjectif vers $\mathbb{F}_2$ et $\mathbb{F}_3$. En conclure que A n'est pas euclidien.

iii) Montrer que pour $a, b \in A \setminus \{0\}$, il existe (q, r) tels que ($r = 0$ ou $N(r) < N(a)$) et ($b = qr + a$ ou $2b = qr + a$). Puis montrer qu'un idéal I de A est engendré par un élément $a \in I$ de norme minimale.

Notre prochain but est de prouver le théorème de transfert de Gauss qui affirme que si A est factoriel alors $A[X]$ l'est aussi. Nous aurons besoin de la notion de corps des fractions d'un anneau intègre.

1.6 Localisation, corps des fractions

1.6.1 *Localisation : construction.* Dans un anneau commutatif A, on dit qu'un sous-ensemble S de A est une *partie multiplicative* si S est stable par multiplication, contient 1 mais ne contient pas 0. (Autrement dit, S est un sous-monoïde unitaire de $(A \setminus \{0\}, \cdot, 1)$).

Exemples. – Voici quelques exemples de parties multiplicatives.
— Lorsque A est intègre, l'ensemble $S = A \setminus \{0\}$.
— Pour A non intègre, l'ensemble $S = A_{\text{reg}}$ des éléments réguliers de A.
— Si $f \in A$ n'est pas nilpotent, l'ensemble $S = \{f^n, n \in \mathbb{N}\}$ des puissances de f.
— Si $\mathfrak{p}$ est un idéal premier, l'ensemble complémentaire $A \setminus \mathfrak{p}$ (le vérifier).

Soit S une partie multiplicative de A. On munit l'ensemble $A \times S$ de la relation d'équivalence suivante (exercice : vérifier la transitivité) :

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

On remarquera que lorque A est intègre, le côté droit se simplifie en : $as' - a's = 0$. On notera $S^{-1}A := (A \times S)/\sim$ l'ensemble quotient, et $\frac{a}{s}$ la classe d'équivalence de (a, s). On définit sur $S^{-1}A$ une addition par la formule suivante :

LEMME. – *i) L'application $(A \times S) \times (A \times S) \longrightarrow A \times S$ qui envoie $((a, s), (b, r))$ sur $(ar + bs, sr)$ induit une loi associative et commutative*

$$\begin{array}{rccc} + : & S^{-1}A \times S^{-1}A & \to & S^{-1}A \\ & (\frac{a}{s}, \frac{b}{r}) & \mapsto & \frac{a}{s} + \frac{b}{r} = \frac{ar+bs}{sr} \end{array}$$

d'élément neutre $0 := \frac{0}{s}$ pour tout s.

ii) L'application $(A \times S) \times (A \times S) \longrightarrow A \times S$ qui envoie $((a, s), (b, r))$ sur (ab, sr) induit une loi associative, commutative, et distributive par rapport à $+$,

$$\begin{array}{rccc} \cdot : & S^{-1}A \times S^{-1}A & \to & S^{-1}A \\ & (\frac{a}{s}, \frac{b}{r}) & \mapsto & \frac{a}{s} \cdot \frac{b}{r} = \frac{ab}{sr} \end{array}$$

d'élément neutre $1 := \frac{1}{1}$. *Ainsi* $(S^{-1}A, +, \cdot)$ *est un anneau.*

iii) L'application $A \xrightarrow{\iota} S^{-1}A$, $a \mapsto \frac{a}{1}$ *est un morphisme d'anneaux.*

Démonstration. i) Vérifions d'abord que la loi est bien définie. Soit $(a', s') \sim (a, s)$ et $(b', r') \sim (b, r)$. Il existe donc $t, u \in S$ tels que $t(as' - a's) = 0 = u(br' - b'r)$. On a alors $ut((ar+bs)s'r' - (a'r'+b's')sr) = 0$ et il s'ensuit que $(ar+bs, sr) \sim (a'r'+b's', s'r')$, ce qui montre que la loi $+$ est bien définie sur $S^{-1}A$. La commutativité de cette loi est évidente, ainsi que le fait que $\frac{0}{s}$ en est un élément neutre (indépendant de s). L'associativité résulte aussi d'un calcul sans difficulté.

ii) Même raisonnement que ci-dessus en plus facile, laissé au lecteur.

iii) Il suffit de l'écrire. $\square$

Remarque. – Le noyau du morphisme canonique $\iota : A \longrightarrow S^{-1}A$ est constitué des éléments a tels que $(a, 1) \sim (0, 1)$. On voit donc que $\mathrm{Ker}(\iota) = \{a \in A, \exists t \in S, at = 0\}$ est constitué en particulier de diviseurs de 0.

Proposition. – *Si A est noethérien, alors $S^{-1}A$ est noethérien.*

Démonstration. Soit J un idéal de $S^{-1}A$. Posons $I := \iota^{-1}(J) = \{a \in A, \frac{a}{1} \in J\}$. Alors pour tout $\frac{a}{s} \in J$, on a $\frac{a}{1} = \frac{a}{s} \cdot \frac{s}{1} \in J$, donc $a \in I$. Il s'ensuit que $J = \iota(I) \cdot S^{-1}A$ est engendré par l'image de I dans $S^{-1}A$, et donc par tout système de générateurs de I dans A. $\square$

Exercice. – Rappelons que l'on note $\mathrm{Spec}(A)$ l'ensemble des idéaux premiers de l'anneau A. Montrer que l'application $\mathfrak{p} \mapsto \iota^{-1}(\mathfrak{p})$ induit une bijection

$$\mathrm{Spec}(S^{-1}A) \xrightarrow{\sim} \{\mathfrak{q} \in \mathrm{Spec}(A), \mathfrak{q} \cap S = \emptyset\}$$

dont la bijection réciproque est $\mathfrak{q} \mapsto S^{-1}\mathfrak{q} := (S \times \mathfrak{q})_{/\sim} = \iota(\mathfrak{q}) \cdot S^{-1}A$.

Exercice. – Montrer que A réduit implique $S^{-1}A$ réduit.

1.6.2 *Localisation : propriété universelle.* La propriété remarquable de $S^{-1}A$ est que les éléments de S "y deviennent inversibles". En effet, si $s \in S$ on a dans $S^{-1}A$ l'égalité $\frac{s}{1} \cdot \frac{1}{s} = \frac{1}{s} \cdot \frac{s}{1} = \frac{s}{s} = \frac{1}{1} = 1$. En fait, $S^{-1}A$ est caractérisé, en tant que A-algèbre, par la propriété universelle suivante :

Proposition. – *Pour toute A-algèbre $A \xrightarrow{\varphi} B$ telle que $\varphi(S) \subset B^\times$, il existe un unique morphisme de A-algèbres $S^{-1}A \xrightarrow{\tilde{\varphi}} B$ (autrement dit un unique morphisme d'anneaux tel que $\tilde{\varphi} \circ \iota = \varphi$).*

Démonstration. Unicité : si $\tilde{\varphi}$ est comme dans l'énoncé, on doit avoir pour tout $a, s \in A \times S$ l'égalité $\tilde{\varphi}(\frac{a}{s})\tilde{\varphi}(\frac{s}{1}) = \tilde{\varphi}(\frac{a}{1}) = \varphi(a)$, et donc $\tilde{\varphi}(\frac{a}{s}) = \varphi(a)\varphi(s)^{-1}$. D'où l'unicité de $\tilde{\varphi}$.

Existence : il nous faut vérifier que l'expression $\tilde{\varphi}(\frac{a}{s}) := \varphi(a)\varphi(s)^{-1}$ est bien définie. Or, si $(a', s') \sim (a, s)$ il existe $t \in S$ tel que $tas' = ta's$ donc $\varphi(t)\varphi(a)\varphi(s') = \varphi(t)\varphi(a')\varphi(s)$, puis $\varphi(a)\varphi(s)^{-1} = \varphi(a')\varphi(s')^{-1}$ (noter que la commutativité de la multiplication est ici cruciale). L'expression voulue est donc bien définie. Reste à voir qu'elle définit un morphisme d'anneau, ce qui est un calcul immédiat. $\square$

Remarque. – Appliquée à $B = S^{-1}A$, l'unicité dans la proposition implique que l'identité est l'unique endomorphisme de la A-algèbre $S^{-1}A$.

Remarque. – L'application $\iota : A \longrightarrow S^{-1}A$ est en général loin d'être surjective. Pourtant, l'unicité dans la proposition ci-dessus montre que ι est un *épimorphisme* au sens catégorique du terme, *i.e.* il est *simplifiable à gauche* : pour toute paire $\psi, \psi' : S^{-1}A \longrightarrow B$ de morphismes de A-algèbres, on a $\psi \circ \iota = \psi' \circ \iota \Rightarrow \psi = \psi'$.

Remarque. – Dans la proposition on peut autoriser B à être non commutative. Voici une conséquence intéressante du cas non commutatif : un A-module M sur lequel chaque élément $s \in S$ agit bijectivement est canoniquement un $S^{-1}A$-module (et réciproquement). De plus, si M et N sont des $S^{-1}A$-modules, tout morphisme de A-modules est automatiquement un morphisme de $S^{-1}A$-modules, *i.e.*

$$\mathrm{Hom}_{S^{-1}A}(M,N) = \mathrm{Hom}_A(M,N).$$

Remarque. – La propriété universelle ci-dessus suggère une autre construction pour $S^{-1}A$, qui utilise la propriété universelle de l'algèbre $A[S]$ du monoïde S. En effet, l'application $s \mapsto \frac{1}{s}$ est un morphisme de monoïdes $S \longrightarrow (S^{-1}A \setminus \{0\}, \cdot, 1)$, donc il existe un morphisme de A-algèbre $\varphi : A[S] \longrightarrow S^{-1}A$ qui envoie e_s sur $\frac{1}{s}$ pour tout $s \in S$. On a alors $\varphi(se_s - 1) = \varphi(s)\varphi(e_s) - 1 = \frac{s}{1}\frac{1}{s} - 1 = 0$ pour tout $s \in S$, donc φ se factorise par un morphisme

$$\bar{\varphi} : A[S]/\langle se_s - 1,\, s \in S\rangle \longrightarrow S^{-1}A,$$

où $\langle se_s - 1,\, s \in S\rangle$ désigne l'idéal engendré par les éléments $se_s - 1$, $s \in S$.

COROLLAIRE. – *Le morphisme $\bar{\varphi}$ ci-dessus est un isomorphisme de A-algèbres.*

Démonstration. Construisons-lui un inverse. Soit $\bar{f}$ l'image d'un $f \in A[S]$ dans le quotient $A[S]/\langle se_s - 1,\, s \in S\rangle$. On a $\bar{s}\bar{e}_s = 1$, donc $\bar{s}$ est inversible dans ce quotient, et donc par la proposition précédente il existe un morphisme $\psi : S^{-1}A \longrightarrow A[S]/\langle se_s - 1,\, s \in S\rangle$ qui envoie $\frac{1}{s}$ sur $\bar{e}_s$. Puisque les $\bar{e}_s$ sont une famille génératrice du A-module $A[S]/\langle se_s - 1,\, s \in S\rangle$, le morphisme ψ est surjectif. Par ailleurs, la composée $\bar{\varphi} \circ \psi$ est l'identité (cf remarque ci-dessus), donc ψ est aussi injectif et $\bar{\varphi}$ est son inverse. □

1.6.3 *Le corps des fractions d'un anneau intègre.* Supposons A intègre et $S = A \setminus \{0\}$. Dans ce cas, tout élément non nul de $S^{-1}A$ est de la forme $\frac{a}{b}$ avec $a, b \neq 0$, et donc est inversible d'inverse $\frac{b}{a}$. Ainsi, $S^{-1}A$ est un corps qui contient A (via ι), appelé *corps des fractions* de A et aussi noté $\mathrm{Frac}(A)$. On retrouve par exemple la construction de $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$ ou du corps $K(X) = \mathrm{Frac}(K[X])$ des fractions rationnelles en une indéterminée sur un corps.

LEMME. – *Soit A intègre de corps des fractions K. Alors* $\mathrm{Frac}(A[X]) = K(X)$.

Démonstration. Puisque tout élément non nul de $A[X] \subset K[X]$ est inversible dans $K(X)$ (qui est un corps), la propriété universelle du localisé nous fournit un morphisme canonique $\mathrm{Frac}(A[X]) \longrightarrow K(X)$, qui est d'ailleurs injectif puisque c'est un morphisme de corps.

Montrons qu'il est surjectif. Pour cela, il faut vérifier que toute fraction rationnelle $Q = \frac{f}{g} \in K(X)$ avec $f, g \in K[X]$ peut s'écrire $\frac{\tilde{f}}{\tilde{g}}$ avec $\tilde{f}, \tilde{g} \in A[X]$. Ecrivons $f = \sum_n \frac{a_n}{b_n} X^n$ et $g = \sum_n \frac{c_n}{d_n} X^n$. Posons $a := \prod_n b_n \prod_n d_n$. Il suffit de poser $\tilde{f} := af$ et $\tilde{g} := ag$. $\square$

Plus généralement, on note $K(X_1, \cdots, X_n) := \mathrm{Frac}(K[X_1, \cdots, X_n])$. Le lemme ci-dessus joint à l'isomorphisme $K[X_1, \cdots, X_n] = K[X_1, \cdots, X_{n-1}][X_n]$ nous montre que $K(X_1, \cdots, X_n) = K(X_1, \cdots, X_{n-1})(X_n)$.

Regardons maintenant le cas particulier d'un anneau factoriel :

PROPOSITION. – *Soit A factoriel et $K := \mathrm{Frac}(A)$. Pour tout élément irréductible $p \in A$, la valuation p-adique se prolonge de manière unique en une fonction*

$$\nu_p : K^\times \longrightarrow \mathbb{Z} \text{ telle que } \nu_p(xy) = \nu_p(x) + \nu_p(y), \forall x, y \in K^\times.$$

De plus, si P désigne un ensemble des classes d'équivalence d'éléments irréductibles de A, alors tout élément $x \in K^\times$ est de la forme $x = u \cdot \prod_{p \in P} p^{\nu_p(x)}$ avec $u \in A^\times$. En particulier on a

$$\forall x \in K^\times,\ x \in A \Leftrightarrow (\forall p \text{ irréductible}, \nu_p(x) \geqslant 0).$$

Démonstration. Si $x = \frac{a}{b}$, la condition d'additivité sur ν_p nous impose $\nu_p(a) = \nu_p(\frac{a}{b} \cdot \frac{b}{1}) = \nu_p(\frac{a}{b}) + \nu_p(b)$ et donc $\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b)$. D'où l'unicité d'un éventuel prolongement. Pour l'existence, il faut vérifier que cette expression ne dépend que de x. Mais si $x = \frac{a'}{b'}$, on a $a'b = ab'$ et donc $\nu_p(a') + \nu_p(b) = \nu_p(a) + \nu_p(b')$ et finalement $\nu_p(a) - \nu_p(b) = \nu_p(a') - \nu_p(b')$ comme voulu. La seconde assertion sur $x = \frac{a}{b}$ découle de la même assertion valable dans A appliquée à a et b. Cette seconde assertion montre le sens $\Leftarrow$ de la dernière équivalence, tandis que le sens $\Rightarrow$ est clair. $\square$

Exercice. – Montrer que pour tous $x, y \in K$ on a $\nu_p(x + y) \geqslant \min(\nu_p(x), \nu_p(y))$ (avec la convention que $\nu_p(0) = \infty$ et $\infty \geqslant n$ pour tout entier n). Ainsi ν_p est une valuation de $K(X)$ au sens de 1.5.2.

Nous sommes maintenant en mesure de prouver le théorème dit "de transfert de Gauss".

THÉORÈME. – *Si A est factoriel, alors $A[X]$ est factoriel.*

Démonstration. D'après la proposition précédente appliquée à l'anneau factoriel (et même principal) $K[X]$, tout polynôme irréductible $f \in K[X]$ fournit une valuation ν_f du corps $K(X)$. Notons V_+ l'ensemble de ces valuations.

Par ailleurs, si un élément $p \in A$ est irréductible dans A, il l'est aussi dans $A[X]$ au vu de l'additivité des degrés. De plus, l'idéal $pA[X]$ qu'il engendre est premier car $A[X]/pA[X] \simeq (A/pA)[X]$ est intègre (puisque A est factoriel). La valuation p-adique ν_p de $A[X]$ étend celle de A, et est donnée explicitement par

$$\nu_p(f) = \min\{\nu_p(a_n), n \in \mathbb{N}\} \text{ pour } f = \textstyle\sum_n a_n X^n.$$

En effet, si m_p désigne le nombre de droite on peut écrire $a_n = p^{m_p}a'_n$ pour tout n et $f = p^{m_p}f'$ avec $f' = \sum_n a'_n X^n$. Comme l'un des a'_n n'est pas divisible par p, l'image de f' dans $A[X]/pA[X] \simeq (A/pA)[X]$ est non nulle, donc f' n'est pas divisible par p dans $A[X]$ et finalement $m_p = \nu_p(f)$.

D'après la proposition précédente, ν_p s'étend au corps des fractions $K(X)$. Notons V_0 l'ensemble des valuations de K de la forme ν_p, et posons $V := V_0 \cup V_+$. On a alors

$$A[X] = K(X)_V := \{f \in K(X), \forall v \in V, v(f) \geqslant 0\}.$$

En effet, la proposition précédente nous dit que $K(X)_{V_+} = K[X]$ et $K_{V_0} = A$, donc la formule $\nu_p(f) = \mathrm{Min}\{\nu_p(a_n), n \in \mathbb{N}\}$ valable pour $f \in K[X]$ (car $\nu_p(f) = \nu_p(af) - \nu_p(a)$ et on peut choisir a pour que $af \in A[X]$) montre que $K(X)_{V_0} \cap K[X] = K_{V_0}[X] = A[X]$.

Il ne nous reste plus qu'à montrer que V satisfait les deux hypothèses de la deuxième proposition 1.5.2.

i) Par la proposition précédente, si $f \in K(X)$ alors l'ensemble $\{v \in V_+, v(f) \neq 0\}$ est fini. Pour la même raison, pour $a \in K$ l'ensemble $\{v \in V_0, v(a) \neq 0\}$ est fini. La formule de $\nu_p(f)$ pour $f \in K[X]$ montre alors que $\{v \in V_0, v(f) \neq 0\}$ est fini. Il en est de même pour toute $f \in K(X)$, puisque elle est de la forme $\frac{g}{h}$ avec $g, h \in K[X]$.

ii) Pour $v \in V_0$, il existe $p_v \in A$ tel que $v = \nu_{p_v}$. On a alors $v(p_v) = 1$ et $w(p_v) = 0$ pour $w \in V_0$ distincte de v. De plus, pour $w \in V_+$ on a aussi $w(p_v) = 0$ puisque w est de la forme ν_f pour un polynôme f de degré > 0. Soit maintenant $v \in V_+$. Elle est de la forme ν_f pour un polynôme irréductible $f \in K[X]$. Soit $c := \prod_{w \in V_0} p_w^{w(f)} \in A$, et posons $f_v := c^{-1}f$. On a alors $w(f_v) = 0$ pour toute valuation $w \in V_0$. De plus, on a aussi $w(f_v) = 0$ pour $w = \nu_g$ dans V_+ distincte de v. □

Remarque. – Pour A intègre général, on peut toujours mettre une fraction sous la forme $x = \frac{a}{b}$ avec a, b sans facteur commun. Lorsque A est factoriel, cette écriture est unique aux unités près, *i.e.* si $x = \frac{a'}{b'}$ avec a', b' sans facteurs communs, alors il existe $u \in A^\times$ tel que $a' = ua$ et $b' = ub$. Cela découle de la proposition ci-dessus. Lorsque A n'est pas factoriel, on n'a pas une telle unicité. Exemple dans $\mathbb{Z}[\sqrt{-5}]$: $\frac{2}{1+\sqrt{-5}} = \frac{1-\sqrt{-5}}{3}$.

Que se passe-t-il si on localise un anneau intègre pour une partie multiplicative quelconque ?

Lemme. – *Soit A intègre et $S \subset A$ une partie multiplicative. On a un isomorphisme canonique*

$$S^{-1}A \xrightarrow{\sim} \{x \in \mathrm{Frac}(A), \exists s \in S, sx \in A\}$$

qui fait de $S^{-1}A$ une sous-A-algèbre de $\mathrm{Frac}(A)$.

Démonstration. Puisque tout $s \in S$ est inversible dans $\mathrm{Frac}(A)$ la propriété universelle du localisé fournit un morphisme canonique $S^{-1}A \longrightarrow \mathrm{Frac}(A)$. Ce morphisme est injectif puisque si $\frac{a}{s}$ est dans le noyau alors $\frac{a}{1}$ aussi, donc $a = 0$ puisque A s'injecte dans $\mathrm{Frac}(A)$. Son image est clairement celle décrite dans l'énoncé. □

On peut remarquer que $S^{-1}A$ est en particulier intègre, de corps des fractions $\mathrm{Frac}(A)$.

Exercice. – Montrer que si A est factoriel, alors $S^{-1}A$ l'est aussi, et que l'application $x \mapsto \frac{x}{1}$ induit une bijection de l'ensemble des classes d'association d'éléments irréductibles de A ne divisant pas un élément de S sur l'ensemble des classes d'association d'éléments irréductibles de $S^{-1}A$.

1.6.4 *Inversion d'un élément.* Lorsque $f \in A$ est non nilpotent et $S = \{f^n, n \in \mathbb{N}\}$, on note aussi $A_{(f)}$ ou encore $A[f^{-1}]$ l'anneau $S^{-1}A$. Cette dernière notation est justifiée par le corollaire 1.6.2 qui implique que l'unique morphisme de A-algèbres $A[X] \longrightarrow A[f^{-1}]$ qui envoie X sur $\frac{1}{f}$ induit un isomorphisme

$$A[X]/(Xf - 1) \xrightarrow{\sim} A[f^{-1}].$$

Remarque. – Comme $\operatorname{Ker}(A \longrightarrow A[f^{-1}]) = \{x \in A, \exists n \in \mathbb{N}, f^n x = 0\}$, on voit que $A[f^{-1}]$ est un anneau non nul, puisque f n'est pas nilpotent. Il contient donc un idéal maximal, dont l'image réciproque dans A est, d'après l'exercice 1.6.1, un idéal premier $\mathfrak{p}$ tel que $f \notin \mathfrak{p}$. On voit ainsi que l'intersection $\bigcap_{\mathfrak{p} \in \operatorname{Spec}(A)} \mathfrak{p}$ est formée d'éléments nilpotents de A. Comme par ailleurs tout nilpotent appartient à tout $\mathfrak{p}$ premier, on a donc obtenu :

Proposition. – $\sqrt{(0)} = \bigcap\limits_{\mathfrak{p} \in \operatorname{Spec}(A)} \mathfrak{p}$.

Exemple. – Dans l'anneau $A[X]$, prenons $f = X$. On retrouve l'anneau $A[X, X^{-1}]$ des polynômes de Laurent.

Exercice. – Soit $A = \mathbb{C}[X, Y]/(X^2Y)$ et $f = X$, montrer que $A[f^{-1}] = \mathbb{C}[X, X^{-1}]$.

Exercice. – Soit $A = \mathbb{C}[X, Y]/(XY)$ et $f = X + Y$. Montrer que l'élément $e = \frac{X}{X+Y}$ est un idempotent dans $A[f^{-1}]$, puis montrer que $A[f^{-1}] = \mathbb{C}[X, X^{-1}] \times \mathbb{C}[Y, Y^{-1}]$.

Interprétation géométrique. (Fonctions régulières sur un ouvert principal de $\mathbb{C}^n$) – Si f est une fonction polynomiale sur $\mathbb{C}^n$, notons

$$U_f := \{z \in \mathbb{C}, f(z) \neq 0\} = \mathbb{C}^n \setminus V(f).$$

C'est un ouvert dense de $\mathbb{C}^n$ et on a $U_f \cap U_{f'} = U_{ff'}$. On aimerait une bonne notion de "fonction régulière" sur U_f. On pourrait penser aux fonctions obtenues comme restriction de fonctions polynomiales sur $\mathbb{C}^n$, mais cela est contraire à l'intuition que sur U_f il devrait y avoir "plus de fonctions régulières", certaines se prolongeant à $\mathbb{C}^n$, d'autres non. La fonction f ne s'annulant pas sur U_f, son inverse f^{-1} semble être le prototype de fonction régulière ne se prolongeant pas à $\mathbb{C}^n$ et nous amène à la définition suivante : *une fonction régulière sur U_f est une fonction de la forme $z \mapsto g(z)f(z)^{-k}$ pour une fonction polynomiale g sur $\mathbb{C}^n$ et un entier $k \in \mathbb{N}$.* L'ensemble $\mathcal{O}(U_f)$ des fonctions régulières sur U_f est une $\mathbb{C}$-algèbre et on a par définition un isomorphisme

$$\mathcal{O}(U_f) = \mathcal{O}(\mathbb{C}^n)[f^{-1}].$$

à comparer avec l'isomorphisme $\mathcal{O}(V(f)) = \mathcal{O}(\mathbb{C}^n)/(f)$.

Interprétation géométrique. (Fonctions rationnelles sur $\mathbb{C}^n$) – Considérons l'ensemble des paires (U, φ) formées d'un ouvert principal de $\mathbb{C}^n$ et d'une fonction régulière $\varphi \in \mathcal{O}(U)$ (par définition, il existe donc $f, g \in \mathbb{C}[X_1, \cdots, X_n]$ tels que $U = U_f$ et $\varphi(z) = g(z)/f(z)^m$). On identifie $(U, \varphi) \sim (U', \varphi')$ si $\varphi_{|U \cap U'} = \varphi'_{U \cap U'}$. On appelle alors *fonction rationnelle* sur $\mathbb{C}^n$ toute classe d'équivalence de paires (U, φ). Le terme "fonction" est donc ici un peu abusif puisque le domaine de définition d'une telle "fonction" n'est pas $\mathbb{C}^n$ tout entier. L'ensemble $\mathcal{M}(\mathbb{C}^n)$ des fonctions rationnelles sur $\mathbb{C}$ est une $\mathbb{C}$-algèbre : on a $(U, \varphi) + (U', \varphi') := (U \cap U', \varphi + \varphi')$ et $(U, \varphi)(U', \varphi') = (U \cap U', \varphi\varphi')$. C'est même un corps où l'inverse est donné par $(U_f, \varphi)^{-1} = (U_g, \varphi^{-1})$ si $\varphi(z) = g(z)/f(z)$ et $\varphi \neq 0$ (et donc $g \neq 0$). Ce corps n'est pas mystérieux :

Lemme. – *On a $\mathcal{M}(\mathbb{C}^n) \simeq \mathbb{C}(X_1, \cdots, X_n)$.*

Démonstration. À une fraction rationnelle $Q = \frac{g}{f} \in \mathbb{C}(X_1, \cdots, X_n)$ on associe la paire (U_f, φ) avec $\varphi(z) = g(z)/f(z)$. On obtient visiblement un morphisme de $\mathbb{C}$-algèbres non nul, donc injectif puisque $\mathbb{C}(X_1, \cdots, X_n)$ est un corps. Par ailleurs, ce morphisme est surjectif par définition des fonctions rationnelles. □

1.6.5 *Localisation en un idéal premier.* Si $\mathfrak{p}$ est un idéal premier d'un anneau A, et $S := A \setminus \mathfrak{p}$, on note généralement $A_\mathfrak{p}$ le localisé $A_\mathfrak{p} := S^{-1}A$. Noter que si (et même seulement si) A est intègre, l'idéal nul $\mathfrak{p} = 0$ est premier et on a vu que le localisé associé est le corps des fractions de A. Ceci est un cas particulier du résultat suivant.

Proposition. – *Soit $\mathfrak{p}A_\mathfrak{p}$ l'idéal de $A_\mathfrak{p}$ engendré par l'image de $\mathfrak{p}$. Alors $A_\mathfrak{p}^\times = A_\mathfrak{p} \setminus \mathfrak{p}A_\mathfrak{p}$, l'idéal $\mathfrak{p}A_\mathfrak{p}$ est l'unique idéal maximal de $A_\mathfrak{p}$ et le morphisme canonique $A \longrightarrow A_\mathfrak{p}$ induit un morphisme injectif $A/\mathfrak{p} \hookrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ qui identifie $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ au corps des fractions de $A/\mathfrak{p}$.*

Démonstration. Considérons la composée $\varphi := A \xrightarrow{\iota} A_\mathfrak{p} \longrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Son noyau contient clairement $\mathfrak{p}$ donc elle se factorise par un morphisme $\overline{\varphi} : A/\mathfrak{p} \longrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Tout élément non nul de l'anneau intègre $A/\mathfrak{p}$ provient d'un élément de $A \setminus \mathfrak{p}$ donc, par définition du localisé $A_\mathfrak{p}$, est envoyé sur un élément inversible de $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Par propriété universelle du corps des fractions d'un anneau intègre on a donc une factorisation de $\overline{\varphi}$:

$$\overline{\varphi} : A/\mathfrak{p} \hookrightarrow \mathrm{Frac}(A/\mathfrak{p}) \xrightarrow{\tilde{\varphi}} A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}.$$

Dans l'autre sens, considérons la composée $\psi : A \longrightarrow A/\mathfrak{p} \hookrightarrow \mathrm{Frac}(A/\mathfrak{p})$. Elle envoie tout élément de $A \setminus \mathfrak{p}$ sur un élément non nul donc inversible dans $\mathrm{Frac}(A/\mathfrak{p})$. Par propriété universelle, ψ se factorise par le localisé $A_\mathfrak{p}$ en $\tilde{\psi} : A_\mathfrak{p} \longrightarrow \mathrm{Frac}(A/\mathfrak{p})$. Clairement, $\mathfrak{p}$ est contenu dans le noyau, donc $\tilde{\psi}$ se factorise à son tour par le quotient

$$\tilde{\psi} : A_\mathfrak{p} \twoheadrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \xrightarrow{\overline{\psi}} \mathrm{Frac}(A/\mathfrak{p}).$$

La composée $\overline{\psi} \circ \tilde{\varphi}$ est un endomorphisme de la A-algèbre $\mathrm{Frac}(A/\mathfrak{p})$, donc de la $A/\mathfrak{p}$-algèbre $\mathrm{Frac}(A/\mathfrak{p})$, donc est égal à l'identité par l'unicité dans la pté universelle du localisé $\mathrm{Frac}(A/\mathfrak{p})$. De même, la composée $\tilde{\varphi} \circ \overline{\psi}$ est un endomorphisme de la A-algèbre $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$.

Un tel endomorphisme est aussi $A_\mathfrak{p}$-linéaire (cf remarque plus haut), i.e est un morphisme de $A_\mathfrak{p}$-algèbres, donc est égal à l'identité de $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Ainsi $\tilde{\varphi}$ et $\overline{\psi}$ sont des isomorphismes réciproques de A-algèbres.

À ce point nous en déduisons que $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ est un corps, donc que $\mathfrak{p}A_\mathfrak{p}$ est un idéal maximal de $A_\mathfrak{p}$ et aussi que $A_\mathfrak{p}^\times \subset A_\mathfrak{p} \setminus \mathfrak{p}A_\mathfrak{p}$. Pour montrer l'inclusion réciproque, soit $x = \frac{a}{b} \in A_\mathfrak{p}$ avec $a \in A$ et $b \in A \setminus \mathfrak{p}$. Si x est dans le complémentaire $A_\mathfrak{p} \setminus \mathfrak{p}A_\mathfrak{p}$ alors $a \in A \setminus \mathfrak{p}$. Donc a est inversible dans $A_\mathfrak{p}$ et x aussi. D'où l'inclusion $A_\mathfrak{p} \setminus \mathfrak{p}A_\mathfrak{p} \subset A_\mathfrak{p}^\times$ voulue. Cette inclusion implique aussi que tout idéal *propre* I de $A_\mathfrak{p}$ est contenu dans $\mathfrak{p}A_\mathfrak{p}$, et donc que ce dernier est bien le seul idéal maximal de $A_\mathfrak{p}$. □

Remarque. – Le premier exercice de 1.6.1 nous dit que l'application $\mathfrak{q} \mapsto \mathfrak{q}A_\mathfrak{p}$ est une bijection $\{\mathfrak{q} \in \mathrm{Spec}(A), \mathfrak{q} \subset \mathfrak{p}\} \xrightarrow{\sim} \mathrm{Spec}(A_\mathfrak{p})$ et la propriété universelle des localisés nous fournit un unique isomorphisme de A-algèbres $A_\mathfrak{q} \xrightarrow{\sim} (A_\mathfrak{p})_{\mathfrak{q}A_\mathfrak{p}}$ pour tout $\mathfrak{q} \subset \mathfrak{p}$.

Exemple. – Supposons A factoriel et $\mathfrak{p}$ principal. Notons $\nu_\mathfrak{p} := \nu_p$ la valuation associée à n'importe quel générateur p de $\mathfrak{p}$ (elle ne dépend que de $\mathfrak{p}$). Alors

$$A_\mathfrak{p} = \{x \in \mathrm{Frac}(A),\ \nu_\mathfrak{p}(x) \geqslant 0\}.$$

En effet, un lemme précédent identifie $A_\mathfrak{p}$ à $\{x \in \mathrm{Frac}(A), \exists s \in (A \setminus \mathfrak{p}), sx \in A\}$. Or, $A \setminus \mathfrak{p} = \{s \in A, \nu_\mathfrak{p}(s) = 0\}$, donc $sx \in A \Rightarrow \nu_\mathfrak{p}(x) = \nu_\mathfrak{p}(sx) \geqslant 0$ et, réciproquement, si $\nu_\mathfrak{p}(x) \geqslant 0$ on peut mettre x sous la forme $x = \frac{a}{s}$ avec $\nu_p(s) = 0$ d'après la proposition 1.6.3. De même on a

$$\mathfrak{p}A_\mathfrak{p} = \{x \in \mathrm{Frac}(A), \nu_\mathfrak{p}(x) > 0\}.$$

Considérons l'exemple $A = \mathbb{C}[X]$ et $\mathfrak{p} = \mathfrak{p}_z = (X - z)$ pour un $z \in \mathbb{C}$ (tout idéal premier non nul de $\mathbb{C}[X]$ est de cette forme car $\mathbb{C}$ est algébriquement clos). On a vu que la valuation ν_{X-z} est l'ordre d'annulation en z d'une fonction polynomiale. La discussion ci-dessus identifie donc le localisé $A_{\mathfrak{p}_z}$ à la sous-algèbre de $\mathbb{C}(X)$ formée des fractions rationnelles qui n'ont pas de pôle en z.

Interprétation géométrique. (*Fonctions rationnelles sur une variété algébrique irréductible*) – Après avoir introduit la notion de fonction rationnelle sur $\mathbb{C}^n$ ci-dessus, on voudrait maintenant faire de même sur un sous-ensemble algébrique $V \subset \mathbb{C}^n$. Nous supposons ici que V est irréductible, *i.e.* que $\mathcal{O}(V)$ est un anneau intègre, donc de la forme $\mathcal{O}(V) = \mathcal{O}(\mathbb{C}^n)/\mathfrak{p}$ avec $\mathfrak{p}$ idéal premier de $\mathcal{O}(\mathbb{C}^n)$. On a alors

$$V = V(\mathfrak{p}) = \{z \in \mathbb{C}^n, \forall f \in \mathfrak{p}, f(z) = 0\} \quad \text{et} \quad \mathfrak{p} = \{f \in \mathcal{O}(\mathbb{C}^n), f_{|V} = 0\}.$$

La discussion que nous avons faite pour $\mathbb{C}^n$ s'adapte sans difficulté à V. On considère les classes d'équivalences de paires (U, φ) où U est un ouvert de V de la forme $U_f = \{z \in V, f(z) \neq 0\}$ pour une fonction $f \in \mathcal{O}(V)$ et $\varphi \in \mathcal{O}(U_f) := \mathcal{O}(V)[f^{-1}]$ est une fonction régulière sur U. On obtient un corps $\mathcal{M}(V)$ qui en termes algébriques s'identifie à $\mathrm{Frac}(\mathcal{O}(V))$. D'où une première définition commode :

$$(1) \qquad \mathcal{M}(V) := \mathrm{Frac}(\mathcal{O}(V)) = \mathrm{Frac}(A/\mathfrak{p}) \text{ où } A := \mathcal{O}(\mathbb{C}^n) = \mathbb{C}[X_1, \cdots, X_n].$$

Néanmoins, l'intuition géométrique voudrait plutôt que l'on tente de définir une fonction rationnelle sur V comme la restriction d'une fonction rationnelle (U, φ) sur $\mathbb{C}^n$. Cela n'est évidemment possible que si le domaine de définition U intersecte V. Dans ce cas on dit que la fonction rationnelle est "définie sur un ouvert de V" et on pose $(U, \varphi)_{|V} := (U \cap V, \varphi_{|U \cap V})$ qui est une paire formée d'un ouvert dense "principal" de V et d'une fonction "régulière" sur cet ouvert. Il est alors naturel de définir

(2) $\mathcal{M}(V)$ comme *l'ensemble des classes d'équivalence de paires de la forme* $(U \cap V, \varphi_{|U \cap V})$,

où la relation d'équivalence sur les paires formées d'un ouvert dense et d'une fonction est la même que précédemment.

Notons alors $\mathcal{M}(\mathbb{C}^n)_V$ l'ensemble des fonctions rationnelles sur $\mathbb{C}^n$ qui sont définies sur un ouvert dense de V. Via l'isomorphisme du lemme précédent, on constate que

$$\mathcal{M}(\mathbb{C}^n)_V \simeq \left\{ Q = \frac{f}{g} \in \mathbb{C}(X_1, \cdots, X_n), g_{|V} \neq 0 \right\} = A_{\mathfrak{p}}.$$

La définition (2) présente alors $\mathcal{M}(V)$ comme le quotient de $\mathcal{M}(\mathbb{C}^n)_V$ par l'idéal I_V des fonctions qui s'annulent sur V. Or via le lemme précédent on peut identifier

$$I_V \simeq \left\{ Q = \frac{f}{g} \in \mathbb{C}(X_1, \cdots, X_n), g_{|V} \neq 0 \text{ et } f_{|V} = 0 \right\} = \mathfrak{p}A_{\mathfrak{p}}.$$

La définition (2) revient donc à poser $\mathcal{M}(V) := A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ et la proposition ci-dessus nous assure que la définition (1) lui est équivalente.

Interprétation géométrique. (*Anneau local d'une variété algébrique en un point*) – Continuons avec le contexte ci-dessus d'un ensemble algébrique irréductible $V \subset \mathbb{C}^n$, et fixons un point $z \in V$. Ce point fournit un morphisme d'évaluation $\mathcal{O}(V) \longrightarrow \mathbb{C}$ dont le noyau est un idéal maximal $\mathfrak{m}_z$. Le localisé $\mathcal{O}(V)_z = \mathcal{O}(V)_{\mathfrak{m}_z}$ correspondant est un sous-anneau de $\mathcal{M}(V)$ qui s'interprète comme l'algèbre des fonctions rationnelles sur V définies au voisinage de z. On l'appelle "anneau local de V en z"

Exemple. (*Un exemple d'anneau noethérien où un élément admet une infinité de diviseurs irréductibles non associés*) – Considérons la courbe V d'équation $X^2 - Y^3 = 0$ dans $\mathbb{C}^2$ et le point $z = (0, 0)$ (qui, si l'on fait le dessin des points réels, apparait comme un point "singulier"). Dans $\mathbb{C}[X, Y]$, considérons la partie multiplicative S formée des polynômes de terme constant non nul. Alors $\mathcal{O}(V)_z = S^{-1}\mathbb{C}[X, Y]/(X^2 - Y^3)$ le quotient du localisé par l'idéal engendré par $(X^2 - Y^3)$. Pour tout $a \in \mathbb{C}$, on a $(aX + Y)(aX - Y) = (a^2X^2 - Y^2)$ dans $\mathbb{C}[X, Y]$. Dans $\mathcal{O}(V)_z$, on a $(a^2X^2 - Y^2) = Y^2(a^2Y - 1)$, et l'élément $a^2Y - 1$ est inversible. Il s'ensuit que Y^2 est divisible, dans $\mathcal{O}(V)_z$, par tous les éléments $aX + Y$, $a \in \mathbb{C}$, dont on vérifie facilement qu'ils sont irréductibles et 2 à 2 non associés.

1.6.6 *L'anneau total des fractions.* Lorsque A n'est pas intègre, l'ensemble $A \setminus \{0\}$ n'est pas une partie multiplicative de A, et on le remplace par l'ensemble $S = A_{\mathrm{reg}}$ des éléments réguliers de A (ie non nuls et non diviseurs de 0). On note parfois $Q(A)$ le localisé $S^{-1}A$ et on l'appelle *anneau total des fractions.* Il a la particularité d'être le "plus grand localisé" dans lequel A *s'injecte.*

Exercice. – Pour $A = \mathbb{C}[X,Y]/(XY)$, montrer que $Q(A) = \mathbb{C}(X) \times \mathbb{C}(Y)$. (Utiliser un exercice précédent).

Plus généralement, lorsque A est *réduit* et *noethérien*, $Q(A)$ est le produit d'un nombre fini de corps. Plus précisément :

PROPOSITION. – *Supposons A réduit et notons* $\mathrm{Spec}(A)_{\min}$ *l'ensemble des idéaux premiers minimaux de A.*

i) Si $\mathfrak{p} \in \mathrm{Spec}(A)_{\min}$*, alors* $\mathfrak{p}A_{\mathfrak{p}} = 0$*, et donc* $\mathrm{Frac}(A/\mathfrak{p}) = A_{\mathfrak{p}}$.

ii) $A_{\mathrm{reg}} = A \setminus \left(\bigcup_{\mathfrak{p} \in \mathrm{Spec}(A)_{\min}} \mathfrak{p} \right)$ *et on a une bijection* $\mathrm{Spec}(A)_{\min} \xrightarrow{\sim} \mathrm{Spec}(Q(A))_{\min}$*,* $\mathfrak{p} \mapsto \mathfrak{p}Q(A)$ *telle que* $A_{\mathfrak{p}} = Q(A)_{\mathfrak{p}Q(A)}$.

iii) Supposons $\mathrm{Spec}(A)_{\min}$ *fini. Alors* $\mathrm{Spec}(Q(A)) = \mathrm{Spec}(Q(A))_{\min}$ *et le morphisme produit*

$$Q(A) \longrightarrow \prod_{\mathfrak{p} \in \mathrm{Spec}(A)_{\min}} Q(A)_{\mathfrak{p}Q(A)} = \prod_{\mathfrak{p} \in \mathrm{Spec}(A)_{\min}} \mathrm{Frac}(A/\mathfrak{p})$$

est un isomorphisme.

iv) Si A est noethérien, alors $\mathrm{Spec}(A)_{\min}$ *est fini.*

Démonstration. i) Le premier exercice de 1.6.1 nous assure que $\mathrm{Spec}(A_{\mathfrak{p}}) = \{\mathfrak{p}A_{\mathfrak{p}}\}$. Le second nous assure que $A_{\mathfrak{p}}$ est réduit, donc $\mathfrak{p}A_{\mathfrak{p}} = \{0\}$. La proposition 1.6.5 nous dit alors que $\mathrm{Frac}(A/\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = A_{\mathfrak{p}}$.

ii) Soit $\mathfrak{p}$ minimal et $a \in \mathfrak{p} \setminus \{0\}$. On vient de voir que l'image de a est nulle dans le localisé $A_{\mathfrak{p}}$. Il s'ensuit que a est diviseur de 0. Réciproquement, soit a un diviseur de 0. Choisissons $b \in A \setminus \{0\}$ tel que $ab = 0$. Puisque b est non nul et donc non nilpotent, il existe un idéal premier $\mathfrak{q}$ qui ne le contient pas. Le lemme de Zorn nous dit que l'on peut trouver un premier minimal $\mathfrak{p}$ dans $\mathfrak{q}$ (car l'intersection d'une suite décroissante d'idéaux premiers est un idéal premier). On a alors $ab \in \mathfrak{p}$ et donc $a \in \mathfrak{p}$. Le reste de l'assertion découle du fait que la bijection du premier exercice 1.6.1 est croissante et du fait que, dans la situation de cet exercice, on a un unique isomorphisme de A-algèbres $A_{\mathfrak{p}} \xrightarrow{\sim} (S^{-1}A)_{S^{-1}\mathfrak{p}}$ par la propriété universelle.

iii) Vu la bijection du premier exercice 1.6.1, l'égalité $\mathrm{Spec}(Q(A)) = \mathrm{Spec}(Q(A))_{\min}$ équivaut à l'égalité $\{\mathfrak{p} \in \mathrm{Spec}(A), \mathfrak{p} \cap A_{\mathrm{reg}} = \emptyset\} = \mathrm{Spec}(A)_{\min}$. D'après le point ii), il faut donc montrer que si $\mathfrak{p}$ premier est contenu dans la réunion des premiers minimaux, alors $\mathfrak{p}$ est minimal. Puisque $\mathrm{Spec}(A)_{\min}$ est supposé fini, il existe un ensemble fini minimal $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}$ de premiers minimaux tel que $\mathfrak{p} \subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$. Supposons $r \geqslant 2$. Il existe donc $a_i \in (\mathfrak{p} \cap \mathfrak{p}_i) \setminus (\bigcup_{j \neq i} \mathfrak{p}_j)$ pour tout i. Puisque $\mathfrak{p}_i$ est premier, l'élément $b_i := \prod_{j \neq i} a_j$

de $\mathfrak{p}$ est dans tous les $\mathfrak{p}_j$ sauf $\mathfrak{p}_i$. La somme $\sum_i b_i$ est alors dans $\mathfrak{p}$ mais dans aucun des $\mathfrak{p}_i$: contradiction. On a donc $r = 1$ et $\mathfrak{p} = \mathfrak{p}_1 \in \mathrm{Spec}(A)_{\min}$.

Puisque tous les idéaux premiers de $Q(A)$ sont minimaux, ils sont aussi maximaux. Soit alors $\mathfrak{p}Q(A) \in \mathrm{Spec}(Q(A))$. Puisqu'il est maximal, $Q(A)/\mathfrak{p}Q(A)$ est un corps, et on a donc $Q(A)/\mathfrak{p}Q(A) = \mathrm{Frac}(Q(A)/\mathfrak{p}Q(A))$. Puisqu'il est minimal, le i) nous dit que $\mathrm{Frac}(Q(A)/\mathfrak{p}Q(A)) = Q(A)_{\mathfrak{p}Q(A)}$. En résumé, le morphisme $Q(A) \longrightarrow Q(A)_{\mathfrak{p}Q(A)}$ induit un isomorphisme $Q(A)/\mathfrak{p}Q(A) \xrightarrow{\sim} Q(A)_{\mathfrak{p}Q(A)}$, et il ne nous reste plus qu'à prouver que le morphisme produit

$$Q(A) \longrightarrow \prod_{\mathfrak{p}\in\mathrm{Spec}(A)_{\min}} Q(A)/\mathfrak{p}Q(A)$$

est un isomorphisme. C'est une version du lemme chinois avec "plusieurs idéaux" (que l'on reverra plus tard). Concrètement, ce morphisme est injectif car son noyau $\bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)_{\min}} \mathfrak{p}Q(A)$ est le nilradical de $Q(A)$ qui est nul. Pour voir qu'il est surjectif, il suffit de montrer qu'il contient chaque idempotent $e_\mathfrak{p} = (0, \cdots, 1, \cdots, 0)$ avec le 1 placé en l'indice $\mathfrak{p}$. Or, par maximalité de tous les $\mathfrak{p}Q(A)$, il existe des éléments $a_{\mathfrak{p}\mathfrak{q}} \in Q(A)$ pour $\mathfrak{p} \neq \mathfrak{q}$ tels que $a_{\mathfrak{p}\mathfrak{q}} \in \mathfrak{p}Q(A)$ et $a_{\mathfrak{p}\mathfrak{q}} + a_{\mathfrak{q}\mathfrak{p}} = 1$. Mais alors, l'élément $a_\mathfrak{p} := \prod_{\mathfrak{q}\neq\mathfrak{p}} a_{\mathfrak{q}\mathfrak{p}}$ a pour image l'idempotent voulu $e_\mathfrak{p}$ dans le produit $\prod_\mathfrak{p} Q(A)/\mathfrak{p}Q(A)$. On notera que ce produit n'est défini que si l'ensemble $\mathrm{Spec}(A)_{\min}$ est fini.

v) Considérons l'ensemble $\mathcal{I}$ des idéaux I pour lesquels $\mathrm{Spec}(A)_{\geqslant I} := \{\mathfrak{p} \in \mathrm{Spec}(A), \mathfrak{p} \supset I\}$ possède une infinité d'éléments minimaux. Si $\mathcal{I}$ est non vide, il admet un élément maximal I, puisque A est supposé noethérien. Alors I n'est manifestement pas premier, et on peut donc trouver $f, g \in A \setminus I$ tels que $fg \in I$. Un idéal premier contenant I contient alors f ou g, de sorte que $\mathrm{Spec}(A)_{\geqslant I}$ est réunion de $\mathrm{Spec}(A)_{\geqslant I+(f)}$ et $\mathrm{Spec}(A)_{\geqslant I+(g)}$ et donc $\mathrm{Spec}(A)_{\geqslant I,\min}$ est contenu dans la réunion de $\mathrm{Spec}(A)_{\geqslant I+(f),\min}$ et $\mathrm{Spec}(A)_{\geqslant I+(g),\min}$. Mais ces deux ensembles sont finis, par maximalité de I, contredisant l'existence même de I. $\square$

Interprétation géométrique. (Composantes irréductibles) – La proposition précédente s'applique à la $\mathbb{C}$-algèbre $\mathcal{O}(V)$ d'un ensemble algébrique $V \subset \mathbb{C}^n$, puisque celle-ci est réduite et noethérienne. Notons $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ les idéaux premiers minimaux de $\mathcal{O}(V)$ et $V_i := \{z \in V, \forall f \in \mathfrak{p}_i, f(z) = 0\}$ le sous-ensemble algébrique de V défini par $\mathfrak{p}_i$. Un théorème de Hilbert que nous verrons plus loin, le *Nullstellensatz*, implique que $\mathfrak{p}_i = \{f \in \mathcal{O}(V),\ f_{|V_i} = 0\}$ (seule l'inclusion $\subset$ est évidente). Ainsi, chaque V_i est *irréductible* (au sens de 1.2.6) puisque $\mathcal{O}(V_i) = \mathcal{O}(V)/\mathfrak{p}_i$ est intègre. La contrepartie géométrique de l'égalité $\bigcap_{i=1}^r \mathfrak{p}_i = \{0\}$ est la propriété de recouvrement $V = V_1 \cup \cdots \cup V_r$. Le Nullstellensatz implique aussi qu'aucun V_i n'est contenu dans la réunion des autres V_j. Ceci caractérise la famille des V_i parmi les familles couvrantes de sous-ensembles irréductibles. On appelle les V_i les *composantes irréductibles* de V.

Définissons maintenant l'algèbre des fonctions rationnelles $\mathcal{M}(V)$ sur V comme le quotient $\mathcal{M}(\mathbb{C}^n)_V/I_V$ avec les mêmes définitions que dans 1.6.5. Ainsi $\mathcal{M}(\mathbb{C}^n)_V$ est l'ensemble des fractions rationnelles $\frac{f}{g}$ avec g telle que $g_{|V_i} \neq 0$ pour tout i. C'est donc le localisé de $\mathcal{O}(\mathbb{C}^n)$ en la partie multiplicative $\bigcap_{i=1}^r(\mathcal{O}(\mathbb{C}^n) \setminus \widetilde{\mathfrak{p}}_i)$ où $\widetilde{\mathfrak{p}}_i$ est la préimage de $\mathfrak{p}_i$ dans $\mathcal{O}(\mathbb{C}^n)$. Il s'ensuit que $\mathcal{M}(V)$ est le localisé de $\mathcal{O}(V)$ en $\bigcap_{i=1}^r(\mathcal{O}(V) \setminus \mathfrak{p}_i)$, et on a donc

$\mathcal{M}(V) = Q(\mathcal{O}(V))$. La proposition précédente nous dit alors que $\mathcal{M}(V) = \prod_{i=1}^{r} \mathcal{M}(V_i)$.

Remarque. – Lorsque $\mathrm{Spec}(A)_{\min}$ n'est pas fini, il peut exister des idéaux premiers $\mathfrak{p}$ non minimaux contenus dans $A \backslash A_{\mathrm{reg}}$. Exemple : soit $A = k[X_1, \cdots, X_n, \cdots]/(X_i X_j, i \neq j)$. Alors l'idéal maximal $(X_1, \cdots, X_n, \cdots)$ est formé de diviseurs de 0 mais n'est pas minimal puisqu'il contient strictement l'idéal premier $(X_2, X_3, \cdots, X_n, \cdots)$.

1.7 Produit tensoriel

Le lecteur a peut-être déjà rencontré la notion de "complexifié" d'un espace vectoriel réel. Nous allons développer un procédé plus général qui permet de passer des modules sur un anneau A à ceux sur une A-algèbre B, et qui repose sur la notion de *produit tensoriel.*

1.7.1 *Applications bilinéaires.* Soit A un anneau commutatif unitaire et M, N, P trois A-modules. Une application $M \times N \xrightarrow{\theta} P$ est dite *A-bilinéaire* si pour tout $m \in M$, resp. pour tout $n \in N$, les applications

$$\theta(m, -) : N \longrightarrow P \text{ et } \theta(-, n) : M \longrightarrow P$$

sont A-linéaires (i.e. des morphismes de A-modules).

Exemple. – Si B est une A-algèbre, l'application produit $B \times B \longrightarrow B$ est A-bilinéaire.

Exemple. – Si M et N sont deux A-modules, l'application $M \times \mathrm{Hom}_A(M, N) \longrightarrow N$, $(m, \varphi) \mapsto \varphi(m)$ est A-bilinéaire.

Nous noterons $\mathrm{Bil}_A(M \times N, P)$ l'ensemble des applications A-bilinéaires de $M \times N$ dans P. c'est naturellement un A-module, avec l'addition $(\theta_1 + \theta_2)(m, n) := \theta_1(m, n) + \theta_2(m, n)$ et l'action de A donnée par $(a\theta)(m, n) := a.\theta(m, n)$.

1.7.2 THÉORÈME.– *Il existe un A-module $M \otimes_A N$ muni d'une application bilinéaire*

$$\begin{array}{ccc} M \times N & \to & M \otimes_A N \\ (m, n) & \mapsto & m \otimes n \end{array}$$

universel au sens suivant : pour tout A-module P muni d'une application bilinéaire θ : $M \times N \longrightarrow P$, il existe un unique morphisme de A-modules $\varphi_\theta : M \otimes N \longrightarrow P$ tel que $\theta(m, n) = \varphi_\theta(m \otimes n)$. En d'autres termes, l'application $\varphi \mapsto \varphi \circ (- \otimes -)$ est un isomorphisme (de A-modules)

$$\mathrm{Hom}_A(M \otimes_A N, P) \xrightarrow{\sim} \mathrm{Bil}_A(M \times N, P).$$

De plus, le A-module $M \otimes_A N$ muni de l'application bilinéaire $(m, n) \mapsto m \otimes n$ est unique à isomorphisme unique près.

Remarque. – Pour une fois, nous définissons l'objet par sa propriété universelle, plutôt que par sa construction. C'est parce que, en général, cette construction ne nous dit pas grand chose.

Démonstration. Comme d'habitude, l'unicité à isomorphisme unique près sera conséquence de la propriété universelle. Pour l'existence, il faut construire $M \otimes_A N$ "à la main" en essayant de respecter le cahier des charges imposé par la propriété universelle.

Partons du A-module libre $A^{(M\times N)}$ dont nous noterons $(e_{m,n})_{(m,n)\in M\times N}$ la base "canonique". Considérons le sous-A-module K de $A^{(M\times N)}$ engendré par les éléments suivants :

— $e_{m+m',n} - e_{m,n} - e_{m',n}$ et $e_{m,n+n'} - e_{m,n} - e_{m,n'}$ où $m, m' \in M$ et $n, n' \in N$.

— $e_{am,n} - ae_{m,n}$ et $e_{m,an} - ae_{m,n}$ où $m \in M$, $n \in N$ et $a \in A$.

Posons alors $M \otimes_A N := A^{(M,N)}/K$ et notons $m \otimes n = \overline{e_{m,n}}$ l'image de $e_{m,n}$ dans ce quotient. Remarquons que, par définition de K, on a la relation

$$(m + m') \otimes n = \overline{e_{m+m',n}} = \overline{e_{m,n}} + \overline{e_{m',n}} = m \otimes n + m' \otimes n.$$

De même on a la relation

$$(am) \otimes n = \overline{e_{am,n}} = a\overline{e_{am,n}} = a.(m \otimes n).$$

Ainsi, l'application $m \mapsto m\otimes n$ est A-linéaire pour tout n. De même, l'application $n \mapsto m\otimes n$ est A-linéaire pour tout m, et finalement l'application $(m, n) \mapsto m \otimes n$ est A-bilinéaire. Par composition on a donc, pour tout A-module P, une application

$$\begin{array}{rcl} \mathrm{Hom}_A(M \otimes_A N, P) & \to & \mathrm{Bil}_A(M \times N, P) \\ \varphi & \mapsto & (\theta_\varphi : (m, n) \mapsto \varphi(m \otimes n)) \end{array}.$$

Il s'agit de prouver que cette application est bijective.

Pour cela nous allons construire une application dans l'autre sens. Partons de $\theta : M \times N \longrightarrow P$ bilinéaire. D'après la propriété universelle des modules libres, il existe un unique morphisme de A-modules $\tilde{\varphi}_\theta : A^{(M\times N)} \longrightarrow P$ tel que $\tilde{\varphi}_\theta(e_{m,n}) = \theta(m, n)$. On remarque alors que

$$\tilde{\varphi}_\theta(e_{m+m',n} - e_{m,n} - e_{m',n}) = \theta(m + m', n) - \theta(m, n) - \theta(m', n) = 0,$$

la dernière égalité venant de la bilinéarité de θ. De même on a

$$\tilde{\varphi}_\theta(e_{am,n} - ae_{m,n}) = \theta(am, n) - a\theta(m, n) = 0,$$

puis aussi

$$\tilde{\varphi}_\theta(e_{m,n+n'} - e_{m,n} - e_{m,n'}) = 0 = \tilde{\varphi}(e_{m,an} - ae_{m,n}).$$

On voit donc que $K \subset \mathrm{Ker}(\tilde{\varphi}_\theta)$. Par la propriété universelle des quotients, on en déduit que $\tilde{\varphi}_\theta$ se factorise par un unique morphisme $\varphi_\theta : A^{(M,N)}/K = M \otimes_A N \longrightarrow P$ qui envoie $m \otimes n = \overline{e_{m,n}}$ sur $\tilde{\varphi}_\theta(e_{m,n}) = \theta(m, n)$. On a donc construit une application

$$\begin{array}{rcl} \mathrm{Bil}_A(M \times N, P) & \to & \mathrm{Hom}_A(M \otimes_A N, P) \\ \theta & \mapsto & \varphi_\theta : m \otimes n \mapsto \theta(m, n) \end{array}.$$

Visiblement, les deux applications ainsi construites sont inverses l'une de l'autre. $\square$

Remarque. (Attention) – Un élément quelconque de $M \otimes_A N$ n'est pas de la forme $m \otimes n$, mais une combinaison A-linéaire de tels éléments.

Les éléments de $M \otimes_A N$ sont parfois appelés *tenseurs*. Un élément de la forme $m \otimes n$ est appelé *tenseur élémentaire*. Tout tenseur est donc combinaison linéaire de tenseurs élémentaires.

1.7.3 *Propriétés fonctorielles.* Soient M, N comme précédemment et soient $\varphi : M \longrightarrow M'$, $\psi : N \longrightarrow N'$ deux morphismes de A-modules.

Lemme. – *Il existe un unique morphisme de A-modules*

$$\varphi \otimes \psi : M \otimes_A N \longrightarrow M' \otimes_A N'$$

qui envoie $m \otimes n$ sur $\varphi(m) \otimes \psi(n)$ pour tous $m \in M$ et $n \in N$.

Démonstration. Considérons l'application $\theta : M \times N \longrightarrow M' \otimes_A N'$ qui envoie un couple (m, n) sur le tenseur $\varphi(m) \otimes \psi(n)$. On a $\theta(am + m', n) = \varphi(am + m') \otimes \psi(n) = (a\varphi(m) + \varphi(m')) \otimes \psi(n) = a(\varphi(m) \otimes \psi(n)) + \varphi(m') \otimes \psi(n) = a\theta(m, n) + \theta(m', n)$, et de même on a $\theta(m, an + n') = a\theta(m, n) + \theta(m, n')$. Donc θ est bilinéaire, et il existe un unique morphisme $M \otimes_A N \longrightarrow M' \otimes_A N'$ qui envoie $m \otimes n$ sur $\theta(m, n) = \varphi(m) \otimes \psi(n)$. $\square$

Remarque. – L'unicité dans le lemme implique que si $\varphi' : M' \longrightarrow M''$ et $\psi' : N' \longrightarrow N''$ sont deux autre morphismes on a $(\varphi' \otimes \psi') \circ (\varphi \circ \psi) = (\varphi' \circ \varphi) \otimes (\psi' \otimes \psi)$.

1.7.4 *Propriétés monoïdales.* Le produit tensoriel joue vraiment un rôle de "multiplication" sur la "catégorie" des A-modules. La proposition suivante nous dit qu'il est "essentiellement" commutatif, associatif, distributif par rapport aux sommes directes, et que A est un "objet" neutre.

Proposition. – *Soient M, M' et N des A-modules.*

i) L'application $M \longrightarrow A \otimes_A M$, $m \mapsto 1 \otimes m$ est un isomorphisme de A-modules dont l'inverse envoie $a \otimes m$ sur am.

ii) Il existe un unique isomorphisme de A-modules

$$M \otimes_A N \xrightarrow{\sim} N \otimes_A M$$

qui envoie $m \otimes n$ sur $n \otimes m$.

iii) Il existe un unique isomorphisme de A-modules

$$(M \oplus M') \otimes_A N \xrightarrow{\sim} (M \otimes_A N) \oplus (M' \otimes_A N)$$

qui envoie $(m, m') \otimes n$ sur $(m \otimes n, m' \otimes n)$.

iv) Il existe un unique isomorphisme de A-modules

$$(M \otimes_A M') \otimes_A N \xrightarrow{\sim} M \otimes_A (M' \otimes_A N)$$

qui envoie $(m \otimes m') \otimes n$ sur $m \otimes (m' \otimes n)$.

Démonstration. i) L'application $A\times M \longrightarrow M$, $(a,m)\mapsto am$ est A-bilinéaire donc provient d'un morphisme $A\otimes_A M \xrightarrow{\varphi} M$ qui envoie $a\otimes m$ sur am. Notons ψ le morphisme de l'énoncé. On a $\varphi\circ\psi(m)=\varphi(1\otimes m)=m$ donc $\varphi\circ\psi=\mathrm{id}_M$. Par ailleurs on a $\psi\circ\varphi(a\otimes m)=\psi(am)=1\otimes(am)=a(1\otimes m)=(a.1)\otimes m=a\otimes m$. Comme les tenseurs élémentaires engendrent $A\otimes_A M$, on en déduit que $\psi\circ\varphi=\mathrm{id}_{A\otimes_A M}$.

ii) L'application $M\times N\longrightarrow N\otimes_A M$ qui envoie (m,n) sur $n\otimes m$ est A-bilinéaire donc provient d'un morphisme $M\otimes_A N\longrightarrow N\otimes_A M$ qui envoie $m\otimes n$ sur $n\otimes m$. Celui-ci est uniquement déterminé par cette propriété puisque les tenseurs $m\otimes n$ engendrent $M\otimes_A N$. Le même argument nous fournit un morphisme dans l'autre sens qui envoie $n\otimes m$ sur $m\otimes n$. Comme les tenseurs engendrent les produits tensoriels, les deux morphismes ainsi construits sont inverses l'un de l'autre.

iii) L'application $(M\oplus M')\times N\longrightarrow (M\otimes_A N)\oplus(M'\otimes_A N)$ qui envoie $((m,m'),n)$ sur $(m\otimes n, m'\otimes n)$ est A-bilinéaire donc provient d'un morphisme comme dans l'énoncé. Dans l'autre sens, l'application $M\times N\longrightarrow (M\oplus M')\otimes_A N$ qui envoie (m,n) sur $(m,0)\otimes n$ est bilinéaire, d'où un morphisme $M\otimes_A N\longrightarrow (M\oplus M')\otimes_A N$ qui envoie $m\otimes n$ sur $(m,0)\otimes n$. De même on a un morphisme $M'\otimes_A N\longrightarrow (M\oplus M')\otimes_A N$ qui envoie $m\otimes n$ sur $(0,m')\otimes n$. La propriété universelle des sommes directes nous fournit alors un morphisme $(M\otimes_A N)\oplus(M'\otimes_A N)\longrightarrow (M\oplus M')\otimes_A N$ qui envoie $(m\otimes n, m'\otimes n)$ sur $(m,0)\otimes n+(0,m')\otimes n=(m,m')\otimes n$. Ce morphisme est visiblement inverse de celui de l'énoncé.

iv) On peut raisonner exactement comme pour ii) par exemple (laissé au lecteur). On peut aussi plus élégamment remarquer que les applications

— $\theta^1 : M\times M'\times N\longrightarrow T^{(1)} := (M\otimes_A M')\otimes_A N$, $(m,m',n)\mapsto (m\otimes m')\otimes n$ et
— $\theta^2 : M\times M'\times N\longrightarrow T^{(2)} := M\otimes_A (M'\otimes_A N)$, $(m,m',n)\mapsto m\otimes(m'\otimes n)$

sont A-trilinéaires et vérifient chacune la propriété universelle suivante : pour toute application A-trilinéaire $\theta : M\times M'\times N\longrightarrow P$ il existe un unique morphisme de A-module $\varphi^i_\theta : T^{(i)}\longrightarrow P$ tel que $\theta=\theta^i\circ\varphi^i_\theta$. Alors $\varphi^1_{\theta^2}$ est le morphisme de l'énoncé et $\varphi^2_{\theta^1}$ est son isomorphisme réciproque.

□

Remarque. – Nous ferons parfois l'abus d'identifier $M\otimes_A(M'\otimes_A N)$ et $(M\otimes_A M')\otimes_A N$ et de les noter simplement
$$M\otimes_A M'\otimes_A N.$$
Comme expliqué dans la preuve ci-dessus, ce dernier est muni de l'application A-trilinéaire $(m,m',n)\mapsto m\otimes m'\otimes n$.

Exercice. – i) Utiliser i) et iii) de la proposition pour montrer que $A^n\otimes_A M\simeq M^n$.

ii) Généraliser iii) de la proposition à des sommes directes arbitraires ainsi :
$$\left(\bigoplus_{i\in I} M_i\right)\otimes_A N\simeq\bigoplus_{i\in I}(M_i\otimes_A N).$$

iii) En déduire $A^{(I)}\otimes_A M\simeq M^{(I)}$ pour tout ensemble I.

Voici un exemple important où le produit tensoriel prend une forme plus explicite.

1.7.5 PROPOSITION.– *Le produit tensoriel de deux modules libres est libre. Plus précisément, pour deux ensembles I, J, l'unique morphisme de A-modules*

$$\varphi : A^{(I\times J)} \longrightarrow A^{(I)} \otimes A^{(J)}$$

qui envoie $e_{i,j}$ sur $e_i \otimes e_j$ est un isomorphisme $A^{(I\times J)} \xrightarrow{\sim} A^{(I)} \otimes A^{(J)}$.

Démonstration. Cela pourrait se déduire de la proposition précédente renforcée par l'exercice ci-dessus, mais voici un argument détaillé. Considérons l'application $A^{(I)} \times A^{(J)} \longrightarrow A^{(I\times J)}$ définie par

$$\left(\sum_i a_i e_i, \sum_j b_j e_j\right) \mapsto \sum_{i,j} a_i b_j e_{i,j}.$$

On vérifie immédiatement qu'elle est A-bilinéaire. Il existe donc un unique morphisme de A-modules

$$\psi : A^{(I)} \otimes_A A^{(J)} \longrightarrow A^{(I\times J)}$$

qui envoie l'élément $(\sum_i a_i e_i) \otimes (\sum_j b_j e_j)$ sur $\sum_{i,j} a_i b_j e_{i,j}$ et donc, en particulier, $e_i \otimes e_j$ sur $e_{i,j}$. Puisque $\psi \circ \varphi(e_{i,j}) = e_{i,j}$, on a $\psi \circ \varphi = \mathrm{id}_{A^{(I\times J)}}$. Par ailleurs, pour $m = \sum_i a_i e_i$ et $n = \sum_j b_j e_j$, on a

$$\begin{aligned} \varphi \circ \psi(m \otimes n) &= \varphi\left(\sum_{i,j} a_i b_j e_{i,j}\right) = \sum_{i,j} a_i b_j (e_i \otimes e_j) = \sum_i a_i (e_i \otimes (\sum_j b_j e_j)) \\ &= \sum_i a_i (e_i \otimes n) = (\sum_i a_i e_i) \otimes n = m \otimes n. \end{aligned}$$

Comme les tenseurs élémentaires engendrent $M \otimes N$ (cf la construction du théorème), cela montre que $\varphi \circ \psi = \mathrm{id}_{A^{(I)}\otimes A^{(J)}}$. □

Exercice. – Soit k un corps et V, W deux k-espaces vectoriels de dimension finie. Notons $V^* := \mathrm{Hom}_k(V, k)$ le dual de V.

i) Montrer qu'il existe un unique isomorphisme $V^* \otimes_k W \xrightarrow{\sim} \mathrm{Hom}_k(V, W)$ qui envoie $f \otimes w$ sur l'application k-linéaire $v \mapsto f(v)w$.

ii) Supposons $W = V$. Montrer qu'il existe une unique forme k-linéaire $V^* \otimes_k V \xrightarrow{\varepsilon} k$ qui envoie $f \otimes v$ sur $f(v)$.

iii) Montrer que la composée $\mathrm{End}_k(V) = \mathrm{Hom}_k(V, V) \xrightarrow{\sim} V^* \otimes_k V \xrightarrow{\varepsilon} k$ est le morphisme $\varphi \mapsto \mathrm{tr}(\varphi)$. [On pourra choisir une base $e_1, \cdots, e_n$ de V, noter $e_1^*, \cdots, e_j^*$ sa base duale dans V^*, remarquer que $e_j^* \otimes e_i$ correspond à l'endomorphisme de V dont la matrice dans la base choisie est la matrice élémentaire E_{ij}, et enfin que $\varepsilon(e_j^* \otimes e_i) = \delta_{ij}$].

Remarque. – Il est important de préciser l'anneau au-dessus duquel on fait le produit tensoriel. Considérons par exemple deux $\mathbb{C}$-espaces vectoriels V et V' de dimension d et d'. Alors $V \otimes_{\mathbb{C}} V'$ est un $\mathbb{C}$-ev de dimension dd' donc aussi un $\mathbb{R}$-ev de dimension $2dd'$. Par contre $V \otimes_{\mathbb{R}} V'$ est un $\mathbb{R}$-ev de dimension $(2d)(2d') = 4dd'$.

1.7.6 *Extension des scalaires.* On suppose maintenant que le A-module M est une A-algèbre, et nous la noterons B. Nous allons étendre la structure de A-module sur $B \otimes_A N$ en une structure de B-module.

Proposition. – *Il existe sur $B \otimes_A N$ une unique structure de B-module telle que*

$$\forall b, b' \in B, \forall n \in N, \; b' \cdot (b \otimes n) = (b'b) \otimes n.$$

Démonstration. On prescrit l'action de b' sur les tenseurs élémentaires, donc l'unicité découle du fait que ces tenseurs élémentaires engendrent $B \otimes_A N$. Reste à voir que l'action de b' ainsi prescrite est bien définie, et qu'elle définit une structure de B-modules.

Existence. Notons $\mu_{b'} : B \longrightarrow B$, $b \mapsto b'b$ la multiplication par b' dans B. C'est un endomorphisme A-linéaire de B. D'après le lemme 1.7.3 il existe un unique morphisme $\Psi_{b'} := \mu_{b'} \otimes \mathrm{id}_N : B \otimes_A N \longrightarrow B \otimes_A N$ qui envoie $b \otimes n$ sur $\mu_{b'}(b) \otimes n = (b'b) \otimes n$.

Structure de B-module. Il s'agit maintenant de vérifier que l'application $b' \in B \mapsto \Psi_{b'} \in \mathrm{End}_A(B \otimes_A N)$ est un morphisme de A-algèbres. Or, l'égalité $((b' + b'')b) \otimes n = (b'b) \otimes n + (b''b) \otimes n$ montre que $\Psi_{b'+b''} = \Psi_{b'} + \Psi_{b''}$, et par ailleurs on a $\Psi_{b''b'}(b \otimes n) = (b''b'b) \otimes n = \Psi_{b''}((b'b) \otimes n) = \Psi_{b''} \circ \Psi_{b'}(b \otimes n)$, d'où $\Psi_{b''b'} = \Psi_{b''} \circ \Psi_{b'}$. $\square$

Exemple. – Si $N = A$, le i) de la proposition 1.7.4 assure que $B \otimes_A A = B$. Plus généralement, si I est un ensemble, le fait que le produit tensoriel "commute aux sommes directes" nous assure que $B \otimes_A A^{(I)} = B^{(I)}$. En d'autres termes :

Proposition. – *Si N est un A-module libre de base $(e_i)_{i \in I}$, alors $B \otimes_A N$ est un B-module libre de base $(1 \otimes e_i)_{i \in I}$.*

Exemple. – Soit V un $\mathbb{R}$-ev. Lorsqu'on ne dispose pas du produit tensoriel, on introduit souvent le *complexifié* $V_{\mathbb{C}}$ de V de l'une des deux manières suivantes :
- soit en choisissant une $\mathbb{R}$-base $(e_i)_{i \in I}$ de V et en posant $V_{\mathbb{C}} := \bigoplus_{i \in I} \mathbb{C}.e_i$,
- soit en posant $V_{\mathbb{C}} := V \oplus V$ et en définissant la multiplication de $a + ib \in \mathbb{C}$ sur (v, w) par $(a + ib).(v, w) := (av - bw, aw + bv)$.

La première méthode est non-canonique puisqu'elle repose sur un choix de base. La seconde semble plus naturelle, mais on serait bien en peine de la généraliser pour, par exemple, définir le "réelifié" d'un $\mathbb{Q}$-espace vectoriel ! Lorsqu'on dispose du produit tensoriel, la bonne manière de définir $V_{\mathbb{C}}$ est de poser $V_{\mathbb{C}} := \mathbb{C} \otimes_{\mathbb{R}} V$. La proposition ci-dessus fait un lien explicite avec la première méthode ci-dessus. Et la décomposition $\mathbb{C} \otimes_{\mathbb{R}} V = (\mathbb{R} \otimes_{\mathbb{R}} V) \oplus (i\mathbb{R} \otimes_{\mathbb{R}} V) \simeq V \oplus iV$ fait le lien avec la seconde.

Voici maintenant la propriété universelle qui caractérise l'extension des scalaires.

Proposition. – *Pour tout B-module M et tout morphisme de A-modules $\psi : N \longrightarrow M$, il existe un unique morphisme de B-modules $\varphi_\psi : B \otimes_A N \longrightarrow M$ tel que $\varphi(b \otimes n) = b\psi(n)$. En d'autres termes, l'application $\varphi \mapsto (\psi_\varphi : n \mapsto \varphi(1 \otimes n))$ est une bijection*

$$\mathrm{Hom}_B(B \otimes_A N, M) \xrightarrow{\sim} \mathrm{Hom}_A(N, M)$$

dont l'inverse est donnée par $\psi \mapsto \varphi_\psi$.

Démonstration. Encore une fois l'unicité de $\varphi = \varphi_\psi$ découle du fait que les tenseurs élémentaires $b\otimes m$ engendrent $B\otimes_A M$. Pour l'existence d'un morphisme de A-modules φ comme dans l'énoncé, il suffit de vérifier que l'application $B\times N \longrightarrow M$, $(b,n)\mapsto bn$ est A-linéaire, ce qui est immédiat. Il faut alors vérifier que φ est bien un morphisme de B-modules, ce qui découle du calcul $\varphi(b'\cdot(b\otimes n)) = \varphi((b'b)\otimes n) = b'bn = b'\varphi(b\otimes n)$. Enfin, il est clair que $\psi_{\varphi_\psi} = \psi$, et d'un autre côté on a $\varphi_{\psi_\varphi}(b\otimes n) = b\psi_\varphi(n) = b\varphi(1\otimes n) = \varphi(b(1\otimes n)) = \varphi(b\otimes n)$. D'où la dernière assertion de l'énoncé. □

Remarque. – Soit M un B-module et N un A-module. Le même raisonnement que pour la première proposition 1.7.6 montre qu'il existe une unique structure de B-module sur $M\otimes_A N$ telle que l'action de $b\in B$ sur un tenseur élémentaire $m\otimes n$ soit donnée par $b\cdot(m\otimes n) := (bm)\otimes n$. En d'autres termes, si $\rho_b : M \longrightarrow M$ désigne la multiplication par b dans M, alors la multiplication par b dans $M\otimes_A N$ est donnée par $\rho_b\otimes \mathrm{id}_N$.

1.7.7 *Transitivité de l'extension des scalaires.* Commençons avec M et N comme dans la remarque ci-dessus et soit M' un autre B-module. Le lemme suivant se montre comme le iv) de la proposition 1.7.4.

Lemme. – *Il existe un unique isomorphisme de B-modules*

$$M\otimes_B (M'\otimes_A N) \xrightarrow{\sim} (M\otimes_B M')\otimes_A N$$

qui envoie $m\otimes(m'\otimes n)$ sur $(m\otimes m')\otimes n$ pour tout $m\in M$, $m'\in M'$ et $n\in N$.

Le cas particulier $M' = B$ de ce lemme nous donne donc un isomorphisme

$$M\otimes_B (B\otimes_A N) \xrightarrow{\sim} (M\otimes_B B)\otimes_A N \xrightarrow{\sim} M\otimes_A N$$

où le second isomorphisme est $i\otimes \mathrm{id}_N$ avec $i : M\otimes_B B \xrightarrow{\sim} M$ l'isomorphisme qui envoie $m\otimes b$ sur bm comme dans le point i) de la proposition 1.7.4. L'isomorphisme réciproque

$$M\otimes_A N \xrightarrow{\sim} M\otimes_B (B\otimes_A N)$$

envoie $m\otimes n$ sur $m\otimes(1\otimes n)$.

Supposons maintenant que M est une B-algèbre, que nous noterons C. On a donc deux morphismes d'anneaux $A\longrightarrow B\longrightarrow C$.

Proposition. – *Il existe un unique isomorphisme de C-modules*

$$C\otimes_A N \xrightarrow{\sim} C\otimes_B (B\otimes_A N)$$

qui envoie $c\otimes n$ sur $c\otimes(1\otimes n)$ et dont l'inverse envoie $c\otimes(b\otimes n)$ sur $cb\otimes n$.

Démonstration. Nous venons de voir que les morphismes en question existent et sont des isomorphismes de B-modules. Il reste à voir qu'ils sont C-linéaires, ce qui est évident vu la définition de l'action de C. □

1.7.8 *Extension des scalaires par un morphisme quotient.* On s'intéresse ici au cas où $B = A/I$ pour un idéal I de A. Si M est un A-module, on note

$$IM := \{m \in M, \exists i_1, \cdots, i_r \in I, \exists m_1, \cdots, m_r \in M m = i_1 m_1 + \cdots + i_r m_r\}$$

On vérifie sans peine que c'est un sous-A-module de M (on remarquera d'ailleurs que si M est un idéal J de A, on retrouve la définition de l'idéal produit IJ). Par construction, l'action de I sur le A-module quotient M/IM est nulle. La structure de A-module $A \longrightarrow \mathrm{End}_{\mathbb{Z}}(M/IM)$ se factorise donc par A/I, ce qui fait de M/IM un A/I-module.

Proposition. – *L'application $m \mapsto 1 \otimes m$ induit un isomorphisme de A/I-modules*

$$M/IM \xrightarrow{\sim} A/I \otimes_A M.$$

Démonstration. L'application ψ de l'énoncé est A-linéaire. Elle envoie un élément im sur $1 \otimes (im) = i(1 \otimes m) = (i.1) \otimes m$ dans $A/I \otimes_A M$. Or $i.1 = 0$ dans A/I, donc $\psi(im) = 0$ dans $A/I \otimes_A M$. Comme IM est engendré par les éléments de la forme im, on en déduit que $\psi(IM) = 0$ et que l'application de l'énoncé se factorise par le quotient M/IM en une application A-linéaire $\overline{\psi} : M/IM \longrightarrow A/I \otimes_A M$. Dans l'autre sens, partons de la projection $M \xrightarrow{m \mapsto \overline{m}} M/IM$. Elle appartient à $\mathrm{Hom}_A(M, M/IM)$ et la propriété universelle de l'extension des scalaires nous assure l'existence de $\varphi \in \mathrm{Hom}_{A/I}(A/I \otimes_A M, M/IM)$ tel que $\varphi(\overline{a} \otimes m) = \overline{a}.\overline{m}$. On a alors, pour tous $a \in A$ et $m \in M$, $\overline{\psi} \circ \varphi(\overline{a} \otimes m) = 1 \otimes am = a(1 \otimes m) = \overline{a} \otimes m$, et $\varphi \circ \overline{\psi}(\overline{m}) = \varphi(1 \otimes m) = \overline{m}$. Ceci montre que φ et $\overline{\psi}$ sont des bijections réciproques. Comme φ est A/I-linéaire, son inverse $\overline{\psi}$ l'est aussi. $\square$

Exemple. – Soit $A = \mathbb{Z}$, M un p-groupe abélien, et l un premier différent de p. Alors $\mathbb{Z}/l\mathbb{Z} \otimes_{\mathbb{Z}} M = 0$. En effet, le corollaire nous dit que que ce module est isomorphe à M/lM, mais la multiplication par l est surjective sur M puisque, si $m \in M$ est annulé par p^k et si $ul + vp^k = 1$, alors $lum = m$.

Exercice. – Soient I, J deux idéaux tels que $I + J = A$ et soit M un A-module annulé par $I \cap J$, c-à-d tel que $(I \cap J)M = 0$. Montrer que $M = IM \oplus JM$, que $IM \simeq M/JM$ et $JM \simeq M/IM$.

1.7.9 *Extension des scalaires par une localisation.* On s'intéresse ici au cas où $B = S^{-1}A$ pour une partie multiplicative $S \subset A$. Si M est un A-module, on peut construire un $S^{-1}A$-module $S^{-1}M$ de la même manière que pour construire $S^{-1}A$. On munit $M \times S$ de la relation d'équivalence $(m, s) \sim (m', s') \Leftrightarrow \exists t \in S, tsm' = ts'm$, et on note $\frac{m}{s}$ la classe d'équivalence de (m, s) dans l'ensemble quotient noté $S^{-1}M$. On vérifie alors qu'il existe une unique loi de groupe abélien sur $S^{-1}M$ telle que $\frac{m}{s} + \frac{m'}{s'} = \frac{s'm+s'm}{ss'}$, puis une unique action de $S^{-1}A$ telle que $\frac{a}{t} \cdot \frac{m}{s} = \frac{am}{ts}$. On appelle $S^{-1}M$ le “localisé de M selon S”.

Proposition. – *L'application $M \longrightarrow S^{-1}M$, $m \mapsto \frac{m}{1}$ induit un isomorphisme de $S^{-1}A$-modules*

$$S^{-1}A \otimes_A M \xrightarrow{\sim} S^{-1}M.$$

Démonstration. L'application de l'énoncé est A-linéaire puisqu'elle envoie am sur $\frac{am}{1} = \frac{a}{1} \cdot \frac{m}{1}$. Par la propriété universelle de l'extension des scalaires, on en déduit un morphisme de $S^{-1}A$-modules $\psi : S^{-1}A \otimes_A M \longrightarrow S^{-1}M$. Dans l'autre sens, on voudrait définir une application φ qui envoie $\frac{m}{s}$ sur $\frac{1}{s} \otimes m$. Pour voir que cela fait sens, soit $(m', s') \sim (m, s)$, et t tel que $tsm' = ts'm$. On a $\frac{1}{s'} \otimes m' = \frac{ts}{tss'} \otimes m' = ts(\frac{1}{tss'} \otimes m') = \frac{1}{tss'} \otimes tsm' = \frac{1}{tss'} \otimes ts'm = ts'(\frac{1}{tss'} \otimes m) = \frac{ts'}{tss'} \otimes m = \frac{1}{s} \otimes m$. Ceci montre que φ est bien définie. On laisse au lecteur le soin de vérifier que ψ et φ sont des bijections réciproques. $\square$

Remarque. – Avec les notations précédentes :

i) Si tout élément de M est annulé par un élément de S, alors $S^{-1}M = 0$. En effet, si m est annulé par t, alors pour tout s on a $\frac{m}{s} = \frac{mt}{st} = 0$.
Exemple : si M est un groupe abélien fini, $\mathbb{Q} \otimes_{\mathbb{Z}} M = 0$.

ii) Si tout élément de s agit bijectivement sur M, alors $S^{-1}M = M$. En effet, le noyau de l'application canonique $m \mapsto \frac{m}{1}$ est l'ensemble $\{m \in M, \exists t \in S, tm = 0\} = \{0\}$, et si on note s_M^{-1} la bijection réciproque (qui ne provient pas nécessairement de l'action d'un élément de A), on a $\frac{m}{s} = \frac{ss_M^{-1}(m)}{s} = \frac{s_M^{-1}(m)}{1}$, ce qui montre que cette application est surjective.
Exemple : $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}$.

Exemple. – Soit $A = \mathbb{Z}$ et M un groupe abélien fini. On sait que M est un produit $\prod_p M_p$ de p-sous-groupes abéliens finis, pour p premier (si on ne le sait pas, on le verra plus loin). Soit $\mathbb{Z}_{(p)}$ le localisé de $\mathbb{Z}$ en l'idéal premier (p) (ie selon la partie multiplicative S engendrée par les premiers $l \neq p$). Alors on a

$$\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} M \simeq M_p.$$

En effet, d'après le i) de la remarque précédente, on a $\mathbb{Z}_{(p)} \otimes M_l = 0$ pour $l \neq p$ car M_l est annulé par une puissance l^k qui est inversible dans S. Et d'après le ii) de la remarque, on a $\mathbb{Z}_{(p)} \otimes M_p = M_p$ puisque tous les $l \neq p$ agissent de manière inversible (avec pour inverse la multiplication par u où $ul + vp^k = 1$ et p^k annule M_p).

1.7.10 *Caractérisation tensorielle des A-algèbres.* Au paragraphe 1.3.3 nous avons remarqué que la donnée d'une A-algèbre (au sens d'un anneau B muni d'un morphisme $A \longrightarrow B$) est équivalente à celle d'un A-module muni d'une structure d'anneau dont la multiplication $B \times B \longrightarrow B$ est A-bilinéaire. Cette multiplication induit donc une application A-linéaire $\mu : B \otimes_A B \longrightarrow B$. Réciproquement, on peut se demander quelles propriétés une telle application μ doit avoir pour être la multiplication d'une A-algèbre.

PROPOSITION. – *Soit $\mu : B \otimes_A B \longrightarrow B$ un morphisme de A-modules. L'application $(b, b') \mapsto b \cdot b' := \mu(b \otimes b')$ fait de B une A-algèbre commutative d'unité 1_B si et seulement* *si les diagrammes suivants sont commutatifs :*

$$
\begin{tikzcd}
B \otimes_A B \otimes_A B \arrow[r, "\mu\otimes\mathrm{id}"] \arrow[d, "\mathrm{id}\otimes\mu"'] & B \otimes_A B \arrow[d, "\mu"] \\
B \otimes_A B \arrow[r, "\mu"'] & B,
\end{tikzcd}
\qquad
\begin{tikzcd}
B \otimes_A B \arrow[r, "\mu"] \arrow[d, "b\otimes b'\mapsto b'\otimes b"'] & B \arrow[d, equal, "\mathrm{id}"] \\
B \otimes_A B \arrow[r, "\mu"] & B
\end{tikzcd}
\qquad
\begin{tikzcd}
 & B \otimes_A B \arrow[dr, "\mu"] & \\
B \arrow[ur, "\mathrm{id}\otimes 1_B"] \arrow[rr, equal, "\mathrm{id}"] & & B
\end{tikzcd}
$$

Démonstration. La commutativité du premier diagramme signifie $\mu\circ(\mu\otimes\mathrm{id}) = \mu\circ(\mathrm{id}\otimes\mu) : B\otimes_A B\otimes_A B \longrightarrow B$. Elle est équivalente à l'assertion $\forall b, b', b'' \in N$, $(b\cdot b')\cdot b'' = b\cdot(b'\cdot b'')$, c'est-à-dire à l'*associativité* de la loi $(b, b') \mapsto \mu(b\otimes b')$. De même la commutativité du second diagramme est équivalente à la commutativité de la loi $(b, b') \mapsto \mu(b\otimes b')$, et celle du troisième diagramme dit que 1_B est élément neutre de cette loi. Quant à la distributivité par rapport à l'addition, elle est incluse dans la bilinéarité de l'application $(b, b') \mapsto \mu(b\otimes b')$. □

1.7.11 *Coproduit de A-algèbres.* On se donne ici deux A-algèbres B et C.

PROPOSITION. – *Il existe sur $B\otimes_A C$ une unique structure de A-algèbres telle que $(b\otimes c)(b'\otimes c') = bb'\otimes cc'$ pour tous $b, b' \in B$ et $c, c' \in C$.*

Démonstration. Encore une fois, l'unicité du produit découle du fait que les tenseurs élémentaires engendrent $B\otimes_A C$. Pour l'existence, notons $\mu^B : B\otimes_A B \longrightarrow B$ et $\mu^C : C\otimes_A C \longrightarrow C$ les morphismes donnant la multiplication de B et C, et considérons le morphisme

$$\mu^{B\otimes C} : (B\otimes_A C)\otimes(B\otimes_A C) \xrightarrow{\sim} (B\otimes_A B)\otimes_A(C\otimes_A C) \xrightarrow{\mu^B\otimes\mu^C} B\otimes_A C.$$

Il envoie $(b\otimes c)\otimes(b'\otimes c')$ sur $(b\otimes b')\otimes(c\otimes c)$, puis sur $(bb'\otimes cc')$. Pour voir que $\mu^{B\otimes C}$ définit une structure de A-algèbres sur $B\otimes_A C$, il faut vérifier la commutativité des diagrammes de la proposition précédente, laquelle découle péniblement mais sans difficulté de la commutativité des mêmes diagrammes pour μ^B et μ^C. □

Exercice. – Si M est un B-module et N un C-module, alors montrer qu'il existe une unique structure de $B\otimes_A C$-module sur $M\otimes_A N$ telle que l'action de $B\otimes_A C$ est donnée sur les tenseurs élémentaires par $(b\otimes c)\cdot(m\otimes n) = (bm\otimes cn)$.

Remarquons que les applications $B \xrightarrow{\mathrm{id}\otimes 1} B\otimes_A C$, $b\mapsto b\otimes 1$ et $C \xrightarrow{1\otimes\mathrm{id}} B\otimes_A C$, $c\mapsto 1\otimes c$ sont des morphismes de A-algèbres. La A-algèbres $B\otimes_A C$, munie de ces deux morphismes, satisfait la propriété universelle suivante :

PROPOSITION. – *Soit D une A-algèbre munie de deux morphismes d'algèbres $\eta : B \longrightarrow D$ et $\psi : C \longrightarrow D$, alors il existe un unique morphisme d'algèbres $B\otimes_A C \xrightarrow{\eta\cdot\psi} D$ tel que $\eta = (\eta\cdot\psi)\circ(\mathrm{id}\otimes 1)$ et $\psi = (\eta\cdot\psi)\circ(1\otimes\mathrm{id})$. De plus on a*

$$\eta\cdot\psi = \mu^D\circ(\eta\otimes\psi)$$

qui est donné sur les tenseurs élémentaires par $b \otimes c \mapsto \eta(b)\psi(c)$*. En d'autres termes, l'application* $\theta \mapsto (\theta \circ (\mathrm{id} \otimes 1), \theta \circ (1 \otimes \mathrm{id}))$ *est une bijection*

$$\mathrm{Hom}_{A-\mathrm{alg}}(B \otimes_A C, D) \xrightarrow{\sim} \mathrm{Hom}_{A-\mathrm{alg}}(B, D) \times \mathrm{Hom}_{A-\mathrm{alg}}(C, D)$$

dont l'inverse est donnée par $(\eta, \psi) \mapsto \eta \cdot \psi$*.*

On remarquera l'analogie avec la propriété universelle des sommes directes de modules, qu'on avait aussi appelées “coproduits de modules”.

Démonstration. On vérifie d'abord immédiatement que $\varphi \cdot \psi$ défini par $\mu^D \circ (\varphi \otimes \psi)$ est bien un morphisme d'algèbres, et qu'on a bien $\varphi = (\varphi \cdot \psi) \circ (\mathrm{id} \otimes 1)$ et $\psi = (\varphi \cdot \psi) \circ (1 \otimes \mathrm{id})$. Pour finir la preuve, il reste alors à voir que $(\theta \circ (\mathrm{id} \otimes 1)) \cdot (\theta \circ (1 \otimes \mathrm{id})) = \theta$. Il suffit de le faire sur les tenseurs élémentaires $b \otimes c$, or pour un tel tenseur on a $\theta(b \otimes c) = \theta((b \otimes 1)(1 \otimes c)) = \theta(b \otimes 1)\theta(1 \otimes c)$ comme voulu. □

Exemple. – Soient I et J deux idéaux de A. On a

$$A/I \otimes_A A/J \simeq A/(I + J).$$

En effet, soient $\pi^I : A/I \longrightarrow A/(I + J)$ et $\pi^J : A/J \longrightarrow A/(I + J)$ les projections canoniques. D'après la proposition elles fournissent un morphisme $\pi^I \cdot \pi^J : A/I \otimes_A A/J \longrightarrow A/(I+J)$ qui envoie $(a \bmod I) \otimes (b \bmod J)$ sur $(ab \bmod I + J)$. Dans l'autre sens, considérons l'application $\varphi : A \longrightarrow A/I \otimes_A A/J$ qui envoie a sur $\varphi(a) := a \cdot ((1 \bmod I) \otimes (1 \bmod J))$. D'un côté on a $\varphi(a) = (a \bmod I) \otimes (1 \bmod J)$, ce qui montre que $I \subset \mathrm{Ker}(\varphi)$. De l'autre côté on a aussi $\varphi(a) = (1 \bmod J) \otimes (a \bmod J)$, ce qui montre que $J \subset \mathrm{Ker}(\varphi)$. On a donc $I + J \subset \mathrm{Ker}(\varphi)$ et par conséquent φ se factorise par un morphisme A-linéaire $\overline{\varphi} : A/(I + J) \longrightarrow A/I \otimes_A A/J$. Par construction on a

- $(\pi^I \cdot \pi^J) \circ \overline{\varphi}(a \bmod I + J) = (\pi^I \cdot \pi^J)(a \cdot ((1 \bmod I) \otimes (1 \bmod J)) = a \cdot (1 \bmod I + J) = a \bmod I + J$
- $\overline{\varphi} \circ (\pi^I \cdot \pi^{j)}((a \bmod I) \otimes (b \bmod J)) = \varphi(ab \bmod I + J) = ab \cdot (1 \bmod I) \otimes (1 \bmod J) = a \cdot (1 \bmod I) \otimes (b \bmod J) = (a \bmod I) \otimes (b \bmod J)$,

donc $\overline{\varphi}$ et $\pi^I \cdot \pi^J$ sont inverses l'un de l'autre.

Exemple. – L'unique morphisme de A-algèbres qui envoie X_1 sur $X_1 \otimes 1$ et X_2 sur $1 \otimes X_2$ est un isomorphisme

$$A[X_1, X_2] \xrightarrow{\sim} A[X_1] \otimes_A A[X_2]$$

dont l'inverse est donné par le morphisme $\iota_1 \cdot \iota_2$ où ι_i est l'inclusion $A[X_i] \hookrightarrow A[X_1, X_2]$. Plus généralement, si $\mathcal{N}_1$ et $\mathcal{N}_2$ sont des monoïdes commutatifs, on a un isomorphisme

$$A[\mathcal{N}_1 \times \mathcal{N}_2] \xrightarrow{\sim} A[\mathcal{N}_1] \otimes_A A[\mathcal{N}_2]$$

déterminé par la condition $e_{(n_1,n_2)} \mapsto e_{n_1} \otimes e_{n_2}$ et dont l'inverse est donné par $\iota_1 \cdot \iota_2$ où $\iota_1 : A[\mathcal{N}_1] \longrightarrow A[\mathcal{N}_1 \times \mathcal{N}_2]$ est déterminé par $e_{n_1} \mapsto e_{(n_1,0)}$ et $\iota_2 : A[\mathcal{N}_2] \longrightarrow A[\mathcal{N}_1 \times \mathcal{N}_2]$ est déterminé par $e_{n_2} \mapsto e_{(0,n_2)}$.

Exemple. (Interprétation géométrique) – L'exemple précédent nous fournit un isomorphisme de $\mathbb{C}$-algèbres $\mathcal{O}(\mathbb{C}^{n_1}) \otimes_{\mathbb{C}} \mathcal{O}(\mathbb{C}^{n_2}) \xrightarrow{\sim} \mathcal{O}(\mathbb{C}^{n_1+n_2})$ qui, en termes de fonctions, envoie $f_1 \otimes f_2$ sur la fonction $(z_1, z_2) \mapsto f_1(z_1)f_2(z_2)$ où $z_1 \in \mathbb{C}^{n_1}$ et $z_2 \in \mathbb{C}^{n_2}$. Plus généralement, si $V_i \subset \mathbb{C}^{n_i}$ est un sous-ensemble algébrique, alors $V_1 \times V_2$ est un sous-ensemble algébrique de $\mathbb{C}^{n_1+n_2}$ et la proposition ci-dessus nous fournit un morphisme de $\mathbb{C}$-algèbres

$$\Psi_{V_1,V_2} : \mathcal{O}(V_1) \otimes_{\mathbb{C}} \mathcal{O}(V_2) \longrightarrow \mathcal{O}(V_1 \times V_2)$$

donné par la même formule sur les fonctions. Si π_{V_i} désigne la surjection $\mathcal{O}(\mathbb{C}^{n_i}) \twoheadrightarrow \mathcal{O}(V_i)$ (donnée par restriction des fonctions), l'égalité $\Psi_{V_1,V_2} \circ (\pi_{V_1} \otimes \pi_{V_2}) = \pi_{V_1 \times V_2} \circ \Psi_{\mathbb{C}^{n_1},\mathbb{C}^{n_2}}$ montre que Ψ_{V_1,V_2} est surjective. Montrons qu'elle est aussi injective. Choisissons pour cela une $\mathbb{C}$-base $(\varepsilon_i)_{i\in I}$ de $\mathcal{O}(V_2)$. Alors un élément $F \in \mathcal{O}(V_1) \otimes_{\mathbb{C}} \mathcal{O}(V_2)$ s'écrit de manière unique $F = \sum_{i\in I} f_i \otimes \varepsilon_i$ où $f_i \in \mathcal{O}(V_1)$ (et est nul sauf pour un nombre fini de i dans I). Si $\Psi_{V_1,V_2}(F) = 0$, alors pour tout $v_1 \in V_1$, la fonction $\sum_{i\in I} f_i(v_1)\varepsilon_i$ est nulle sur V_2, donc chaque $f_i(v_1)$ est nul, puisque les ε_i forment une base de $\mathcal{O}(V_2)$. Comme v_1 est arbitraire, il s'ensuit que $f_i = 0$ pour tout i et finalement $F = 0$.

Remarque. – Si on part de deux sous-ensembles algébriques $V_1, V_2 \subset \mathbb{C}^n$ d'idéaux annulateurs respectifs $I_1, I_2 \subset \mathcal{O}(\mathbb{C}^n)$. Alors l'idéal $I_1 + I_2$ annule l'ensemble algébrique $V_1 \cap V_2$ et le premier exemple ci-dessus nous fournit donc un morphisme surjectif

$$\mathcal{O}(V_1) \otimes_{\mathcal{O}(\mathbb{C}^n)} \mathcal{O}(V_2) \twoheadrightarrow \mathcal{O}(V_1 \cap V_2).$$

On peut montrer que l'idéal annulateur de $V_1 \cap V_2$ est le radical de $I_1 + I_2$, ce qui équivaut à dire que le noyau du morphisme ci-dessus est le nilradical de $\mathcal{O}(V_1) \otimes_{\mathcal{O}(\mathbb{C}^n)} \mathcal{O}(V_2)$. La présence de nilpotents dans cette algèbre est liée à la non-transversalité de l'intersection. Par exemple dans $\mathbb{C}^2$, si V_1 est la parabole d'idéal $(Y - X^2)$ et V_2 la droite d'idéal (Y), alors $I_1 + I_2 = (X^2, Y)$ n'est pas radiciel puisque $X \notin I_1 + I_2$.

Revenons aux notations générales. Si on voit maintenant $B \otimes_A C$ comme une B-algèbre via l'homomorphisme $\mathrm{id} \otimes 1$, alors celle-ci satisfait la propriété universelle suivante :

COROLLAIRE. – *Pour toute B-algèbre D, l'application $\varphi \mapsto (\psi_\varphi : c \mapsto \varphi(1 \otimes c))$ est une bijection*

$$\mathrm{Hom}_{B-\mathrm{alg}}(B \otimes_A C, D) \xrightarrow{\sim} \mathrm{Hom}_{A-\mathrm{alg}}(C, D)$$

dont l'inverse est donné par $\psi \mapsto \varphi_\psi : b \otimes c \mapsto b\psi(c)$.

Démonstration. On peut déduire ce résultat de deux manières :
- Soit à partir de la proposition précédente dans laquelle on fixe η comme étant celui qui donne la structure de B-algèbre de D.
- Soit à partir de la deuxième proposition de 1.7.6 appliquée à $M = D$ et $N = C$ en remarquant que la bijection $\mathrm{Hom}_B(B \otimes_A C, D) \xrightarrow{\sim} \mathrm{Hom}_A(C, D)$ envoie morphismes multiplicatifs sur morphismes multiplicatifs.

□

Exemple. – L'unique morphisme de A-algèbres qui envoie X sur $1 \otimes X$ est un isomorphisme
$$A[X] \xrightarrow{\sim} A \otimes_{\mathbb{Z}} \mathbb{Z}[X]$$
dont l'inverse est donné par le morphisme $\iota \cdot \kappa$ où $\iota : A \longrightarrow A[X]$ est l'injection canonique et $\mathbb{Z}[X] \longrightarrow A[X]$ est l'unique morphisme d'anneaux qui envoie X sur X. Plus généralement, si $\mathcal{N}$ est un monoïde, on a un isomorphisme
$$A[\mathcal{N}] \xrightarrow{\sim} A \otimes_{\mathbb{Z}} \mathbb{Z}[\mathcal{N}].$$

Exemple. – Soit B une A-algèbre, I un idéal de A et IB l'idéal engendré par l'image de I dans B. Alors on a un isomorphisme de B-algèbres
$$B \otimes_A (A/I) \xrightarrow{\sim} B/IB$$
donné par $\pi \cdot \iota$ où π est la projection $B \longrightarrow B/IB$ et $\iota : A/I \longrightarrow B/IB$ est déduit par passage au quotient de $A \longrightarrow B \longrightarrow B/IB$. Pour construire l'inverse, on part de $\mathrm{id} \otimes 1 : B \longrightarrow B \otimes_A (A/I)$, qui envoie b sur $b \otimes (1 \mathrm{mod} I)$. On remarque que ce morphisme de B-algèbres envoie ib sur $ib \otimes (1 \mathrm{mod} I) = b \otimes (i \mathrm{mod} I) = b \otimes 0 = 0$. Donc il se factorise par un morphisme $B/IB \longrightarrow B \otimes_A (A/I)$ qui est l'inverse cherché.

Exemple. – On a un isomorphisme
$$\varphi : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \xrightarrow{\sim} \mathbb{C} \times \mathbb{C}$$
qui envoie $z_1 \otimes z_2$ sur $(z_1 z_2, z_1 \bar{z}_2)$. Pour vérifier qu'il est bien défini on peut utiliser la proposition et remarquer que $\varphi = \varphi_1 \cdot \varphi_2$ où $\varphi_i : \mathbb{C} \longrightarrow \mathbb{C} \times \mathbb{C}$ est défini par $\varphi_1(z) = (z, z)$ et $\varphi_2(z) = (z, \bar{z})$. On remarque que $\varphi(z \otimes 1) = (z, z)$ et $\varphi(iz \otimes i) = (-z, z)$. On en déduit que φ est surjectif, et par égalité des dimensions (sur $\mathbb{C}$ ou sur $\mathbb{R}$) qu'il est bijectif. Plus précisément, son inverse envoie (z, z') sur $\frac{1}{2}(z \otimes 1 - iz \otimes i + z' \otimes 1 + iz' \otimes i)$.

Voici une autre façon de voir cet isomorphisme. Partons de l'isomorphisme de $\mathbb{R}$-algèbres $\mathbb{R}[X]/(X^2+1) \xrightarrow{\sim} \mathbb{C}$ qui envoie X sur i. Alors on a
$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} &\simeq \mathbb{C} \otimes_{\mathbb{R}} (\mathbb{R}[X]/(X^2+1)) = \mathbb{C} \otimes_{\mathbb{R}} (\mathbb{R}[X] \otimes_{\mathbb{R}[X]} (\mathbb{R}[X]/(X^2+1))) \\ &= (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[X]) \otimes_{\mathbb{R}[X]} (\mathbb{R}[X]/(X^2+1)) = \mathbb{C}[X]/(X^2+1) \\ &= \mathbb{C}[X]/((X-i)(X+i)) = \mathbb{C}[X]/(X-i) \times \mathbb{C}[X]/(X+i) \simeq \mathbb{C} \times \mathbb{C}. \end{aligned}$$
On a utilisé les exemples précédents à la première ligne et les restes chinois à la deuxième. Si on veut expliciter cette suite d'isomorphismes, on constate qu'elle envoie $z \otimes 1$ sur (z, z) (car chaque isomorphisme est $\mathbb{C}$-linéaire), et que, en écrivant $z = a + ib$, elle envoie $1 \otimes z$ sur $((a + Xb) \bmod (X - i), (a + Xb) \bmod (X + i)) = (a + ib, a - ib) = (z, \bar{z})$. On retrouve donc bien l'isomorphisme précédent.

Exemple. – Essayons de généraliser l'exemple précédent en partant d'un corps K de dimension finie sur $\mathbb{Q}$ et en regardant la $\mathbb{C}$-algèbre $\mathbb{C} \otimes_{\mathbb{Q}} K$. Appelons *plongement* de K dans

$\mathbb{C}$ tout morphisme de corps $\sigma : K \longrightarrow \mathbb{C}$. Notons qu'un tel morphisme est automatiquement $\mathbb{Q}$-linéaire, donc n'est rien d'autre qu'un morphisme de $\mathbb{Q}$-algèbres. Le produit de tous ces plongements est un morphisme de $\mathbb{Q}$-algèbres $K \longrightarrow \prod_{\sigma:K\hookrightarrow\mathbb{C}} \mathbb{C}$. Comme le terme de droite est une $\mathbb{C}$-algèbre, le corollaire ci-dessus fournit un morphisme de $\mathbb{C}$-algèbres

$$(*) \quad \mathbb{C} \otimes_{\mathbb{Q}} K \longrightarrow \prod_{\sigma\colon K\hookrightarrow\mathbb{C}} \mathbb{C}$$

qui envoie $z \otimes x$ sur $(z\sigma(x))_{\sigma:K\hookrightarrow\mathbb{C}}$. Nous montrerons plus tard que le corps K peut être engendré, en tant que $\mathbb{Q}$-algèbre, par un élément α (qui est loin d'être unique). Ceci signifie que l'unique morphisme de $\mathbb{Q}$-algèbres $\mathbb{Q}[X] \longrightarrow K$ qui envoie X sur α est surjectif. Notons I son noyau. Comme $\mathbb{Q}[X]$ est principal, il existe un unique polynôme unitaire $f \in \mathbb{Q}[X]$ tel que $I = (f)$. On a donc un isomorphisme

$$\mathbb{Q}[X]/(f) \xrightarrow{\sim} K, \;\; X \mapsto \alpha$$

qui montre d'après le deuxième corollaire de 1.4.3 que $\deg(f) = \dim_{\mathbb{Q}}(K) =: n$ et que $(1, \alpha, \cdots, \alpha^{n-1})$ est une $\mathbb{Q}$-base de K. Ceci nous permet de calculer

$$\mathbb{C} \otimes_{\mathbb{Q}} K \simeq \mathbb{C} \otimes_{\mathbb{Q}} (\mathbb{Q}[X]/(f)) = \mathbb{C} \otimes_{\mathbb{Q}} \mathbb{Q}[X] \otimes_{\mathbb{Q}[X]} (\mathbb{Q}[X]/(f)) = \mathbb{C}[X]/(f).$$

Nous montrerons aussi que f se factorise en $f = (X - \alpha_1)\cdots(X - \alpha_n)$ dans $\mathbb{C}[X]$, avec $\alpha_1, \cdots, \alpha_n$ distincts 2 à 2 dans $\mathbb{C}$. Le théorème des restes chinois nous assure alors que

$$\mathbb{C}[X]/(f) = \mathbb{C}[X]/(X - \alpha_1) \times \cdots \times \mathbb{C}[X]/(X - \alpha_n) = \mathbb{C}^n.$$

Explicitons l'isomorphisme

$$(**) \quad \mathbb{C} \otimes_{\mathbb{Q}} K \xrightarrow{\sim} \mathbb{C}^n$$

ainsi obtenu. Il envoie $z \otimes 1$ sur $(z, z, \cdots, z)$ puisqu'il est $\mathbb{C}$-linéaire. Par ailleurs, on a vu que $(1, \alpha, \cdots, \alpha^{n-1})$ est une $\mathbb{Q}$-base de K, donc on peut écrire un élement $x \in K$ sous la forme $x = g(\alpha)$ pour un unique polynôme $g(X) \in \mathbb{Q}[X]$ de degré $< n$. On constate alors que l'isomorphisme ci-dessus envoie $1 \otimes x$ sur $(g(X)\mathrm{mod}(X - \alpha_1), \cdots, g(X)\mathrm{mod}(X - \alpha_n))$ qui n'est autre que $(g(\alpha_1), g(\alpha_2), \cdots, g(\alpha_n)) \in \mathbb{C}^n$.

Quel rapport entre $(*)$ et $(**)$? Se donner un plongement de $K = \mathbb{Q}[X]/(f)$ dans $\mathbb{C}$ revient à se donner l'image de $X = \alpha$ dans $\mathbb{C}$ et celle-ci doit annuler f, donc appartenir à $\{\alpha_1, \cdots, \alpha_n\}$. On a donc une bijection $\sigma \mapsto \sigma(\alpha)$ entre $\{\sigma : K \hookrightarrow \mathbb{C}\}$ et $\{\text{racines de } f\}$. Notons σ_i le plongement tel que $\sigma_i(\alpha) = \alpha_i$. Alors pour tout $x = g(\alpha)$ comme ci-dessus, on a $\sigma_i(x) = \sigma_i(g(\alpha)) = g(\sigma_i(\alpha)) = g(\alpha_i)$. Ainsi, si l'on réécrit le morphisme $(*)$ sous la forme

$$\mathbb{C} \otimes_{\mathbb{Q}} K \longrightarrow \mathbb{C}^n, \;\; z \otimes x \mapsto (z\sigma_1(x), \cdots, z\sigma_n(x)),$$

on constate que $(**)$ et $(*)$ sont les même morphismes, et on en déduit du coup que $(*)$ est un isomorphisme.

Exemple. – Reprenons l'exemple précédent, mais calculons cette fois la $\mathbb{R}$-algèbre $\mathbb{R} \otimes_{\mathbb{Q}} K$. Avec les mêmes notations, on a $\mathbb{R} \otimes_{\mathbb{Q}} K \simeq \mathbb{R}[X]/(f)$, mais cette fois f n'est pas scindé. Soit r le nombre de racines réelles de f et $2s$ le nombre de racines non réelles (chacune vient avec sa conjuguée, donc il y en a un nombre pair). On a $n = r + 2s$. Numérotons les racines de sorte que $\alpha_1, \cdots, \alpha_r$ soient les racines réelles, et $\alpha_{r+1}, \cdots, \alpha_n$ les non réelles, avec en plus la relation $\alpha_{r+s+i} = \bar{\alpha}_{r+i}$ pour $i = 1, \cdots, s$. On a alors la factorisation en éléments irréductibles de $\mathbb{R}[X]$

$$f = f_1 \cdots f_{r+s} \quad \text{avec } f_i = \begin{cases} X - \alpha_i & \text{si } i \leqslant r \\ X^2 - 2\Re(\alpha_i) + |\alpha_i|^2 & \text{si } i > r \end{cases}$$

Comme les f_i sont 2 à 2 premiers entre eux, le théorème des restes chinois nous donne donc un isomorphisme

$$\mathbb{R} \otimes_{\mathbb{Q}} K \xrightarrow{\sim} \prod_{i=1}^{r+s} \mathbb{R}[X]/(f_i) = \mathbb{R}^r \times \mathbb{C}^s.$$

Explicitement, cet isomorphisme est toujours donné par $y \otimes 1 \mapsto (y, \cdots, y)$ et $1 \otimes x \mapsto (g(\alpha_1), \cdots, g(\alpha_{r+s}))$ si $x = g(\alpha)$ avec $\deg(g) < n$. En termes de plongements, il envoie $1 \otimes x$ sur $(\sigma_1(x), \cdots, \sigma_{r+s}(x))$ (remarquer que pour $i \leqslant r$, $\sigma_i(K) \subset \mathbb{R}$).

Remarquons maintenant que, en composant avec la conjugaison complexe, on obtient une permutation involutive (ie d'ordre 2) de l'ensemble des plongements $\{\sigma : K \hookrightarrow \mathbb{C}\}$ et que l'ensemble $\Sigma := \{\sigma_1, \cdots, \sigma_{r+s}\}$ est un ensemble de représentants des classes de conjugaison de plongements. On écrit parfois l'isomorphisme sous la forme suivante :

$$\mathbb{R} \otimes_{\mathbb{Q}} K \xrightarrow{\sim} \prod_{\sigma \in \Sigma} \mathbb{R}_\sigma$$

où Σ où, par convention, $\mathbb{R}_\sigma$ vaut $\mathbb{R}$ si σ est réelle et $\mathbb{C}$ sinon.

1.8 Quelques conséquences du lemme chinois

Dans cette section, A est un anneau commutatif général.

1.8.1 LEMME.– *Soit I un idéal de la forme $I = \mathfrak{m}_1^{v_1}\mathfrak{m}_2^{v_2} \cdots \mathfrak{m}_r^{v_r}$ avec $\mathfrak{m}_1, \cdots, \mathfrak{m}_r$ maximaux deux à deux distincts. Alors le produit des projections canoniques est un isomorphisme de A-algèbres*

$$A/I \xrightarrow{\sim} A/\mathfrak{m}_1^{v_1} \times \cdots \times A/\mathfrak{m}_r^{v_r}.$$

Démonstration. Nous avons déjà démontré une version du théorème des restes chinois sous la forme :

$$J + K = A \text{ implique } A/(J \cap K) \xrightarrow{\sim} A/J \times A/K.$$

Remarquons que JK est toujours inclus dans $J \cap K$ et lui est égal si $J + K = A$, puisque dans ce cas on a $(J \cap K) = (J \cap K) \cdot J + (J \cap K) \cdot K \subset JK$. On peut donc l'énoncer sous la forme

$$J+K=A \text{ implique } A/JK \xrightarrow{\sim} A/J\times A/K.$$

Montrons que $\mathfrak{m}_1^{v_1}+(\mathfrak{m}_2^{v_2}\cdots\mathfrak{m}_r^{v_r})=A$. Ceci montrera que $A/I\simeq A/\mathfrak{m}_1^{v_1}\times A/\mathfrak{m}_2^{v_2}\cdots\mathfrak{m}_r^{v_r}$ et le lemme en découlera par récurrence sur r. Puisque $\mathfrak{m}_1$ et $\mathfrak{m}_i$, $i\neq 1$ sont maximaux et distincts, on a $\mathfrak{m}_1+\mathfrak{m}_i=A$ pour $i>1$. Il s'ensuit que

$$A=(\mathfrak{m}_1+\mathfrak{m}_i)^{v_i}\subset \mathfrak{m}_1^{v_i}+\mathfrak{m}_1^{v_i-1}\mathfrak{m}_i+\cdots+\mathfrak{m}_1\mathfrak{m}_i^{v_i-1}+\mathfrak{m}_i^{v_i}\subset\mathfrak{m}_1+\mathfrak{m}_i^{v_i},$$

donc $A=\mathfrak{m}_1+\mathfrak{m}_i^{v_i}$. De même $A=(\mathfrak{m}_1+\mathfrak{m}_i^{v_i})^{v_1}\subset\mathfrak{m}_1^{v_1}+\mathfrak{m}_i^{v_i}=A$. Enfin,

$$A=(\mathfrak{m}_1^{v_1}+\mathfrak{m}_2^{v_2})(\mathfrak{m}_1^{v_1}+\mathfrak{m}_3^{v_3})\cdots(\mathfrak{m}_1^{v_1}+\mathfrak{m}_r^{v_r})\subset\mathfrak{m}_1^{v_1}+(\mathfrak{m}_2^{v_2}\mathfrak{m}_3^{v_3}\cdots\mathfrak{m}_r^{v_r})$$

comme voulu. □

Notation. – Pour un A-module M et un idéal I de A on note

$$\begin{aligned}&M[I]:=\{m\in M,\forall i\in I, im=0\}\quad\text{et}\\&M[I^\infty]:=\bigcup_{n\in\mathbb{N}}M[I^n]=\{m\in M,\exists n\in\mathbb{N},\forall i_1,\cdots,i_n\in I,\ i_1\cdots i_n m=0\}\end{aligned}$$

Ce sont des sous-A-modules de M. On dit que M est "annulé par I" si $IM=0$, ce qui équivaut donc à $M[I]=M$.

Rappelons aussi qu'on note $\mathrm{Max}(A)$ l'ensemble des idéaux maximaux de A.

1.8.2 Théorème.– *Soit A un anneau commutatif et M un A-module annulé par un produit fini d'idéaux maximaux.*

i) Pour tout $\mathfrak{m}\in\mathrm{Max}(A)$ on a $M[\mathfrak{m}^\infty]\simeq M_{\mathfrak{m}}$ et $\{\mathfrak{m}\in\mathrm{Max}(A), M_{\mathfrak{m}}\neq 0\}$ est fini.

ii) On a $M=\bigoplus_{\mathfrak{m}\in\mathrm{Max}(A)}M[\mathfrak{m}^\infty]\simeq\prod_{\mathfrak{m}}M_{\mathfrak{m}}$.

Démonstration. Par hypothèse, M est annulé par un idéal de la forme $I=\mathfrak{m}_1^{v_1}\cdots\mathfrak{m}_r^{v_r}$ avec les $\mathfrak{m}_i$ maximaux et 2 à 2 distincts. D'après le lemme ci-dessus et l'égalité $IM=0$, on a la décomposition suivante de M :

$$(*)\quad M=M/IM\simeq(A/I)\otimes_A M\simeq\prod_{i=1}^r(A/\mathfrak{m}_i^{v_i})\otimes_A M=\prod_{i=1}^r M/\mathfrak{m}_i^{v_i}M.$$

Remarquons maintenant que si les points i) et ii) sont vrais pour M et M' à support fini, alors ils le sont aussi pour $M\oplus M'$, qui est clairement à support fini aussi. D'après la décomposition $(*)$ on peut donc supposer que I est de la forme $\mathfrak{n}^v$ pour un $\mathfrak{n}\in\mathrm{Max}(A)$.

Supposons d'abord que $\mathfrak{m}\neq\mathfrak{n}$. On a vu dans le lemme précédent que $\mathfrak{m}+\mathfrak{n}^v=A$, choisissons donc $p\in\mathfrak{m}$ et $q\in\mathfrak{n}^v$ tels que $p+q=1$. Alors $p\in\mathfrak{m}$ agit par l'identité sur M donc $M[\mathfrak{m}^\infty]=0$. De plus, q annule M mais $q\in A\setminus\mathfrak{m}$, donc $M_{\mathfrak{m}}=0$. Donc les deux modules $M[\mathfrak{m}^\infty]$ et $M_{\mathfrak{m}}$ sont bien isomorphes et en fait nuls, ce qui montre aussi que l'ensemble considéré dans le i) possède au plus un élément.

Supposons maintenant $\mathfrak{m} = \mathfrak{n}$. Puisque $\mathfrak{n}^v$ annule M, on a $M = M[\mathfrak{n}^\infty] = M[\mathfrak{n}^v] = M/\mathfrak{n}^v M$. Pour montrer que $M \xrightarrow{\sim} M_\mathfrak{n}$ il faut voir que tout $x \in A \setminus \mathfrak{n}$ agit de manière inversible sur M. Or, pour un tel x, on a $(x) + \mathfrak{n} = A$ par maximalité de $\mathfrak{n}$. Donc, comme dans la preuve du lemme précédent, on a $(x) + \mathfrak{n}^\nu = A$ d'où l'existence de $y \in A$ et $q \in \mathfrak{n}^v$ tels que $xy + q = 1$. Comme q annule M, l'action de x sur M est donc inversible, et son inverse est l'action de y. $\square$

Remarque. – Si M est annulé par $\mathfrak{m}_1^{v_1} \cdots \mathfrak{m}_r^{v_r}$ avec les $\mathfrak{m}_i$ maximaux et 2 à 2 distincts, la décomposition du théorème s'écrit plus précisément

$$M = M[\mathfrak{m}_1^{v_1}] \oplus \cdots \oplus M[\mathfrak{m}_r^{v_r}] \simeq M_{\mathfrak{m}_1} \times \cdots \times M_{\mathfrak{m}_r}.$$

1.8.3 *Exemple*– Supposons que $A = K[X]$ et M est un A-module qui est de dimension finie en tant que K-espace vectoriel. Ainsi l'action de X sur M est donnée par un endomorphisme K-linéaire u de M. Si $f_u \in K[X]$ désigne le polynôme minimal de u, alors par définition l'idéal (f_u) annule le $K[X]$-module M. Cet idéal est produit d'idéaux maximaux puisque $K[X]$ est principal. Ecrivons plus précisément $f_u = \prod_{i=1}^r f_i^{v_i}$ pour des $f_i \in K[X]$ irréductibles deux à deux distincts. Chaque f_i engendre un idéal maximal $\mathfrak{m}_i$ et on a $(f_u) = \prod_{i=1}^r \mathfrak{m}_i^{v_i}$, et $M[\mathfrak{m}_i^{v_i}] = \mathrm{Ker}(f_i^{v_i})$. Ainsi la décomposition ci-dessus n'est autre que celle donnée par le “lemme des noyaux” $M = \bigoplus_i \mathrm{Ker}(f_i^{v_i})$. Lorsque K est algébriquement clos, on a $f_i = X - \lambda_i$ et les λ_i sont les valeurs propres de u, tandis que $M[\mathfrak{m}_i^{v_i}] = \mathrm{Ker}((u - \lambda_i)^{v_i})$ est le sous-espace caractéristique associé à λ_i, de sorte que la décomposition ci-dessus n'est autre que la décomposition de M en somme de sous-espaces caractéristiques.

1.8.4 *Modules de longueur finie.* Voici un exemple important où les hypothèses du théorème sont satisfaites.

DÉFINITION. – *Soit M un A-module et soit L l'ensemble des entiers $n \in \mathbb{N}$ tels que il existe une chaîne strictement croissante de sous-modules $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$. On note $\ell(M) := \mathrm{Sup}(L) \in \mathbb{N} \cup \{\infty\}$ et on l'appelle* longueur de M.

Exemple. – On a $\ell(M) = 1$ si et seulement si M est non nul et ses seuls sous-modules sont $\{0\}$ et M. On dit alors que M est un *A-module simple.*

Remarque. – Si M est de longueur n, alors pour toute chaîne $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$, les modules M_i/M_{i-1} sont simples pour tout $i = 1, \cdots, n$.

DÉFINITION. – *Si M est un A-module, l'*annulateur *d'un élément $m \in M$ est le sous-ensemble*

$$\mathrm{Ann}_A(m) := \{a \in A, am = 0\}.$$

C'est un idéal de A. L'annulateur $\mathrm{Ann}_A(M)$ de M est alors l'idéal

$$\mathrm{Ann}_A(M) := \bigcap_{m \in M} \mathrm{Ann}_A(m) = \{a \in A, aM = 0\}.$$

Lemme. – *L'annulateur d'un module simple est un idéal maximal. Un module de longueur finie est annulé par un produit fini d'idéaux maximaux.*

Démonstration. Si M est simple et $m \in M\backslash\{0\}$, alors $Am = M$ et le morphisme $A \overset{a \mapsto am}{\longrightarrow} M$ induit un isomorphisme $A/\mathrm{Ann}_A(m) \overset{\sim}{\longrightarrow} M$. Puisque M est simple, l'anneau quotient $A/\mathrm{Ann}_A(m)$ n'a pas d'idéaux propres non nuls, donc est un corps, donc $\mathrm{Ann}_A(m)$ est un idéal maximal. Soit maintenant M un A-module quelconque. Remarquons que pour un sous-module N de M, si I annule N et J annule M/N alors IJ annule M. En effet, l'action de $j \in J$ est nulle sur M/N donc $jM \subset N$, et donc $ijM \subset iN = 0$. Il s'ensuit par une récurrence immédiate que si on a une filtration $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ et si I_i annule M_i/M_{i-1} pour $i = 1, \cdots, n$, alors $I_1 I_2 \cdots I_n$ annule M. Lorsque M est de longueur finie, on en déduit la seconde assertion de l'énoncé. □

Remarque. – Les applications $M \mapsto \mathrm{Ann}_A(M)$ et $\mathfrak{m} \mapsto A/\mathfrak{m}$ établissent une bijection entre modules simples à isomorphisme près et idéaux maximaux. Par ailleurs, l'exemple $A = \mathbb{C}[X,Y]$ et $M = A/(X^2, Y)$ montre que l'annulateur d'un module de longueur finie n'est pas nécessairement un produit d'idéaux maximaux.

Corollaire. – *Le théorème 1.8.2 s'applique à tout module de longueur finie.*

Exemple. – Tout groupe abélien fini M est un $\mathbb{Z}$-module de longueur finie (on le voit par récurrence sur le cardinal par exemple). Un groupe abélien fini est donc canoniquement produit (fini) $M = \prod_p M[p^\infty]$ de ses p-sous-groupes maximaux.

Le lemme suivant est utile pour faire des raisonnements par récurrence sur la longueur.

Lemme. – *Soient $N \subset M$ deux A-modules. Alors M est de longueur finie si et seulement si N et M/N le sont, et dans ce cas on a $\ell(M) = \ell(N) + \ell(M/N)$.*

Démonstration. Soient $0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_r = N$ une chaîne strictement croissante dans N et $0 \subsetneq \overline{M}_1 \subsetneq \cdots \subsetneq \overline{M}_s = M/N$ une chaîne strictement croissante dans M/N. Posons $M_i := N_i$ si $i = 0, \cdots, r$ et $M_{r+i} := \pi^{-1}(\overline{M}_i)$ pour $i = 1, \cdots s$, où π est la projection $M \longrightarrow M/N$. On obtient une chaîne strictement croissante de longueur $r + s$. Ceci prouve que $\ell(M) \geqslant \ell(N) + \ell(M/N)$.

Soit maintenant $0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ une chaîne strictement croissante dans M. Posons $N_i := M_i \cap N$ et $\overline{M}_i := \pi(M_i)$. On obtient deux chaînes croissantes, mais en général pas strictement croissantes. Néanmoins, la suite exacte $N_{i+1}/N_i \hookrightarrow M_{i+1}/M_i \twoheadrightarrow \overline{M}_{i+1}/\overline{M}_i$ montre que pour tout i, on a $N_i \subsetneq N_{i+1}$ ou $\overline{M}_i \subsetneq \overline{M}_{i+1}$. Il s'ensuit que si r et s désignent les longueurs des chaînes strictement croissantes obtenues en ne gardant que les sauts, on a $r + s \geqslant n$. On a donc $\ell(N) + \ell(M/N) \geqslant \ell(M)$. □

Exercice. – Si M est de longueur finie, montrer que toute chaîne strictement croissante maximale est de longueur $\ell(M)$.

Exercice. – On dit qu'un module est *artinien* si toute suite décroissante de sous-modules est stationnaire. Montrer qu'un module artinien et noethérien est de longueur finie.

1.8.5 *Application aux algèbres de dimension finie.* Voici un cas particulier important du corollaire ci-dessus. Supposons que A soit une K-algèbre sur un corps K, et soit M un A-module qui est de dimension finie. Alors M est de longueur finie. En effet, toute suite strictement croissante $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ est de "longueur" n inférieure à $\dim_K(M)$, donc on peut en prendre une de "longueur" n maximale, et les quotients successifs d'une telle suite sont nécessairement simples.

Corollaire. – *Soit A une algèbre commutative de dimension finie sur un corps K. Alors* $\mathrm{Max}(A)$ *est fini et A est produit de ses localisées en ses idéaux maximaux :*

$$A \xrightarrow{\sim} \prod_{\mathfrak{m} \in \mathrm{Max}(A)} A_{\mathfrak{m}}.$$

Démonstration. C'est le cas $M = A$ de ce qui précède. □

Exemple. – Soit $A = \mathbb{C}[X]/(f)$ où f est unitaire. Factorisons $f = \prod_{i=1}^{r}(X - z_i)^{v_i}$. Le théorème des restes chinois nous donne $A \xrightarrow{\sim} \mathbb{C}[X]/(X - f_1)^{v_1} \times \cdots \times \mathbb{C}[X]/(X - f_r)^{v_r}$. Les idéaux maximaux de A sont les $\mathfrak{m}_i$, $i = 1, \cdots, r$ respectivement engendrés par l'image de $X - z_i$ dans A, et le localisé $A_{\mathfrak{m}_i}$ n'est autre que le facteur $\mathbb{C}[X]/(X - f_i)^{v_i}$.

Rappelons que la A-algèbre $A_{\mathfrak{m}}$ possède un unique idéal maximal, à savoir $\mathfrak{m}A_{\mathfrak{m}}$. On dit qu'elle est *locale*. Le corollaire affirme donc que toute algèbre de dimension finie sur un corps est produit d'algèbres locales. On peut préciser un peu la structure d'une telle algèbre.

Proposition. – *Soit A une algèbre locale de dimension finie sur un corps K, et soit* $\mathfrak{m}$ *son idéal maximal. Alors* $\mathfrak{m}$ *est nilpotent. Plus précisément on a* $\mathfrak{m}^d = 0$ *si* $d = \dim_K(A)$.

Démonstration. La suite décroissante $\mathfrak{m} \supset \mathfrak{m}^2 \supset \cdots \supset \mathfrak{m}^n \supset$ se stabilise avant l'indice $n = d$ puisque ce sont des K-ev de dimension finie. Supposons $\mathfrak{m}^{r+1}A = \mathfrak{m}^r A$. Le célèbre lemme suivant nous assure que $\mathfrak{m}^r A = 0$. □

Lemme. (de Nakayama) – *Soit A un anneau local d'idéal maximal* $\mathfrak{m}$ *et M un A-module de type fini. Si $M = \mathfrak{m}M$, alors M est nul.*

Démonstration. Supposons $M \neq 0$ et soit $\{m_1, \cdots, m_r\}$ un ensemble *minimal* de générateurs de M. Puisque $m_r \in \mathfrak{m}M$ il existe $i_1, \cdots, i_r \in \mathfrak{m}$ tels que $m_r = i_1 m_1 + \cdots + i_r m_r$. Or $1 - i_r \notin \mathfrak{m}$ donc l'idéal $(1 - i_r)$ n'est pas contenu dans $\mathfrak{m}$, donc il n'est pas propre (puisque $\mathfrak{m}$ est l'unique idéal maximal), donc il est égal à A et donc $1 - i_r \in A^\times$. Il s'ensuit que $m_r = (1 - i_r)^{-1}(i_1 m_1 + \cdots i_{r-1} m_{r-1})$, contredisant ainsi la minimalité de l'ensemble de générateurs choisi. □

Application. – Une algèbre commutative A *réduite* et de dimension finie sur un corps K est un produit fini $A = K_1 \times \cdots \times K_r$ d'extensions finies de K.

Remarque. – Plus généralement, un anneau noethérien et artinien est de longueur finie comme module sur lui-même, donc est produit d'anneaux locaux dont les idéaux maximaux sont nilpotents.

1.9 Modules de type fini sur un anneau principal

On sait bien que les modules de type fini sur un corps sont classifiés, à isomorphisme près, par leur dimension. L'approche la plus élémentaire vers cette classification est donnée par le pivot de Gauss : toute matrice $n \times m$ est équivalente à une matrice avec r entrées égales à 1 sur la diagonale et toutes ses autres entrées nulles, l'entier r (le rang) étant uniquement déterminé par la matrice.

Après les corps, les anneaux principaux sont quasiment les seuls à avoir le privilège d'admettre une jolie classification de leurs modules de type fini à isomorphisme près. L'approche la plus concrète est encore donnée par une adaptation du pivot de Gauss.

1.9.1 *Équivalence de matrices.* Soit $\mathrm{M}_{n\times m}(A)$ le A-module des matrices de taille $n\times m$. Comme sur un corps, on dit que $R, R' \in \mathrm{M}_{n\times m}(A)$ sont *équivalentes* s'il existe $P \in \mathrm{GL}_n(A)$ et $Q \in \mathrm{GL}_m(A)$ telles que $R' = PRQ$.

Théorème. – *Si A est principal, toute matrice R dans $\mathrm{M}_{n\times m}(A)$ est équivalente à une matrice R' "diagonale" telle que $a_{11}|a_{22}|\cdots|a_{ss}$ où $s = \min(n,m)$ et l'on autorise $a_{ii} = 0$. De plus, les idéaux (a_{ii}) sont uniquement déterminés par R.*

Démonstration. Existence de la matrice équivalente R'. Pour $a \in A$, posons $\ell(a) := \sum_{\mathfrak{p}\in\mathrm{Max}(A)} v_{\mathfrak{p}}(a)$. C'est le nombre de diviseurs irréductibles de a, à association près et comptés avec multiplicité. C'est aussi la longueur du A-module $A/(a)$ (exercice), d'où la notation. Pour une matrice $R = (a_{ij})_{i,j}$ on pose $\ell(R) := \min\{\ell(a_{ij}), 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$.

On raisonne par double récurrence, sur $s(R) = \min(n,m)$, puis sur $\ell(R)$.

Supposons $s(R) = 1$ et $R \neq 0$. Quitte à transposer la matrice, on peut supposer $n = 1$. Quitte à échanger des colonnes (multiplication à droite par une matrice de transposition), on peut supposer que $\ell(R) = \ell(a_{11})$. Deux cas se présentent alors :

– si a_{11} divise tous les a_{1j}, ce qui est en particulier le cas lorsque $\ell(R) = 0$ puisque a_{11} est alors inversible, on obtient une ligne $(a_{11}, 0, \cdots, 0)$ en multipliant par une matrice de transvection à droite (substitution de colonnes) et on a donc terminé.

– sinon, on peut supposer après échange de colonnes que a_{11} ne divise pas a_{12}. Soit alors $d := \mathrm{pgcd}(a_{11}, a_{12})$, et écrivons $a_{11} = a'_{11}d$ et $a_{12} = a'_{12}d$. Il existe donc u, v tels que $a'_{11}u + a'_{12}v = 1$, et on constate alors que la matrice $\begin{bmatrix} u & -a'_{12} \\ v & a'_{11} \end{bmatrix}$ est de déterminant 1, donc inversible et vérifie :

$$\begin{bmatrix} a_{11} & a_{12} & \cdots \end{bmatrix} \begin{bmatrix} u & -a'_{12} & 0 \\ v & a'_{11} & 0 \\ 0 & 0 & I_{m-2} \end{bmatrix} = \begin{bmatrix} d & 0 & \cdots \end{bmatrix}.$$

La ligne obtenue R' vérifie $\ell(R') < \ell(R)$ et on peut donc conclure le cas $s(R) = 1$ par récurrence sur $\ell(R)$.

Supposons maintenant $s(R) > 1$ et la propriété connue jusqu'à $s(R)-1$, puis raisonnons par récurrence sur $\ell(R)$. Comme précédemment, on peut effectuer des échanges de lignes et de colonnes pour avoir $\ell(a_{11}) = \ell(R)$. Si $\ell(R) = 0$, alors a_{11} est inversible et on peut s'en servir de "pivot" pour faire des substitutions de lignes et colonnes afin d'obtenir une matrice dont la première ligne et la première colonne sont nulles sauf a_{11}. On applique alors l'hypothèse de récurrence sur $s(R)$ à la sous-matrice $R' = (a_{ij})_{2\leqslant i\leqslant m, 2\leqslant j\leqslant n}$.

Si $\ell(R) > 0$, deux cas se présentent à nouveau :

– Si a_{11} ne divise pas la première ligne ou ne divise pas la première colonne, alors comme précédemment, on peut faire chuter $\ell(R)$ à l'aide d'une matrice 2×2 et du lemme de Bézout.

– Si a_{11} divise la première ligne et la première colonne alors on peut faire des substitutions de colonnes puis de lignes pour obtenir une matrice dont la première ligne et la première colonne sont nulles sauf a_{11}. Si a_{11} divise tous les autres a_{ij}, $i > 1$ et $j > 1$, on applique l'hypothèse de récurrence à la sous-matrice $R' = (a_{ij})_{2\leqslant i\leqslant m, 2\leqslant j\leqslant n}$. Sinon, si a_{11} ne divise pas a_{ij} on obtient par substitution de L_1 par $L_1 + L_i$ une matrice R' équivalente à R telle que a_{11} ne divise pas la première ligne. On se retrouve dans le premier cas juste traité.

Unicité des (a_{ii}). Notons $I_r(R)$ l'idéal engendré par les mineurs de taille $r\times r$ de la matrice $R \in \mathrm{M}_{n\times m}(A)$. Le point clef est que si $S \in \mathrm{M}_{m\times p}(A)$, alors $I_r(RS) \subset I_r(R)I_r(S)$ (voir 1.9.8 ci-dessous). De cela il suit que si P est carrée de taille $\geqslant r$ et inversible, alors $I_r(P) = A$, puis on en déduit que deux matrices équivalentes R et R' satisfont $I_r(R) = I_r(R')$ pour tout r. Si R' est de la forme du théorème, on a donc $(a_{11}) = I_1(R)$, $(a_{11}a_{12}) = I_2(R)$, etc. Ceci montre que les (a_{ii}) sont déterminés par R. $\square$

Exercice. – Soit $u \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^n)$ dont le déterminant $\det(u) \in \mathbb{Z}$ est non nul. Montrer que $\mathrm{Coker}(u)$ est fini d'ordre égal à $|\det(u)|$.

1.9.2 COROLLAIRE.– *Soit M un module de type fini sur A principal. Il existe un unique entier r et une unique suite d'idéaux propres $I_1 \supset I_2 \supset \cdots \supset I_r$ telle que*

$$M \simeq A/I_1 \oplus A/I_2 \oplus \cdots \oplus A/I_r.$$

De plus, l'entier r est le nombre minimal de générateurs de M.

Démonstration. (Existence) En fait, seule l'existence est un corollaire du théorème précédent. L'unicité sera prouvée en 1.9.7. Pour prouver l'existence, choisissons une famille génératrice $m_1, \cdots, m_n$ de M. Il lui est associé un morphisme surjectif $\pi : A^n \twoheadrightarrow M$. Puisque A est noethérien, $\mathrm{Ker}(\pi)$ est aussi de type fini, et est donc l'image d'un morphisme $u : A^m \longrightarrow A^n$. En d'autres termes, π induit un isomorphisme $\mathrm{Coker}(u) := A^n/u(A^m) \xrightarrow{\sim} M$. Soit R la matrice de u dans les bases canoniques, et soit P, Q comme dans le théorème précedent. Alors P est la matrice d'un automorphisme ρ de A^n et Q celle d'un automorphisme θ de A^m. Posons $u' := \rho\circ u\circ\theta : A^m \longrightarrow A^n$. Le morphisme $\pi\circ\rho^{-1}$ induit un isomorphisme $\mathrm{Coker}(u') \xrightarrow{\sim} M$. Or, la matrice de u' est la matrice "diagonale" R' du théorème. On a donc $\mathrm{Coker}(u') = A/(a_{11}) \oplus \cdots \oplus A/(a_{ss}) \oplus A^{n-s}$. Soit k le plus grand entier i tel que a_{ii} est inversible (on pose $k = 0$ si a_{11} n'est pas inversible). Alors en posant $I_i := (a_{k+i,k+i})$ pour $1 \leqslant i \leqslant s-k$ et $I_i = 0$ pour $s-k < i \leqslant n-k =: r$, on a une suite décroissante d'idéaux comme dans l'énoncé. $\square$

Remarque. – Ce corollaire est encore vrai pour les modules *de torsion* (au sens ci-dessous) sur un *anneau de Dedekind*, c'est-à-dire un anneau intègre noethérien dont les localisés en chaque idéal premier sont principaux. Par exemple l'anneau des entiers d'un corps de nombres algébriques est un anneau de Dedekind.

Remarque. – Supposons que M est un A-module de type fini et de $\mathfrak{p}^\infty$-torsion pour un idéal maximal $\mathfrak{p}$ de A (i.e. $M = M[\mathfrak{p}^\infty]$). En vertu du théorème 1.8.2, la décomposition du corollaire ne peut alors faire intervenir que des puissances de $\mathfrak{p}$. Il existe donc un unique entier r et une unique suite $m_1 \leqslant m_2 \leqslant \cdots \leqslant m_r$ telle que

$$M \simeq A/\mathfrak{p}^{m_1} \oplus A/\mathfrak{p}^{m_2} \oplus \cdots \oplus A/\mathfrak{p}^{m_r}.$$

1.9.3 *Application à la réduction des endomorphismes.* Reprenons les notations de l'exemple 1.8.3. Donc K est un corps, V un K-espace vectoriel de dimension finie n et $u \in \mathrm{End}_K(V)$ un endomorphisme de V, ce qui nous donne un $A = K[X]$-module $M = V$ où X agit par u. Supposons K algébriquement clos et factorisons le polynôme minimal $f_u = \prod_{i=1}^r (X - \lambda_i)^{v_i}$. Nous avons déjà décomposé $M = \bigoplus_{i=1}^r M[(X-\lambda_i)^{v_i}]$, ce qui correspond à la décomposition $V = \bigoplus_{i=1}^r \mathrm{Ker}((u-\lambda_i)^{v_i}$ de V en somme de sous-espace caractéristique. La remarque ci-dessus nous fournit une décomposition en somme de sous-modules cycliques

$$M[(X-\lambda_i)^{v_i}] = K[X]/(X-\lambda_i)^{m_{i1}} \oplus \cdots \oplus K[X]/(X-\lambda_i)^{m_{ir_i}}.$$

Écrivons cette décomposition sous la forme

$$V[f_i^{v_i}] = V_{i1} \oplus \cdots \oplus V_{ir_i} \text{ avec } V_{ij} = K[X]w_{ij} \text{ et } K[X]/((X-\lambda_i)^{m_{ij}}) \xrightarrow{\sim} K[X]w_{ij}$$

Alors chaque V_{ij} est stable par u et la famille $w_{ijk} := (u-\lambda_i)^{k-1}(w_{ij})$, $k = 1, \cdots, m_{ij}$ est une K-base de V_{ij} dans laquelle la matrice de u est de la forme $\lambda_i I + N$ où N est la matrice de taille $m_{ij} \times m_{ij}$ avec des 1 sur la “surdiagonale” et des 0 ailleurs. En d'autres termes, la matrice de u dans la base $\{w_{ijk}, i = 1, \cdots, r, j = 1, \cdots, r_i, k = 1, \cdots m_{ij}\}$ est sous forme de Jordan.

1.9.4 Définition.– *Soit M un module sur un anneau intègre A. On dit que m est un* élément de torsion *si* $\mathrm{Ann}_A(m) \neq \{0\}$. *Le sous-ensemble*

$$M_{\mathrm{tors}} := \{m \in M,\ \mathrm{Ann}_A(m) \neq \{0\}\}$$

des éléments de torsion est un sous-A-module de M appelé le sous-module de torsion *de M. On dit que M est* sans torsion *si $M_{\mathrm{tors}} = \{0\}$ et est* de torsion *si $M = M_{\mathrm{tors}}$.*

Exercice. – Montrer que M/M_{tors} est sans torsion.

Exercice. – Soit $K = \mathrm{Frac}(A)$. Montrer que M est sans torsion si et seulement si le morphisme $i : M \longrightarrow V := K \otimes_A M$ est injectif.

En général, un module sans torsion n'a aucune raison d'être libre. Par exemple, sur $A = \mathbb{C}[X, Y]$ l'idéal (X, Y) est un A-module sans torsion (puisque contenu dans A) mais pas libre. Néanmoins, sur A principal on a le résultat spectaculaire suivant :

1.9.5 COROLLAIRE. (Théorème des bases adaptées)– *Soit A principal, et M un A-module sans torsion de type fini. Alors*

i) M est libre.

ii) Si N un sous-module de M, il existe une base $e_\bullet = (e_1, \cdots, e_m)$ de M, un entier $n \leqslant m$ et des éléments $a_1|a_2|\cdots|a_n$ de A tels que $a_1e_1, \cdots, a_ne_n$ forment une base de N. De plus, les idéaux $(a_1) \supseteq \cdots \supseteq (a_n)$ ne dépendent que de M et N.

Démonstration. i) découle du corollaire précédent, puisque A/I est sans torsion si et seulement si $I = (0)$.

ii) (Existence) Remarquons que N est aussi sans torsion, donc libre par i), et rappelons que son rang n est inférieur au rang m de M. Choisissons deux bases $e'_\bullet = (e'_1, \cdots e'_m)$ de M et $f'_\bullet = (f'_1, \cdots, f'_n)$ de N, et notons R la matrice dans ces bases de l'inclusion $N \hookrightarrow M$. Soient P, Q et $R' = PRQ$ comme dans le théorème 1.9.1. On peut voir P^{-1} comme la matrice de passage de la base $e'_\bullet$ à une base $e_\bullet$ de M, et Q comme la matrice de passage de la base $f'_\bullet$ à une base $f_\bullet$ de N. Alors R' est la matrice de l'inclusion $N \hookrightarrow M$ dans les bases (f) et $e_\bullet$. La forme de R' montre donc, avec les notations du théorème 1.9.1, que $f_j = a_{jj}e_j$ pour tout $j = 1, \cdots, n$.

(Unicité) Avec $e_\bullet$ et $(a_i)_i$ comme dans l'énoncé de ii), la matrice $R \in \mathrm{M}_{m\times n}(A)$ de "diagonale" $a_1, \cdots, a_n$ représente l'inclusion $N \hookrightarrow M$ dans certaines bases de M et N (à savoir $e_\bullet$ et $f_\bullet = (a_1e_1, \cdots, a_ne_n)$). Toute matrice représentant cette inclusion dans d'autres bases est équivalente à R donc l'unicité découle de celle du théorème 1.9.1. $\square$

Remarque. – Pour le i), l'hypothèse "de type fini" est aussi importante. Par exemple, le $\mathbb{Z}$-module $\mathbb{Q}$ est sans torsion, mais n'est pas libre. En effet, s'il admettait une base $(e_i)_{i\in I}$, on pourrait définir un morphisme non nul vers $\mathbb{Z}/p\mathbb{Z}$ en envoyant par exemple chaque e_i sur $\bar{1}$, mais il n'existe évidemment pas de tel morphisme.

1.9.6 *Puissances extérieures.* Afin de prouver l'unicité dans le théorème 1.9.1 et le corollaire 1.9.2, nous allons utiliser une construction classique utile dans d'autres domaines comme la géométrie différentielle. Ici, A peut être un anneau commutatif quelconque. Soit M un A-module. Considérons le A-module

$$\otimes^r M := M \otimes_A M \otimes_A \cdots \otimes_A M \ (r \text{ facteurs})$$

et son sous-module A^rM engendré par les tous les tenseurs élémentaires $m_1 \otimes \cdots \otimes m_r$ "redondants" au sens où il existe $i \neq j$ tels que $m_i = m_j$. Le module quotient

$$\wedge^r M := (\otimes^r M)/(A^r M)$$

est appelé "r-ème puissance extérieure de M". L'image d'un tenseur élémentaire $m_1 \otimes \cdots \otimes m_r$ dans $\wedge^r M$ est notée $m_1 \wedge \cdots \wedge m_r$. Partant d'égalités du type $0 = (m_1 + m_2) \wedge (m_1 + m_2) = m_1 \wedge m_2 + m_2 \wedge m_1$, on voit que pour toute permutation $\sigma \in \mathfrak{S}_r$ on a $m_{\sigma(1)} \wedge \cdots \wedge m_{\sigma(r)} = \mathrm{sgn}(\sigma) \cdot m_1 \wedge \cdots \wedge m_r$. En fait, $\wedge^r M$ possède la propriété universelle suivante : pour tout A-module N, on a une bijection canonique entre $\mathrm{Hom}_A(\wedge^r M, N)$ et l'ensemble $\mathrm{Alt}^r(M,N)$ des applications r-multilinéaires alternées de M^r dans N.

Les puissances extérieures sont fonctorielles en M : si $u : M \longrightarrow N$ est un morphisme de A-modules, il induit un morphisme $\otimes^r u : \otimes^r M \longrightarrow \otimes^r N$ qui passe au quotient pour donner un morphisme $\wedge^r u : \wedge^r M \longrightarrow \wedge^r N$. De plus on a $\wedge^r(v \circ u) = \wedge^r v \circ \wedge^r u$.

On a des morphismes évidents de concaténation : $(\otimes^{r_1} M) \otimes_A (\otimes^{r_2} M) \longrightarrow \otimes^{r_1+r_2} M$ qui passent au quotient pour donner $(\wedge^{r_1} M) \otimes_A (\wedge^{r_2} M) \longrightarrow \wedge^{r_1+r_2} M$. Si l'on pose aussi $\otimes^0 M = A$ et $\wedge^0 M = A$, alors ces morphismes de concaténation munissent la somme directe $\otimes^\bullet M := \bigoplus_{r\in\mathbb{N}} \otimes^r M$ d'une structure de A-algèbre non commutative (et graduée) appelée "algèbre tensorielle de M". De même on a une "algèbre extérieure" $\wedge^\bullet M$ et la projection canonique $\otimes^\bullet M \longrightarrow \wedge^\bullet M$ est un morphisme de A-algèbres.

Soient maintenant M_1 et M_2 deux A-modules. Fonctorialité et concaténation fournissent donc des morphismes $(\wedge^{r_1} M_1) \otimes_A (\wedge^{r_2} M_2) \longrightarrow \wedge^{r_1+r_2}(M_1 \oplus M_2)$.

Lemme. – *La somme des morphismes ci-dessus est un isomorphisme*

$$\bigoplus_{r_1+r_2=r} (\wedge^{r_1} M_1) \otimes_A (\wedge^{r_2} M_2) \xrightarrow{\sim} \wedge^r(M_1 \oplus M_2).$$

Démonstration. Nous allons construire un morphisme dans l'autre sens. Les propriétés monoïdales du produit tensoriel nous donnent une décomposition

$$\otimes^r(M_1 \oplus M_2) = \bigoplus_{\alpha:\{1,\cdots,r\}\longrightarrow\{1,2\}} N_\alpha, \text{ avec } N_\alpha := M_{\alpha(1)} \otimes_A \cdots \otimes_A M_{\alpha(r)}.$$

Fixons $\alpha : \{1,\cdots,r\} \longrightarrow \{1,2\}$ et notons r_α le cardinal de la fibre $\alpha^{-1}(1)$. Soit $\sigma \in \mathfrak{S}_r$ une permutation telle que $\sigma(\{1,\cdots,r_\alpha\}) = \alpha^{-1}(1)$. On lui associe un isomorphisme

$$\tilde{\psi}_{\alpha,\sigma} : N_\alpha \xrightarrow{\sim} (\otimes^{r_\alpha} M_1) \otimes_A (\otimes^{r-r_\alpha} M_2)$$

qui envoie un tenseur élémentaire $n_1 \otimes \cdots \otimes n_r \in N_\alpha$ sur le tenseur élémentaire

$$\mathrm{sgn}(\sigma) \cdot (n_{\sigma(1)} \otimes \cdots \otimes n_{\sigma(r_\alpha)}) \otimes (n_{\sigma(r_\alpha+1)} \otimes \cdots \otimes n_{\sigma(r)}).$$

Cet isomorphisme dépend clairement du choix de σ, mais la composée

$$\psi_\alpha : N_\alpha \longrightarrow (\wedge^{r_\alpha} M_1) \otimes_A (\wedge^{r-r_\alpha} M_2)$$

n'en dépend pas. En sommant sur α on obtient finalement un morphisme

$$\psi = \bigoplus_\alpha \psi_\alpha : \otimes^r(M_1 \oplus M_2) \longrightarrow \bigoplus_{r_1+r_2} (\wedge^{r_1} M_1) \otimes_A (\wedge^{r_2} M_2).$$

Montrons que ce morphisme se factorise par $\wedge^r(M_1 \oplus M_2)$. Pour cela, faisons agir (à droite) $\mathfrak{S}_r$ sur $\otimes^r(M_1 \oplus M_2)$ par permutation des facteurs tensoriels : $\sigma(n_1 \otimes \cdots \otimes n_r) := n_{\sigma(1)} \otimes \cdots \otimes n_{\sigma(r)}$. On remarque que $\sigma(N_\alpha) = N_{\alpha\circ\sigma}$ et que, par construction, $\psi_{\alpha\circ\sigma} = \mathrm{sgn}(\sigma) \cdot (\psi_\alpha \circ \sigma)$.

Maintenant, par définition, $A^r(M_1 \oplus M_2)$ est engendré par les tenseurs élémentaires $n = n_1 \otimes \cdots \otimes n_r$ tels qu'il existe une transposition τ telle que $n = \tau(n)$. Écrivons un tel n sous la forme $\sum_\alpha n_\alpha$ (de manière unique, donc) : on a alors $n_{\alpha\circ\tau} = \tau(n_\alpha)$ pour tout α. Si $\alpha \circ \tau \neq \alpha$ on a donc $\psi(n_\alpha + n_{\alpha\circ\tau}) = \psi_\alpha(n_\alpha) + \psi_{\alpha\circ\tau}(n_{\alpha\circ\tau}) = \psi_\alpha(n_\alpha) - \psi_\alpha(\tau(n_{\alpha\circ\tau})) = 0$ par ce qui précède. Si $\alpha \circ \tau = \alpha$, alors $\tilde{\psi}_{\alpha,\sigma}(n_\alpha)$ est fixe par la transposition $\sigma^{-1}\tau\sigma \in \mathfrak{S}_{r_\alpha} \times \mathfrak{S}_{r-r_\alpha}$ (où σ est comme au début de la preuve), et donc $\psi_\alpha(n_\alpha) = 0$. En sommant, on obtient $\psi(n) = 0$, et donc le morphisme ψ passe au quotient pour donner un morphisme

$$\bar{\psi} : \wedge^r(M_1 \oplus M_2) \longrightarrow \bigoplus_{r_1+r_2} (\wedge^{r_1} M_1) \otimes_A (\wedge^{r_2} M_2).$$

On laisse au lecteur le soin de vérifier qu'il est inverse de celui de l'énoncé. □

1.9.7 *Preuve de l'unicité dans le corollaire 1.9.2.* Soit $M = A/I_1 \oplus \cdots \oplus A/I_s$ avec $I_1 \supset \cdots \supset I_s$. Nous allons voir comment récupérer s et les I_k à partir des puissances extérieures de M. Remarquons d'abord que pour tout $r > 0$, le lemme précédent fournir par récurrence un isomorphisme

$$\wedge^r(M) = \bigoplus_{r_1+\cdots+r_s=r} \wedge^{r_1}(A/I_1) \otimes_A \cdots \otimes_A \wedge^{r_s}(A/I_s).$$

On a $\wedge^0(A/I) = A$ (par convention) et $\wedge^1(A/I) = A/I$. De plus, pour $r > 1$, tout élément de $\otimes^r(A/I)$ est un A-multiple de $1 \otimes \cdots \otimes 1$, donc $\wedge^r(A/I) = 0$ dès que $r > 1$. On peut donc réécrire la somme ci-dessus sous la forme

$$\wedge^r(M) = \bigoplus_{\{k_1<\cdots<k_r\}\subset\{1,\cdots,s\}} (A/I_{k_1}) \otimes \cdots \otimes (A/I_{k_r}) = \bigoplus_{\{k_1<\cdots<k_r\}\subset\{1,\cdots,s\}} A/I_{k_1}.$$

où la deuxième égalité vient du fait que I_{k_1} contient tous les autres I_{k_i}. Il s'ensuit que

$$s = \mathrm{Max}\{r \in \mathbb{N}, \wedge^r(M) \neq 0\} \text{ et } I_k = \mathrm{Ann}_A(\wedge^{s+1-k} M).$$

On a donc récupéré s et les I_k et on remarquera que ce raisonnement n'utilise aucune hypothèse sur A.

1.9.8 *Preuve de l'unicité dans le théorème 1.9.1.* On peut la déduire de celle du corollaire 1.9.2 de la manière suivante : soit $u : A^m \longrightarrow A^n$ le morphisme représenté par R dans les bases canoniques. Alors la matrice R' représente ce même morphisme dans d'autres bases. Il s'ensuit que $\mathrm{Coker}(u) \simeq A/(a_{11}) \oplus \cdots \oplus A/(a_{ss})$. L'unicité du corollaire 1.9.2 nous dit que les (a_{ii}) ne dépendent que de $\mathrm{Coker}(u)$ donc que de u et enfin, que de R.

Cependant, il est intéressant de terminer la preuve directe esquissée plus haut en démontrant que $I_r(SR) \subset I_r(R)I_r(S)$ (cf les notations à la fin de la preuve du théorème 1.9.1). Pour cela, notons $e_1, \cdots, e_n$ la base canonique de A^n et $f_1, \cdots, f_m$ celle de A^m. Comme ci-dessus, on voit que $\wedge^r(A^n)$ est libre de rang $\binom{n}{r}$ et que l'ensemble des

$$e_I := e_{i_1} \wedge \cdots \wedge e_{i_r} \text{ pour } I = \{i_1 < \cdots < i_r\} \subset \{1, \cdots, n\}$$

en est une base. De même on a une base $(f_J)_J$ de $\wedge^r(A^m)$, où $J \subset \{1, \cdots, m\}$ est de cardinal r. Soit alors $\wedge^r R$ la matrice de $\wedge^r u$ dans les bases $(e_I)_I$ et $(f_J)_J$. Le lemme ci-dessous nous assure que $I_r(R) = I_1(\wedge^r R)$. Comme on a aussi $\wedge^r(RS) = (\wedge^r R)(\wedge^r S)$, il s'ensuit que $I_r(RS) = I_1(\wedge^r(RS)) \subset I_1(\wedge^r R) I_1(\wedge^r S) = I_r(R) I_r(S)$. (Noter que pour $r = 1$, l'inégalité $I_1(RS) \subset I_1(R) I_1(S)$ découle immédiatement des formules de produit matriciel).

Lemme. – *L'entrée a^r_{IJ} de la matrice $\wedge^r(R)$ est le mineur de R associé au sous-ensemble de lignes I et au sous-ensemble de colonnes J.*

Démonstration. Soit $I = \{i_1 < \cdots < i_r\}$ et $J = \{j_1 < \cdots < j_r\}$. Notons a_{ij} les entrées de R. On a

$$(\wedge^r u)(f_{j_1} \wedge \cdots \wedge f_{j_r}) = u(f_{j_1}) \wedge \cdots \wedge u(f_{j_r}), \quad \text{avec } u(f_{j_k}) = \sum_{i=1}^{n} a_{i j_k} e_i.$$

En utilisant la multilinéarité pour développer le produit, et les égalités $e_{i_{\sigma(1)}} \wedge \cdots \wedge e_{i_{\sigma(r)}} = \mathrm{sgn}(\sigma) \cdot e_{i_1} \wedge \cdots \wedge e_{i_r}$ si $\sigma \in \mathfrak{S}_r$, on constate que le terme en $e_{i_1} \wedge \cdots \wedge e_{i_r}$ dans cette somme est

$$\sum_{\sigma \in \mathfrak{S}_r} \mathrm{sgn}(\sigma) \cdot a_{i_{\sigma(1)} j_1} \cdots a_{i_{\sigma(r)} j_r}$$

qui est bien le mineur associé à I et J. $\square$

2 Extensions de corps. Théorie de Galois

La "théorie de Galois" moderne est l'étude des extensions de corps et de leurs groupes d'automorphismes. Elle est née d'un problème bien concret que se posaient les mathématiciens du 19^{me} siècle, qui était de savoir si toutes les "équations algébriques" étaient "résolubles par radicaux". En d'autres termes, tout polynôme irréductible de $\mathbb{Q}[X]$ admet-il une solution (dans $\mathbb{C}$) qui s'exprime avec les opérations $+, -, \times, \div$ et $\sqrt[n]{x}$? Les formules classiques du trinôme, de Cardan (troisième degré) et Ferrari (quatrième degré) montraient que c'était possible jusqu'en degré 4, mais Galois (et Abel) a exhibé un polynôme de degré 5 pour lequel ce n'était pas possible. En fait, il est même rare que ce soit possible en degré $\geqslant 5$. Pour ce faire, Galois a étudié les ensembles de symétries des solutions d'équations polynomiales (que l'on appelle maintenant "groupes de Galois") et a remarqué que la solubilité par radicaux d'une équation polynomiale était équivalente à la résolubilité de son groupe de symétries (au sens de la théorie des groupes moderne, qui n'existait pas à l'époque). Le groupe de symétrie d'une équation de degré n se plonge dans le groupe symétrique $\mathfrak{S}_n$. Pour $n < 5$, le groupe $\mathfrak{S}_n$ est résoluble, ce qui explique l'existence des formules classiques. Par contre le groupe $\mathfrak{A}_5$ est simple et n'est donc pas résoluble et Galois a justement exhibé une équation dont le groupe de symétrie est $\mathfrak{A}_5$.

2.1 Généralités sur les extensions de corps. Nullstellensatz

2.1.1 DÉFINITION.– *Soit k un corps. Une "extension" K de k est un corps K muni d'un morphisme de corps $k \longrightarrow K$.*

Remarquons qu'un morphisme de corps est simplement un morphisme d'anneaux, donc une extension de k n'est rien d'autre qu'une k-algèbre qui est un corps. Le terme "extension" se justifie par le fait qu'un morphisme de corps est toujours injectif. On abuse souvent en notant simplement $k \subset K$. Une *sous-extension* de K est alors un sous-corps K' de K qui contient k.

Notation. – Soit $k \subset K$ une extension de corps et $\alpha \in K$. On notera
— $k[\alpha]$ la sous-k-algèbre de K engendrée par α.
— $k(\alpha)$ la sous-extension de K engendrée par α.

Comme d'habitude "engendrée" signifie "la plus petite contenant α". Concrètement, $k[\alpha]$ est l'image de l'unique morphisme de k-algèbres $k[X] \longrightarrow K$ qui envoie X sur α, donc $k[\alpha]$ est engendrée, en tant que k-module, par les puissances de α. Comme on a évidemment $k[\alpha] \subset k(\alpha)$, on voit que $k(\alpha) = \mathrm{Frac}(k[\alpha])$. En revanche, $k(\alpha)$ *n'est pas toujours l'image d'un morphisme* $k(X) \longrightarrow K$.

Exemple. – $k = \mathbb{Q} \subset K = \mathbb{C}$, $\alpha = i$. Dans ce cas, $\mathbb{Q}[i] = \mathbb{Q} \oplus \mathbb{Q}i$ est un corps, donc $\mathbb{Q}[i] = \mathbb{Q}(i)$ est de dimension 2 sur $\mathbb{Q}$ alors que $\mathbb{Q}(X)$ est de dimension infinie sur $\mathbb{Q}$. Comme un morphisme de corps est injectif, il n'y a pas de morphisme de corps $\mathbb{Q}(X) \longrightarrow \mathbb{Q}(i)$.

2.1.2 *Alternative algébrique/transcendant.*

PROPOSITION. – *Soit $k \subset K$ une extension de corps et $\alpha \in K$. Notons $\varphi_\alpha : k[X] \longrightarrow K$ le morphisme de k-algèbres qui envoie X sur α. On a alors l'alternative suivante :*

i) Soit φ_α est injectif, auquel cas il induit un isomorphisme $k[X] \xrightarrow{\sim} k[\alpha]$ qui se prolonge uniquement en un isomorphisme $k(X) \xrightarrow{\sim} k(\alpha)$. En particulier, $k[\alpha]$ et $k(\alpha)$ sont de dimension infinie sur k.

ii) Soit φ_α n'est pas injectif, auquel cas on a les propriétés suivantes :

  (a) Son noyau est engendré par un unique polynôme unitaire irréductible $f_\alpha \in k[X]$

  (b) φ_α induit un isomorphisme $k[X]/(f_\alpha) \xrightarrow{\sim} k[\alpha]$

  (c) $k[\alpha]$ est de dimension finie sur k, égale au degré $\deg(f_\alpha)$

  (d) $k(\alpha) = k[\alpha]$.

Démonstration. Dans le cas i), les seules choses à prouver sont l'existence et l'unicité du prolongement de φ_α en un isomorphisme $k(X) \xrightarrow{\sim} k(\alpha)$. Mais celles-ci découlent de la propriété universelle du corps des factions, puisque φ_α envoie tout élément $f \in k[X]$ non nul sur un élément inversible dans K.

Dans le cas ii), le fait que $\mathrm{Ker}(\varphi_\alpha)$ est engendré par un seul polynôme provient du fait que $k[X]$ est principal. Ce polynôme est bien défini à multiplication par un inversible près ;

on peut le rendre unitaire en multipliant par un $\lambda \in k^\times$, et cela le rend unique puisque $k[X]^\times = k^\times$. Par ailleurs, φ_α induit un isomorphisme $k[X]/\operatorname{Ker}(\varphi_\alpha) \xrightarrow{\sim} k[\alpha]$ (propriété universelle des quotients), et puique $k[\alpha] \subset K$ est intègre, $\operatorname{Ker}(\varphi_\alpha)$ est un idéal premier et donc f_α est irréductible. On a donc prouvé (a) et (b). Le point (c) découle alors du second corollaire de 1.4.3. Quant au point (d), il s'agit se prouver que $k[\alpha]$ est un corps. On peut le voir de deux manières : soit en rappelant que tout idéal premier de $k[X]$ est maximal, soit en invoquant le lemme d'intérêt indépendant suivant :

LEMME. – *Une algèbre A intègre de dimension finie sur un corps k est un corps.*

Démonstration. La multiplication par $x \in A \setminus \{0\}$ est un endomorphisme k-linéaire injectif de A, donc bijectif par le théorème du rang. Il existe en particulier y tel que $xy = 1$. □

□

DÉFINITION. – *Dans le contexte de la proposition, on dit que α est* transcendant sur *k dans le cas i), et on dit qu'il est* algébrique sur *k dans le cas ii). Dans ce dernier cas, f_α est appelé* polynôme minimal *de α.*

Exemples. – Considérons l'extension $\mathbb{Q} \subset \mathbb{C}$. Les nombres complexes i, j ou $\sqrt{2}$ sont algébriques sur $\mathbb{Q}$. Les premiers nombres transcendants construits furent les "nombres de Liouville", qui admettent de bonnes approximations par les nombres rationnels. Lindemann prouva ensuite que les nombres de la forme e^a avec a algébrique sont transcendants. Comme $e^{i\pi} = 1$, cela implique que π est transcendant, ce qui montre au passage l'impossibilité de la "quadrature du cercle". Par contre, on ne sait toujours pas si des nombres comme e^π ou $\pi + e$ sont transcendants.

Remarque. – En fait il y a "beaucoup plus" de nombres complexes transcendants qu'il n'y en a d'algébriques. Plus précisément, le sous-ensemble $\overline{\mathbb{Q}} \subset \mathbb{C}$ formé de tous les nombres algébriques est dénombrable. En effet, chaque nombre algébrique annule un polynôme à coefficients entiers. Ces polynômes sont en bijection avec les suites presque nulles d'entiers, et ces suites forment un ensemble dénombrable (exercice !). Il s'ensuit que l'ensemble $\mathbb{C} \setminus \overline{\mathbb{Q}}$ des nombres transcendants est indénombrable.

2.1.3 *Indépendance algébrique.* Soit $k \subset K$ une extension de corps, et soit $(\alpha_i)_{i\in I}$ une famille d'éléments de K indexée par un ensemble I. Comme dans le paragraphe précédent, on note
— $k[(\alpha_i)_{i\in I}]$ la sous-k-algèbre de K engendrée par les α_i
— $k((\alpha_i)_{i\in I})$ la sous-extension de K engendrée par les α_i.

DÉFINITION. – *On dit que la famille $(\alpha_i)_{i\in I}$ est* algébriquement indépendante *sur k si le morphisme de k-algèbres $k[(X_i)_{i\in I}] \longrightarrow K$ qui envoie X_i sur α_i pour tout i est injectif.*

Lorsque les α_i sont algébriquement indépendants, le morphisme de la définition se prolonge uniquement en un isomorphisme $k((X_i)_{i\in I}) := \operatorname{Frac}(k[(X_i)_{i\in I}]) \xrightarrow{\sim} k((\alpha_i)_{i\in I})$.

Exemple. – Si l'on prend "au hasard" n éléments dans $\mathbb{C}$, ils ont toutes les chances d'être algébriquement indépendants. Par contre, il est très difficile de prouver l'indépendance de nombres donnés à l'avance, par exemple on ne sait pas si e et π sont algébriquement indépendants. Il est conjecturé que les valeurs de la fonction ζ de Riemann aux entiers impairs $\zeta(3), \zeta(5)$, etc... sont algébriquement indépendantes (sur $\mathbb{Q}$). La célébrité du théorème d'Apery, qui montre "simplement" l'irrationnalité de $\zeta(3)$, donne une idée de l'envergure de cette conjecture.

Remarque. – Si $I = I_1 \sqcup I_2$ (réunion disjointe), on a $k((\alpha_i)_{i\in I}) = k((\alpha_i)_{i\in I_1})((\alpha_i)_{i\in I_2})$. De plus, la famille $(\alpha_i)_{i\in I}$ est algébriquement indépendante sur k si et seulement si la famille $(\alpha_i)_{i\in I_1}$ est algébriquement indépendante sur k et la famille $(\alpha_i)_{i\in I_2}$ est algébriquement indépendante sur $k((\alpha_i)_{i\in I_1})$.

2.1.4 DÉFINITION.– *Une extension $k \subset K$ est dite :*
— finie *si K est de dimension finie comme k-ev. On note alors $[K : k] := \dim_k(K)$ et on l'appelle* degré *de K sur k.*
— algébrique *si tout élément $\alpha \in K$ est algébrique sur k.*
— de type fini *si K est engendrée, en tant qu'extension de corps, par une famille finie d'éléments.*
— monogène *si K est engendrée, en tant qu'extension de corps, par un seul élément.*
— transcendante pure *si K est engendrée par une famille algébriquement indépendante sur k.*

Remarque. – Vu les définitions, une extension finie est algébrique et une extension est algébrique si et seulement si elle est réunion de sous-extensions finies. De plus, une extension algébrique est finie si et seulement si elle est de type fini. Enfin, si α est algébrique sur k, alors $k(\alpha)$ est finie et $[k(\alpha) : k] = \deg(f_\alpha)$.

Exemple. – L'extension $k \subset k(X_1, \cdots, X_n)$ est de type fini et transcendante pure.

2.1.5 *Le Nullstellensatz.* On pourrait penser qu'une extension $k \subset K$ puisse avoir une propriété intermédiaire entre être *finie* et *de type fini*, à savoir que K *soit une k-algèbre de type fini.* Mais le théorème suivant montre qu'on n'obtient rien de nouveau.

THÉORÈME. – *Soit $k \subset K$ une extension de corps telle que K soit une k-algèbre de type fini. Alors $k \subset K$ est une extension finie (i.e. K est de dimension finie sur k).*

Démonstration. On raisonne par récurrence sur le nombre n de générateurs de K comme k-algèbre. Si $n = 0$, il n'y a rien à montrer. Supposons donc $n \geqslant 1$ et choisissons $\alpha_1, \cdots, \alpha_n$ tels que $K = k[\alpha_1, \cdots, \alpha_n]$. On a a fortiori $K = k(\alpha_1)[\alpha_2, \cdots, \alpha_n]$, donc notre hypothèse de récurrence assure que l'extension $k(\alpha_1) \subset K$ est finie et il nous reste à montrer que α_1 est algébrique sur k.

Choisissons une base $\beta_1 := 1, \beta_2, \cdots, \beta_m$ de K sur $k(\alpha_1)$. La multiplication dans K est déterminée par les formules $\beta_i\beta_j = \sum_{k=1}^m a_{ijk}\beta_k$ avec $a_{ijk} \in k(\alpha_1)$. Par ailleurs, écrivons chaque $\alpha_1, \cdots, \alpha_n$ sous la forme $\alpha_i = \sum_{j=1}^m b_{ij}\beta_j$ avec $b_{ij} \in k(\alpha_1)$. Soit alors

$A := k[a_{ijk}, b_{ij}]_{i,j,k}$ la sous-k-algèbre de $k(\alpha_1)$ engendrée par les a_{ijk} et les b_{ij}. On a manifestement $k[\alpha_1, \cdots, \alpha_n] \subset A\beta_1 \oplus \cdots \oplus A\beta_m$.

Supposons maintenant que α_1 est *transcendant*, de sorte que $k[\alpha_1] \simeq k[X]$. Les a_{ijk} et les b_{ij} sont donc des fractions rationnelles en α_1, disons $a_{ijk} = \frac{f_{ijk}}{g_{ijk}}$ et $b_{ij} = \frac{f_{ij}}{g_{ij}}$ avec $f_{ij}, f_{ijk}, g_{ij}, g_{ijk} \in k[\alpha_1]$. Il s'ensuit que si g est n'importe quel polynôme premier aux g_{ij} et g_{ijk} (par exemple le produit des g_{ij} et des g_{ijk} plus 1), alors $\frac{1}{g} \notin A$. Donc $\frac{1}{g} \notin k[\alpha_1, \cdots, \alpha_n]$, ce qui contredit l'hypothèse $k[\alpha_1, \cdots, \alpha_n] = K$. $\square$

Voici une formulation équivalente mais plus "géométrique".

Théorème. – *Si $\mathfrak{m}$ est un idéal maximal de $k[X_1, \cdots, X_n]$, alors son corps résiduel $K = k[X_1, \cdots, X_n]/\mathfrak{m}$ est une extension finie de k.*

Application géométrique : On a vu précédemment que les points d'un ensemble algébrique V sont en bijection avec les morphismes de $\mathbb{C}$-algèbres $\mathcal{O}(V) \longrightarrow \mathbb{C}$, et donc avec l'ensemble des idéaux maximaux de $\mathcal{O}(V)$ dont le corps résiduel est $\mathbb{C}$. Puisque toute extension finie de $\mathbb{C}$ est égale à $\mathbb{C}$ (on le rappellera plus loin), le théorème ci-dessus implique que l'application $z \mapsto \mathfrak{m}_z = \{f \in \mathcal{O}(V), f(z) = 0\}$ est une bijection $V \xrightarrow{\sim} \mathrm{Max}(\mathcal{O}(V))$.

Il dit aussi, et cela justifie le nom *Nullstellensatz*, que tout système d'équations polynômiales $f_1(z) = \cdots = f_r(z) = 0$ dans $\mathbb{C}^n$ possède au moins une solution dès que l'idéal $(f_1, \cdots, f_r)$ est propre. En fait, la bijection $\mathbb{C}^n \xrightarrow{\sim} \mathrm{Max}(\mathcal{O}(\mathbb{C}^n))$ induit une bijection

$$V(f_1, \cdots, f_r) \xrightarrow{\sim} \{\mathfrak{m} \in \mathrm{Max}(\mathcal{O}(\mathbb{C}^n)), \mathfrak{m} \supset (f_1, \cdots, f_r)\}$$

et l'existence d'une solution découle donc du lemme de Zorn !

Voici maintenant un corollaire qui va nous mener à une forme plus forte de ces énoncés.

Définition. – *Un anneau A est dit* de Jacobson *si pour tout idéal $I \subset A$ on a*

$$\sqrt{I} = \bigcap_{I \subset \mathfrak{m} \in \mathrm{Max}(A)} \mathfrak{m}.$$

Remarque. – On a déja vu qu'on a toujours $\sqrt{I} = \bigcap_{I \subset \mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$. On voit donc que A est de Jacobson si et seulement si pour tout idéal premier $\mathfrak{p}$ on a $\mathfrak{p} = \bigcap_{\mathfrak{p} \subset \mathfrak{m} \in \mathrm{Max}(A)} \mathfrak{m}$. Cette propriété équivaut à la densité de $\mathrm{Max}(A/I)$ dans $\mathrm{Spec}(A/I)$ muni de la topologie de Zariski, pour tout idéal I de A.

Corollaire. – *Toute k-algèbre de type fini est un anneau de Jacobson.*

Démonstration. Quitte à quotienter par I on peut supposer $I = 0$. On doit alors montrer que $\bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} \mathfrak{m} = \mathrm{Nilp}(A)$. L'inclusion $\supset$ est claire. Montrons l'autre inclusion par contrapposée. Soit donc f non nilpotent. Alors $A[f^{-1}] = A[X]/(Xf - 1)$ est encore une k-algèbre de type fini. Choisissons un idéal maximal $\tilde{\mathfrak{m}}$ de $A[f^{-1}]$ et soit $\mathfrak{m}$ son image réciproque dans A. C'est un idéal premier de A qui ne contient pas f (cf exercice 1.6.1), donc si nous montrons qu'il est maximal, nous avons terminé. Or, on a $k \subset A/\mathfrak{m} \subset A[f^{-1}]/\tilde{\mathfrak{m}}$ et le théorème précédent affirme que $A[f^{-1}]/\tilde{\mathfrak{m}}$ est une extension finie de k. Il s'ensuit que $A/\mathfrak{m}$ est une k-algèbre intègre de dimension finie, donc un corps, et $\mathfrak{m}$ est bien maximal. $\square$

Application géométrique. Nous pouvons enfin décrire précisément l'algèbre des fonctions polynômiales $\mathcal{O}(V)$ d'un ensemble algébrique $V = V(f_1, \cdots, f_r) \subset \mathbb{C}^n$. En effet, on a par définition $\mathcal{O}(V) = \mathcal{O}(\mathbb{C}^n)/I(V)$ avec

$$\begin{aligned} I(V) &= \{f \in \mathcal{O}(\mathbb{C}^n), \forall z \in V, f(z) = 0\} \\ &= \{f \in \mathcal{O}(\mathbb{C}^n), \forall z \in \mathbb{C}^n, f_1(z) = \cdots = f_r(z) = 0 \Rightarrow f(z) = 0\} \\ &= \{f \in \mathcal{O}(\mathbb{C}^n), \forall \mathfrak{m} \in \mathrm{Max}(\mathcal{O}(\mathbb{C}^n)), f_1, \cdots, f_r \in \mathfrak{m} \Rightarrow f \in \mathfrak{m}\} \\ &= \bigcap_{\mathfrak{m} \in \mathrm{Max}(\mathcal{O}(\mathbb{C}^n), f_i \in \mathfrak{m}} \mathfrak{m} = \sqrt{(}f_1, \cdots, f_r) \end{aligned}$$

De là on déduit que les applications $I \mapsto V(I)$ et $V \mapsto I(V)$ sont des bijections réciproques entre l'ensemble des idéaux radiciels de $\mathcal{O}(\mathbb{C}^n)$ et l'ensemble des sous-ensembles algébriques de $\mathbb{C}^n$.

Exercice. – Montrer que si $\varphi : A \longrightarrow B$ est un morphisme d'anneaux avec A de Jacobson et B de type fini sur A, alors pour tout $\mathfrak{m} \in \mathrm{Max}(B)$ on a $\varphi^{-1}(\mathfrak{m}) \in \mathrm{Max}(A)$. Donner un exemple d'anneau (et même de k-algèbre) qui n'est pas de Jacobson, et un exemple de morphisme d'anneaux pour lequel il existe $\mathfrak{m}$ maximal tel que $\varphi^{-1}(\mathfrak{m})$ n'est pas maximal.

2.1.6 *Clôture algébrique relative.*

Lemme. – *Soit $k \subset k' \subset K$ une tour d'extensions de corps.*

i) K est finie sur k si et seulement si K est finie sur k' et k' est finie sur k. De plus, on a dans ce cas l'égalité $[K : k] = [K : k'][k' : k]$.

ii) K est algébrique sur k si et seulement si K est algébrique sur k' et k' est algébrique sur k.

Démonstration. i) L'équivalence est claire. Pour l'égalité, posons $n = [K : k']$ et $m = [k' : k]$. Alors $K \simeq k'^n$ en tant que k'-ev, et $k' \simeq k^m$ en tant que k-ev. Il s'ensuit que $K \simeq (k^m)^n = k^{mn}$ en tant que k-ev. En pratique, si $\alpha_1, \cdots, \alpha_n$ est une base de K sur k' et si $\beta_1, \cdots, \beta_m$ est une base de k' sur k, alors $\{\alpha_i\beta_j, i = 1, \cdots, n; j = 1, \cdots, m\}$ est une base de K sur k.

ii) L'implication $\Rightarrow$ est claire. Pour l'autre implication, soit $\alpha \in K$. Notons $f_\alpha = X^n + a_1X^{n-1} + \cdots + a_n \in k'[X]$ son polynôme minimal sur k'. Ainsi α est algébrique sur le corps $k(a_1, \cdots, a_n)$. Or chacun des a_i est algébrique sur k, donc $k(a_1, \cdots, a_n)$ est fini sur k (par une récurrence à l'aide de i)). Il s'ensuit que $k(a_1, \cdots, a_n, \alpha)$ est fini sur k et en particulier α est algébrique sur k. $\square$

La proposition suivante montre que toute extension contient une unique sous-extension algébrique maximale.

Proposition. – *Soit $k \subset K$ une extension de corps. L'ensemble K_{alg} de tous les éléments de K algébriques sur k est un corps. On l'appelle* clôture algébrique de k dans K.

Démonstration. Soient $\alpha, \beta \in K$ algébriques sur k. Alors $k(\alpha)$ est fini sur k et, comme β est a fortiori algébrique sur $k(\alpha)$, $k(\alpha, \beta)$ est fini sur $k(\alpha)$. Il s'ensuit que $k(\alpha, \beta)$ est fini sur k. En particulier, $\alpha + \beta$ et $\alpha\beta$ sont algébriques sur k. □

Exemple. – L'ensemble $\overline{\mathbb{Q}}$ introduit plus haut est la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$.

2.1.7 *Bases de transcendance et degré de transcendance.* Une extension $k \subset K$ contient toujours une sous-extension $k \subset K'$ transcendante pure et telle que $K' \subset K$ soit algébrique. En effet, il suffit de prendre pour K' l'extension engendrée par une famille algébriquement indépendante maximale (pour l'inclusion). L'exemple suivant montre que K' est loin d'être unique.

Exemple. – Soit C la courbe d'équation $X^2 = Y^3 - 1$. Son anneau de fonctions polynomiales est $A = \mathbb{C}[X, Y]/(X^2 - Y^3 + 1)$ et son corps de fonctions rationnelles est $K = \text{Frac}(A) = \mathbb{C}(Y)[X]/(X^2 - Y^3 + 1)$. Le corps K n'est pas transcendant pur, mais est de degré 2 sur le corps $\mathbb{C}(Y)$ transcendant pur. On peut aussi l'écrire $K = \mathbb{C}(X)[Y]/(Y^3 - X^2 - 1)$, ce qui montre qu'il est de degré 3 sur le corps $\mathbb{C}(X)$ transcendant pur.

On voit néanmoins dans cet exemple que les sous-corps purement transcendants sont à une indéterminée. Ceci se généralise ainsi.

Théorème. – *Soit $k \subset K$. Les familles maximales d'éléments de K algébriquement indépendants sur k sont toutes de même cardinal. On les appelle* bases de transcendance de K sur k *et leur cardinal est appelé* degré de transcendance *de l'extension $k \subset K$ et noté* deg.tr.(K/k).

Démonstration. Nous ne prouvons ce résultat que lorsque K admet une famille algébriquement indépendante maximale *finie*. Supposons donc qu'il existe des éléments algébriquement indépendants $\alpha_1, \cdots, \alpha_n$ tels que K est algébrique sur $k(\alpha_1, \cdots, \alpha_n)$. Soit alors $\beta_1, \cdots, \beta_m$ une autre famille algébriquement indépendante. Il nous suffira de montrer que $m \leqslant n$. Nous allons utiliser plusieurs fois le lemme suivant.

Lemme. – *Soient α, β deux éléments de K, chacun transcendant sur un sous-corps k' mais algébriquement liés sur ce sous-corps. Alors α est algébrique sur $k'(\beta)$.*

Démonstration. Il existe un polynôme irréductible $f \in k'[X, Y]$ tel que $f(\alpha, \beta) = 0$. Développons $f = \sum_{k \in \mathbb{N}} g_k(Y) X^k$ avec $g_k \in k'[Y]$. Puisque f est non nul, les polynômes g_k sont non tous nuls. Puisque β est transcendant, les éléments $g_k(\beta)$ sont donc eux aussi non tous nuls. Il s'ensuit que α est racine d'un polynôme non nul à coefficients dans $k'(\beta)$. □

Revenons à la preuve du théorème. Posons $I_0 := \{1, \cdots, n\}$. Puisque β_1 est transcendant sur k, l'ensemble

$$\{I \subset I_0, \beta_1 \text{ est transcendant sur } k((\alpha_i)_{i \in I})\}$$

contient $I=\emptyset$ et est donc non vide. Choisissons I_1 maximal dans cet ensemble. Puisque β_1 est algébrique sur $k(\alpha_1,\cdots,\alpha_n)$, on a $I_1 \subsetneq I_0$. Pour chaque $j\in I_0\setminus I_1$, les éléments β_1 et α_j sont algébriquement liés sur $k((\alpha_i)_{i\in I_1})$ et le lemme nous assure que α_j est algébrique sur $k(\beta_1)((\alpha_i)_{i\in I_1})$. Il s'ensuit que K est algébrique sur $k(\beta_1)((\alpha_i)_{i\in I_1})$.

En particulier, β_2 est algébrique sur $k(\beta_1)((\alpha_i)_{i\in I_1})$, mais transcendant sur $k(\beta_1)$. Donc il existe $I_2\subsetneq I_1$ maximal tel que β_2 est transcendant sur $k(\beta_1)((\alpha_i)_{i\in I_2})$ et, comme ci-dessus, K est alors algébrique sur $k(\beta_1,\beta_2)((\alpha_i)_{i\in I_2})$. Par récurrence, on trouve un sous-ensemble I_m de I_0 tel que K est algébrique sur $k(\beta_1,\cdots,\beta_m)((\alpha_i)_{i\in I_m})$. Comme la suite $I_0\supsetneq I_1\supsetneq\cdots\supsetneq I_m$ est strictement décroissante, on a $0\leqslant |I_m|\leqslant n-m$, ce qui montre que $m\leqslant n$. □

Exemple. – Comme $\mathbb{Q}(X_1,\cdots,X_n)$ est dénombrable pour tout n, on voit que $\mathbb{C}$ est de degré de transcendance infini sur $\mathbb{Q}$.

Remarque. – Si $V\subset\mathbb{C}^n$ est un sous-ensemble algébrique tel que $\mathcal{O}(V)$ est intègre, alors l'entier $\mathrm{deg.tr.}(\mathcal{M}(V)/\mathbb{C})$ joue le rôle d'une dimension. On peut montrer que c'est aussi la longueur de toute chaîne maximale d'idéaux premiers $\mathfrak{p}_0=\{0\}\subsetneq\mathfrak{p}_1\subsetneq\cdots\subsetneq\mathfrak{p}_n\subsetneq\mathcal{O}(V)$.

LEMME. – *Soit $k\subset k'\subset K$ deux extensions de corps. K est de degré de transcendance fini sur k si et seulement si il en est de même de k' sur k et de K sur k'. De plus, on a alors* $\mathrm{deg.tr.}(K/k)=\mathrm{deg.tr.}(K/k')+\mathrm{deg.tr.}(k'/k)$.

Démonstration. Clair. □

2.2 Corps algébriquement clos, clôtures algébriques

2.2.1 DÉFINITION.– *Un corps K est dit algébriquement clos si les conditions équivalentes suivantes sont satisfaites :*
— *tout polynôme $f\in K[X]$ possède une racine dans K*
— *tout polynôme $f\in K[X]$ est scindé*
— *les éléments irréductibles de $K[X]$ sont les polynômes de degré* 1.

On rappelle qu'une "racine de f dans K" est un élément $x\in K$ tel que $(X-x)|f$ (ce qui équivaut à $f(x)=0$), et que "f est scindé" signifie que f se factorise $f=\lambda(X-\alpha_1)\cdots(X-\alpha_n)$. On rappelle aussi le célèbre théorème suivant.

THÉORÈME. – $\mathbb{C}$ *est algébriquement clos.*

Démonstration. Soit $f=X^n+a_1X^{n-1}+\cdots+a_{n-1}X+a_n$. Raisonnons par l'absurde, et supposons que f ne s'annule pas sur $\mathbb{C}$. Montrons que f atteint son minimum sur $\mathbb{C}$. On a $f(0)=a_n\neq 0$. Comme $\lim_{|z|\to+\infty}|P(z)|=+\infty$, il existe donc $R>0$ tel que $|z|>R\Rightarrow|P(z)|>|a_n|$. Comme le disque $D=\{z\in\mathbb{C},|z|\leqslant R\}$ est compact, f y atteint son minimum. Celui-ci est inférieur à $f(0)=|a_n|$ et est donc le minimum de f sur $\mathbb{C}$.

Quitte à faire un changement de variable $X\mapsto X+z_0$ on peut supposer que f atteint son minimum en 0. Quittes à multiplier f par une constante, on peut supposer que $f(0)=1$. Alors, si k est l'ordre d'annulation en 0 de $f-1$, on a $f(z)=1+a_{n-k}z^k+o(z^k)$ au voisinage de $z = 0$. Soit maintenant θ tel que $a_{n-k}e^{ik\theta} = -|a_{n-k}|$ (ie $k\theta = \pi - \arg(a_{n-k})$). Alors $f(re^{i\theta}) = 1 - |a_{n-k}|r^k + o(r^k)$, et donc $f(re^{i\theta}) < 1$ pour r assez petit non nul, ce qui contredit le fait que 1 est le minimum de f. □

2.2.2 DÉFINITION.– *Soit k un corps. Une* clôture algébrique de k *(absolue) est une extension algébrique $k \subset \overline{k}$ avec $\overline{k}$ algébriquement clos.*

LEMME. – *Soit $k \subset K$ une extension avec K algébriquement clos. Alors la clôture algébrique (relative) K_{alg} de k dans K est une clôture algébrique (absolue) de k.*

Démonstration. Par construction, K_{alg} est algébrique sur k. Il s'agit donc de montrer que K_{alg} est algébriquement clos. Soit donc $f \in K_{\mathrm{alg}}[X]$. Puisque K est algébriquement clos, f admet une racine α dans K. Cet élément α est algébrique sur K_{alg}, et donc aussi sur k. Donc il appartient à K_{alg}. □

Exemple. – $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$.

Si on a deux extensions $k \hookrightarrow K$ et $k \hookrightarrow K'$, un *morphisme d'extensions* est un morphisme de k-algèbres, ce qui est la même chose dans ce contexte qu'un morphisme k-linéaire de corps $K \longrightarrow K'$. Il induit donc l'identité sur k. Comme un tel morphisme est toujours injectif, on parle aussi de *plongement*, ou si l'on veut préciser, de *k-plongement.*

2.2.3 PROPOSITION.– *Si $k \subset \overline{k}$ est une clôture algébrique de k, alors toute extension algébrique de k se plonge dans $\overline{k}$.*

Démonstration. Soit K une extension algébrique de k et soit $K' \subset K$ une sous-extension munie d'un plongement $\iota : K' \hookrightarrow \overline{k}$. Le point clef est que pour tout $\alpha \in K$, le plongement ι admet un prolongement à $K'(\alpha)$. En effet, puisque α est algébrique sur k, donc a fortiori sur K', on a $K'(\alpha) = K'[\alpha] \simeq K'[X]/(f_\alpha)$. où $f_\alpha \in K'[X]$ désigne le polynôme minimal de α sur K'. Considérons alors le polynôme $\iota(f_\alpha) \in \overline{k}[X]$ obtenu en appliquant ι aux coefficients de f_α. C'est donc l'image de f_α par l'unique morphisme de K'-algèbres $K'[X] \longrightarrow \overline{k}[X]$ qui envoie X sur X et K' dans $\overline{k}$ via ι. Puisque $\overline{k}$ est algébriquement clos, on peut choisir une racine x de $\iota(f_\alpha)$ dans $\overline{k}$. Considérons alors l'unique morphisme de K'-algèbres φ : $K'[X] \longrightarrow \overline{k}$ qui envoie X sur x et prolonge ι. Pour tout polynôme $f \in K'[X]$ on a $\varphi(f) = \iota(f)(x)$. En particulier $\varphi(f_\alpha) = 0$, donc φ se factorise par un morphisme de K'-algèbres

$$K'[X]/(f_\alpha) \longrightarrow \overline{k}$$

lequel est nécessairement un plongement de corps, et prolonge ι comme voulu. Remarquons cependant que ce prolongement est loin d'être canonique puiqu'il dépend du choix de la racine x de f_α choisie, et même de α, puisque $K'(\alpha)$ admet certainement d'autres générateurs.

On contourne le problème de non-unicité des prolongements en invoquant le lemme de Zorn. Considérons l'ensemble $\mathcal{P}$ des paires (K', ι') formées d'une sous-extension $K' \subset K$ de k et d'un plongement $\iota : K' \hookrightarrow \overline{k}$. Cet ensemble est partiellement ordonné par la relation d'ordre $(K', \iota') \leqslant (K'', \iota'') \Leftrightarrow (K' \subset K''$ et $\iota' = \iota''_{|K'})$. Cet ordre est "inductif", au sens où toute suite croissante possède un majorant. En effet, si $(K'_n, \iota'_n)_{n\in\mathbb{N}}$ est une suite croissante, alors $K' := \bigcup_n K'_n$ est un sous-corps et on définit un plongement ι' en envoyant $x \in K'$ sur $\iota'_n(x)$, qui ne dépend pas du choix de n tel que $x \in K'_n$. Alors la paire (K', ι') majore tous les (K'_n, ι'_n). Maintenant, le lemme de Zorn nous dit alors que tout ensemble ordonnée inductif possède un élément maximal. Soit donc (K', ι') maximal dans $\mathcal{P}$. S'il existait $\alpha \in K \setminus K'$, la construction du début de la preuve contredirait la maximalité de (K', ι'). Donc $K' = K$. □

Corollaire. – *Deux clôtures algébriques $\overline{k}$ et $\overline{k}'$ de k sont isomorphes, en tant qu'extensions de k.*

Démonstration. D'après la proposition, il existe un k-plongement $\overline{k}' \hookrightarrow \overline{k}$. L'image K de ce plongement est un corps isomorphe à $\overline{k}'$, donc algébriquement clos. Tout élément α de $\overline{k}$ est algébrique sur k, donc a fortiori sur K. Son polynôme minimal f_α sur K est de degré 1 puisque K est algébriquement clos, donc de la forme $X - a_0$. Il s'ensuit que $\alpha = a_0 \in K$, puis que $K = \overline{k}$ et $\overline{k}' \xrightarrow{\sim} \overline{k}$. □

Remarque. – Il n'y a généralement pas d'isomorphisme canonique. Par exemple, $\mathbb{C}$, $\mathbb{R}[X]/(X^2+1)$ et $\mathbb{R}[X]/(X^2+X+1)$ sont des clôtures algébriques de $\mathbb{R}$ mais il n'y a pas d'isomorphisme canonique entre ces corps. On peut paraphraser le corollaire en disant : *une clôture algébrique est unique à isomorphisme* ***non*** *unique prés.*

Remarque. – Soit K une extension finie de k. Supposons que K soit monogène et choisissons un élément $\alpha \in K$ tel que $K = k(\alpha)$. Alors, en notant $f_\alpha \in k[X]$ le polynôme minimal de α, la preuve de la proposition fournit une bijection $\iota \mapsto \iota(\alpha)$

$$\{\text{Plongements } k\text{-linéaires } \iota : K \hookrightarrow \overline{k}\} \leftrightarrow \{\text{Racines de } f_\alpha \text{ dans } \overline{k}\}.$$

2.2.4 *Construction d'une clôture algébrique.* Nous allons maintenant prouver l'existence de clôtures algébriques pour tout corps k. Commençons par un moyen inductif de construction de corps :

Lemme. – *Soit $k_0 \xrightarrow{\tau_0} k_1 \xrightarrow{\tau_1} \cdots \xrightarrow{\tau_{n-1}} k_n \xrightarrow{\tau_n} \cdots$ une suite de morphismes de corps. Alors il existe un corps k_∞ muni de plongements $\iota_n : k_n \hookrightarrow k_\infty$ tels que $\iota_n \circ \tau_{n-1} = \iota_{n-1}$ pour tout $n > 0$, et qui satisfait la propriété universelle suivante : pour tout corps K et toute collection $\sigma_n : k_n \longrightarrow K$ de plongements telle que $\sigma_n \circ \tau_{n-1} = \sigma_{n-1}$ pour tout $n > 0$, il existe un unique plongement $k_\infty \xrightarrow{\sigma} K$ tel que $\sigma \circ \iota_n = \sigma_n$ pour tout n.*

Démonstration. Si la suite de morphismes donnée était une suite d'inclusions $k_0 \subset k_1 \subset \cdots \subset k_n \subset \cdots$ à l'intérieur d'un "gros" corps $\mathbb{K}$, il suffirait de prendre $k_\infty := \bigcup_n k_n$. La subtilité ici est qu'on se donne des corps "abstraits" non contenus dans un gros corps, et qu'il faut donc construire de façon "externe" leur "réunion".

Pour cela, considérons la somme directe $\bigoplus_{n\in\mathbb{N}} k_n$. C'est un k_0-ev et même une k_0-algèbre sans unité (un idéal de $\prod_{n\in\mathbb{N}} k_n$). Par définition des sommes directes, on a des inclusions

$\tilde{\iota}_n : k_n \hookrightarrow \bigoplus_{m\in\mathbb{N}} k_m$ qui envoient un élement $x_n \in k_n$ sur la suite nulle partout sauf au rang n où elle vaut x_n. Soit R le sev engendré par les éléments $\tilde{\iota}_n(\tau_{n-1}(x_{n-1})) - \tilde{\iota}_{n-1}(x_{n-1}) = (0, \cdots, 0, -x_{n-1}, \tau_{n-1}(x_{n-1}), 0, 0, \cdots)$ pour $n \in \mathbb{N}^*$ et $x_{n-1} \in k_{n-1}$. Posons

$$k_\infty := \left(\bigoplus_n k_n\right)/R \quad \text{et} \quad \iota_n : k_n \xrightarrow{\tilde{\iota}_n} \bigoplus_{m\in\mathbb{N}} k_m \twoheadrightarrow k_\infty.$$

Par définition, pour tout $n > 0$ on a $\tilde{\iota}_{n-1}(k_{n-1}) \subset \tilde{\iota}_n(k_n) + R$ donc $\iota_{n-1}(k_{n-1}) \subset \iota_n(k_n)$. Comme on a aussi $k_\infty = \sum_{n\in\mathbb{N}} \iota_n(k_n)$, on en déduit que $k_\infty = \bigcup_n \iota_n(k_n)$. Par ailleurs, grâce à l'injectivité des τ_i on voit que toute suite $(x_m)_{m\in\mathbb{N}}$ dans R admet au moins deux termes non nuls. Il s'ensuit que pour tout n on a $\tilde{\iota}_n(k_n) \cap R = \{0\}$ et donc ι_n est injective. Ainsi ι_n induit un isomorphisme k_0-linéaire de k_n sur son image $\iota_n(k_n)$ pour tout n, et chaque inclusion $\iota_{n-1}(k_{n-1}) \subset \iota_n(k_n)$ correspond au morphisme τ_{n-1} via ces isomorphismes. En d'autres termes le diagramme suivant est commutatif :

$$\begin{tikzcd}
k_n \arrow[r, "\sim", "\iota_n"'] & \iota_n(k_n) \\
k_{n-1} \arrow[u, "\tau_{n-1}"] \arrow[r, "\sim", "\iota_{n-1}"'] & \iota_{n-1}(k_{n-1}) \arrow[u, hook]
\end{tikzcd}$$

On peut maintenant munir le k_0-ev k_∞ d'une multiplication : pour $x, y \in k_\infty$, choisissons n assez grand pour que $x, y \in \iota_n(k_n)$ et posons $xy := \iota_n(\iota_n^{-1}(x)\iota_n^{-1}(y))$. Alors cette définition ne dépend pas du choix de n et fait de k_∞ une k_0-algèbre. Comme cette algèbre est réunion des sous-corps $\iota_n(k_n)$, c'est un corps.

La propriété universelle de k_∞ muni des ι_n se prouve sur le même principe : si $x \in k_\infty$ est dans l'image de ι_n on pose $\sigma(x) := \sigma_n(\iota_n^{-1}(x))$, et on a tout fait pour que cela ne dépende pas du choix de n. L'unicité de σ découle du fait que $k_\infty = \bigcup_n \iota_n(k_n)$. $\square$

Nous appliquerons ce lemme sous les hypothèses du suivant :

Lemme. – *Avec les notations du lemme précédent. Supposons que pour tout $n \geqslant 0$ et tout polynôme $f_n \in k_n[X]$, le polynôme $\tau_n(f_n) \in k_{n+1}[X]$ admette une racine dans k_{n+1}. Alors k_∞ est algébriquement clos.*

Démonstration. Soit $f \in k_\infty[X]$. Il existe n tel que les coefficients de f soient dans $\iota_n(k_n)$. Alors f est de la forme $\iota_n(f_n)$ pour un (unique) polynôme $f_n \in k_n[X]$. Par hypothèse, le polynôme $\tau_n(f_n) \in k_{n+1}[X]$ admet une racine x_{n+1} dans k_{n+1}. Il s'ensuit que $\iota_{n+1}(x_{n+1})$ est une racine du polynôme $\iota_{n+1}(\tau_n(f_n)) = \iota_n(f_n) = f$ dans k_∞. Donc k_∞ est algébriquement clos. $\square$

Ainsi, pour prouver l'existence de clôtures algébriques, il suffira d'utiliser inductivement la proposition suivante :

Proposition. – *Soit k un corps. Il existe une extension algébrique K de k dans laquelle tout polynôme $f \in k[X]$ admet une racine.*

Remarque. (Corps de rupture) – Avant de donner la preuve, remarquons qu'il est facile de construire une extension K_f de k dans laquelle un polynôme irréductible $f \in k[X]$ donné admet une racine. Il suffit de prendre $K_f := k[X]/(f)$, qui est un corps puisque (f) est un idéal maximal, et dans lequel X (ou plutôt son image) est une racine de f. Un tel corps K_f s'appelle *corps de rupture* de f.

On peut alors tout aussi facilement construire inductivement une extension $K_{f_1,\cdots,f_n}$ de k dans lequel chacun des polynômes f_i donnés admet une racine. On peut même le faire pour une famille $(f_n)_{n\in\mathbb{N}}$ en utilisant le premier lemme par exemple. Mais en général, l'ensemble des polynômes irréducibles n'est pas nécessairement dénombrable. La preuve qui suit adapte cette idée au cas général.

Démonstration. Notons $(f_i)_{i\in I}$ la famille des polynômes irréducibles unitaires de $k[X]$. Considérons l'anneau de polynômes $\mathcal{R} := k[(X_i)_{i\in I}]$ dont les indéterminées sont indexées par I, et son idéal $\mathcal{I}$ engendré par les $f_i(X_i)$ pour $i \in I$.

Supposons que cet idéal est propre. Alors, par Zorn, il est contenu dans un idéal maximal $\mathfrak{m}$ de $\mathcal{R}$, dont le quotient $K := \mathcal{R}/\mathfrak{m}$ est un corps contenant k. Par construction, l'image de X_i dans K est une racine de f_i dans K. De plus, K est engendré par les images de X_i (en tant qu'extension), donc K est algébrique et satisfait la proposition.

Il nous suffit donc de prouver que $\mathcal{I}$ est bien un idéal propre de $\mathcal{R}$. Raisonnons par l'absurde et supposons que $\mathcal{I} = \mathcal{R}$. Alors il existe un sous-ensemble *fini* $J \subset I$ et des éléments $g_j \in \mathcal{R}$ tels que $\sum_{j\in J} g_j f_j(X_j) = 1$. Puisque J est fini, on a expliqué ci-dessus qu'il existe une extension K_J de k dans laquelle chaque f_j possède une racine, disons x_j. Considérons alors l'unique morphisme de k-algèbres $\mathcal{R} \longrightarrow K_J$ qui envoie X_i sur x_i si $i \in J$ et sur 0 si $i \notin J$. Ce morphisme envoie $f_j(X_j)$ sur $f_j(x_j) = 0$, donc aussi $\sum_{j\in J} g_j f_j(X_j)$ sur 0. Comme $0 \neq 1$ dans le corps K_J on obtient une contradiction. □

2.2.5 THÉORÈME.– *Tout corps possède une clôture algébrique.*

Démonstration. Soit $k = k_0$ un corps. La proposition précédente nous fournit une extension algébrique k_1 dans laquelle tout polynôme $f \in k_0[X]$ possède une racine. Inductivement on en déduit une suite d'extensions algébrique $k_0 \subset k_1 \subset \cdots \subset k_n \subset \cdots$ satisfaisant les hypothèse du second lemme ci-dessus. Mais alors la construction du premier lemme nous fournit un corps algébriquement clos k_∞ contenant k et algébrique sur k. □

2.3 Automorphismes. Extensions normales

Nous commençons cette section en fixant une clôture algébrique $\overline{k}$ de k.

2.3.1 *Automorphismes de $\overline{k}$.* On note généralement

$$\mathrm{Aut}(\overline{k}/k) := \mathrm{Aut}_{k-\mathrm{alg}}(\overline{k}) = \mathrm{Hom}_{k-\mathrm{alg}}(\overline{k}, \overline{k})$$

le groupe des automorphismes de l'extension $\overline{k} \supset k$. Notons que si $\overline{k}'$ est une autre clôture algébrique de k alors tout isomorphisme d'extensions $\psi : \overline{k}' \xrightarrow{\sim} \overline{k}$ induit un isomorphisme $\sigma \mapsto \psi^{-1}\sigma\psi :\ \mathrm{Aut}(\overline{k}/k) \xrightarrow{\sim} \mathrm{Aut}(\overline{k}'/k)$.

LEMME. – *Soit $K \supset k$ une extension algébrique de k et soient $\iota_1, \iota_2 : K \hookrightarrow \overline{k}$ deux k-plongements de K dans $\overline{k}$. Alors il existe un automorphisme $\sigma \in \mathrm{Aut}(\overline{k}/k)$ tel que $\iota_2 = \sigma \circ \iota_1$.*

Démonstration. C'est une conséquence de la proposition 2.2.3. En effet, le plongement ι_2 fournit une clôture algébrique de K. Le plongement ι_1 fait de $\overline{k}$ une extension algébrique de K. La proposition 2.2.3 nous fournit alors un morphisme de K-extensions $\sigma : \overline{k} \longrightarrow \overline{k}$. Mais attention, ici le terme de gauche est une extension de K via ι_1 et celui de droite via ι_2. On a donc $\sigma \circ \iota_1 = \iota_2$ par définition d'un morphisme de K-extensions. Par ailleurs, σ est k-linéaire puisque ι_1 et ι_2 le sont. Donc $\sigma \in \mathrm{Aut}(\overline{k}/k)$. □

2.3.2 *Conjugaison dans $\overline{k}$.*

PROPOSITION. – *Pour $\alpha, \beta \in \overline{k}$, les propriétés suivantes sont équivalentes :*

i) Il existe $\sigma \in \mathrm{Aut}(\overline{k}/k)$, $\sigma(\alpha) = \beta$.

ii) $f_\alpha = f_\beta$ (polynômes minimaux sur k.)

Lorsque ces propriétés sont satisfaites, on dit que α et β sont conjugués.

Démonstration. Pour $\sigma \in \mathrm{Aut}(\overline{k}/k)$, notons encore $\sigma : \overline{k}[X] \longrightarrow \overline{k}[X]$ l'unique automorphisme de k-algèbres qui prolonge σ et envoie X sur X. Ainsi pour tout polynôme $f \in \overline{k}[X]$ et tout $x \in \overline{k}$, on a $\sigma(f(x)) = \sigma(f)(\sigma(x))$. De plus, puisque le polynôme minimal f_x de x sur k est dans $k[X]$, on a $\sigma(f_x) = f_x$.

i) $\Rightarrow$ *ii)*. Supposons que $\beta = \sigma(\alpha)$ pour un $\sigma \in \mathrm{Aut}(\overline{k}/k)$. Alors, $f_\alpha(\beta) = f_\alpha(\sigma(\alpha)) = \sigma(f_\alpha)(\sigma(\alpha)) = \sigma(f_\alpha(\alpha)) = 0$. Donc $f_\beta | f_\alpha$. De même $f_\alpha | f_\beta$ et finalement $f_\alpha = f_\beta$.

ii) $\Rightarrow$ *i)*. Si $f_\alpha = f_\beta$, il existe un unique isomorphisme de k-algèbres $k[\alpha] \xrightarrow{\sim} k[\beta]$ qui envoie α sur β (passer par l'intermédiaire $k[X]/(f)$ avec $f = f_\alpha = f_\beta$). En composant avec l'inclusion $k[\beta] \subset \overline{k}$, on obtient un plongement $\iota :\ k[\alpha] \hookrightarrow \overline{k}$ qui envoie α sur β. Mais alors le lemme précédent appliqué à $K = k[\alpha]$, ι_1 l'inclusion naturelle et $\iota_2 = \iota$ nous fournit un plongement $\sigma :\ \overline{k} \longrightarrow \overline{k}$ qui prolonge ι, et envoie donc α sur β. □

Exemple. – Si $k = \mathbb{R}$ et $\overline{k} = \mathbb{C}$, on a $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, z \mapsto \bar{z}\}$ et la notion de conjugaison de la proposition redonne celle de conjugaison complexe usuelle.

Exemple. – Soit $k = \mathbb{Q}$ et $\overline{k} = \overline{\mathbb{Q}}$. L'ensemble des conjugués de $\sqrt[3]{2}$ est $\{\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\}$, où $j = \frac{-1+i\sqrt{3}}{2}$ est une racine 3-ème primitive de l'unité.

2.3.3 *Sous-extensions normales de $\overline{k}$.*

PROPOSITION. – *Soit K une sous-extension de $\overline{k}$. Les propriétés suivantes sont équivalentes :*

i) Pour tout $\alpha \in K$, les racines de f_α dans $\overline{k}$ appartiennent à K.

ii) Pour tout $\sigma \in \mathrm{Aut}(\overline{k}/k)$, on a $\sigma(K) \subset K$.

Si ces propriétés sont satisfaites on dit que K est une sous-extension normale de $\overline{k}$.

Démonstration. *i)* $\Rightarrow$ *ii)*. Soit $\sigma \in \mathrm{Aut}(\overline{k}/k)$ et $\alpha \in K$. La proposition précédente nous dit que $\sigma(\alpha)$ est une racine de f_α, donc l'hypothèse i) implique que $\sigma(\alpha) \in K$. D'où ii).

ii) $\Rightarrow$ *i)*. Soit $\alpha \in K$ et β une autre racine de f_α. Alors $f_\beta = f_\alpha$ et la proposition précédente nous fournit σ tel que $\sigma(\alpha) = \beta$. Puisque K est stable par σ (hypothèse ii)), on a bien $\beta \in K$. □

Corollaire. – *Soit $K \subset \overline{k}$ une sous-extension normale. L'application de restriction $\sigma \mapsto \sigma_{|K}$ induit un morphisme de groupes surjectif*

$$\mathrm{Aut}(\overline{k}/k) \twoheadrightarrow \mathrm{Aut}(K/k)$$

dont le noyau est $\mathrm{Aut}(\overline{k}/K)$.

Démonstration. Le ii) de la proposition précédente nous dit que l'application est bien définie. C'est évidemment un morphisme de groupes. Enfin, le dernier lemme nous assure que tout automorphisme γ de K se prolonge en un automorphisme σ de $\overline{k}$: il suffit d'appliquer ce lemme à ι_1 l'inclusion naturelle et ι_2 la composée de γ et de l'inclusion naturelle. D'où la surjectivité annoncée. Le noyau est formé des automorphismes $\sigma \in \mathrm{Aut}(\overline{k}/k)$ tels que $\sigma_{|K} = \mathrm{id}_K$, c'est-à-dire des automorphismes de K-algèbres de $\overline{k}$ comme annoncé. □

Exemple. – Soit $k = \mathbb{Q}$ et $\overline{k} = \overline{\mathbb{Q}}$.
- L'extension $\mathbb{Q}[j]$ de $\mathbb{Q}$ est normale (de degré 2) puisque tout $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}})$ envoie j sur j ou j^2, donc laisse stable $\mathbb{Q}[j]$.
- L'extension $\mathbb{Q}[\sqrt[3]{2}]$ de $\mathbb{Q}$ (de degré 3) n'est pas normale, car il existe $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}})$ tel que $\sigma(\sqrt[3]{2}) = j\sqrt[3]{2} \notin \mathbb{Q}[\sqrt[3]{2}]$.
- L'extension $\mathbb{Q}[j, \sqrt[3]{2}]$ de $\mathbb{Q}$ est normale (de degré 6).

2.3.4 *Extensions normales.* Ici nous ne travaillons pas à l'intérieur d'une clôture $\overline{k}$ fixée.

Proposition. – *Soit $K \supset k$ une extension algébrique. Les propriétés suivantes sont équivalentes :*

i) Pour tout $\alpha \in K$, le polynôme f_α est scindé dans $K[X]$.

ii) Si ι_1, ι_2 sont deux plongements de K dans une clôture algébrique $\overline{k}$ alors $\iota_1(K) = \iota_2(K)$.

iii) L'image de K par tout plongement dans une clôture algébrique est une sous-extension normale au sens du paragraphe précédent.

Si ces propriétés sont satisfaites, $K \supset k$ est dite normale

Démonstration. $i) \Rightarrow ii)$. Soit $\alpha \in K$. Puisque f_α est scindé, chacun des plongements ι_1, ι_2 induit une bijection de l'ensemble des racines de f_α dans K dans celui des racines de f_α dans $\overline{k}$. En particulier $\iota_2(\alpha)$ est une racine de f_α, donc de la forme $\iota_1(\beta)$ et en particulier dans $\iota_1(K)$. Ceci montre $\iota_2(K) \subset \iota_1(K)$ et l'autre inclusion suit par symétrie.

$ii) \Rightarrow iii)$. Soit $\iota : K \hookrightarrow \overline{k}$. Pour tout $\sigma \in \mathrm{Aut}(\overline{k}/k)$, ii) implique que $\sigma(\iota(K)) = \iota(K)$, donc $\iota(K)$ est une sous-extension normale de $\overline{k}$.

$iii) \Rightarrow i)$. On peut plonger K dans une clôture algébrique $\iota : K \hookrightarrow \overline{k}$. Le polynôme $\iota(f_\alpha)$ est alors scindé dans $\overline{k}[X]$: on peut l'écrire $\iota(f_\alpha) = \prod_{i=1}^m (X - x_i)^{v_i}$. Mais iii) implique que les x_i sont dans $\iota(K)$, disons $x_i = \iota(\alpha_i)$. Il s'ensuit que $f_\alpha = \prod_i (X - \alpha_i)^{v_i}$ est scindé dans $K[X]$. $\square$

Exemple. – Reprenons l'exemple du paragraphe précédent de manière "abstraite" (i.e. non plongée dans $\overline{\mathbb{Q}}$). L'extension $\mathbb{Q}[X]/(X^2 + X + 1) \supset \mathbb{Q}$ est normale et l'extension $\mathbb{Q}[X]/(X^3 - 2) \supset \mathbb{Q}$ ne l'est pas.

2.3.5 *Corps de décomposition d'un polynôme.* Voici l'exemple fondamental d'extension normale.

DÉFINITION. – *Soit $f \in k[X]$. Un* corps de décomposition *de f est une extension K de k telle que*

— *f est* scindé *dans $K[X]$, c-à-d $\exists x_1, \cdots, x_n \in K$ tels que $f = \lambda \prod_{i=1}^n (X - x_i)$,*

— *K est engendrée par les racines x_i de f.*

COROLLAIRE. – *Tout polynôme admet un corps de décomposition, et celui-ci est unique à isomorphisme (non unique) près. De plus, ce corps est un extension normale de k.*

Démonstration. Soit $\overline{k}$ une clôture algébrique de k. Le polynôme f se scinde en $f = \lambda \prod_{i=1}^n (X - x_i)$ avec $\lambda \in k$ et $x_1, \cdots, x_n \in \overline{k}$. Alors le sous-corps $K_f = k(x_1, \cdots, x_n)$ de $\overline{k}$ est un corps de décomposition de f. Soit maintenant $K' \supset k$ un autre corps de décomposition de f. Alors K' est algébrique sur k donc se plonge dans $\overline{k}$. Son image est engendrée par les racines de f donc égale à K_f. Donc K' est isomorphe à K_f. Ceci montre aussi que K_f est normale. $\square$

Exemple. – Le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$ est le corps $\mathbb{Q}[j, \sqrt[3]{2}]$.

Exercice. – Soient $n, m \in \mathbb{N}$. Montrer que le corps de décomposition de $X^n - m$ est $\mathbb{Q}[\zeta_n, \sqrt[n]{m}]$ où $\zeta_n = \exp(2i\pi/n)$ et $\sqrt[n]{m}$ est l'unique racine n-ème réelle positive de m.

Remarque. – L'action de $\mathrm{Aut}(K_f/k)$ sur K_f permute l'ensemble $f^{-1}(0)$ des racines de f dans K_f. Comme celles-ci engendrent K_f, on a une injection dans le groupe de permutations

$$\mathrm{Aut}(K_f/k) \hookrightarrow \mathfrak{S}_{f^{-1}(0)}.$$

L'idée basique de la théorie de Galois est d'utiliser le groupe $\mathrm{Aut}(K_f/k)$ comme groupe de symétries de l'équation algébrique $f = 0$. Néanmoins, ce groupe peut parfois être trivial : prenons $k = \mathbb{F}_p(T)$ et $f = X^p - T$. Dans ce cas $K_f = \mathbb{F}_p(T)[X]/(X^p - T) = \mathbb{F}_p(T^{1/p})$. En fait, f se factorise en $X^p - T = (X - T^{1/p})^p$ dans K_f, ce qui montre que $T^{1/p}$ est la seule racine p-ème de T (avec multiplicité p). Donc le groupe $\mathfrak{S}_{f^{-1}(0)}$ est trivial et $\mathrm{Aut}(K_f/k)$ aussi. Ce phénomène appelé “inséparabilité” est étudié dans les sections suivantes.

2.4 Caractéristique et endomorphisme de Frobenius

2.4.1 *Caractéristique d'un corps.* Soit A un anneau commutatif. Il existe un *unique* morphisme d'anneaux $\mathbb{Z} \longrightarrow A$. En effet, un tel morphisme doit envoyer 1 sur 1_A et n sur $1_A + \cdots + 1_A$ (n fois). Le noyau de ce morphisme est appelé *idéal caractéristique* de A. Lorsque $A = k$ est un corps, deux cas peuvent se produire :
— l'idéal caractéristique est nul auquel cas on dit que k *est de caractéristique nulle.*
— l'idéal caractéristique est premier, donc engendré par un unique nombre premier p, auquel cas on dit que k *est de caractéristique* p.

Remarque. – Si p est un nombre premier, on dit plus généralement qu'un anneau A est “de caractéristique p” si l'idéal caractéristique de A est égal à (p). Dans ce cas, le morphisme $\mathbb{Z} \longrightarrow A$ se factorise par $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, le corps fini à p éléments, et A est donc une $\mathbb{F}_p$-algèbre. Réciproquement, toute $\mathbb{F}_p$-algèbre est un anneau de caractéristique p.

2.4.2 *Sous-corps premier.* On appelle *sous-corps premier* d'un corps k le plus petit sous-corps de k, c'est-à-dire l'intersection de tous les sous-corps de k. Deux cas peuvent se produire :
— Si k est de caractéristique nulle, alors k contient $\mathbb{Z}$ donc $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$ et le sous-corps premier de k est donc $\mathbb{Q}$.
— Si k est de caractéristique $p > 0$, alors k contient $\mathbb{F}_p$, qui est donc le sous-corps premier de k.

2.4.3 *Endomorphisme de Frobenius.*

PROPOSITION. – *Soit A un anneau de caractéristique p. Alors l'application*

$$F_A : A \longrightarrow A,\ a \mapsto a^p$$

est un endomorphisme de $\mathbb{F}_p$-algèbres. On l'appelle endomorphisme de Frobenius de A.

Démonstration. Soit $a, b \in A$. On a clairement $(ab)^p = a^p b^p$. Par ailleurs on a $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$ avec $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Maintenant, pour $0 < k < p$, p ne divise ni $k!$ ni $(p-k)!$. Mais p divise $p!$, donc divise $\binom{p}{k}$. Il s'ensuit que, dans A, on a $(a+b)^p = a^p + b^p$. $\square$

Remarque. – Les endomorphismes de Frobenius “commutent” avec n'importe quel morphisme de $\mathbb{F}_p$-algèbres : si $\varphi : A \longrightarrow B$ est un tel morphisme, alors $\varphi \circ F_A = F_B \circ \varphi$.

Pour un corps k de caractéristique p, notons

$$k^F := \{x \in k,\ F_k(x) = x\}$$

l'ensemble des points fixes de l'endomorphisme de Frobenius. C'est un sous-corps de k, puisque F_k est un endomorphisme de corps.

LEMME. – *k^F est le sous-corps premier $\mathbb{F}_p$ de k.*

Démonstration. Pour $x \in k$, on a $F_k(x) = x \Leftrightarrow x^p = x \Leftrightarrow (X-x)|(X^p - X)$ dans $k[X]$. Par ailleurs, pour tout $a \in \mathbb{F}_p$ on a $a^p = a$. Comme les polynômes irréductibles $X - a$ sont deux à deux premiers entre eux lorsque a décrit $\mathbb{F}_p$, on a la factorisation $X^p - X = \prod_{a \in \mathbb{F}_p}(X-a)$ dans $\mathbb{F}_p[X]$ et dans $k[X]$. Donc $x \in \mathbb{F}_p$. □

Plus généralement, pour tout $r \in \mathbb{N}^*$, le sous-ensemble

$$k^{F^r} := \{x \in k, F_k^r(x) = x\}$$

des points fixes de l'endomorphisme $F_k^r = F_k \circ F_k \circ \cdots \circ F_k$ est un sous-corps de k. Le cas où k est une clôture algébrique de $\mathbb{F}_p$ est particulièrement intéressant.

2.4.4 *Corps finis.* Choisissons une clôture algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$ et notons F son automorphisme de Frobenius.

THÉORÈME. – *Le corps $\overline{\mathbb{F}}_p^{F^r}$ est un corps de décomposition du polynôme $X^{p^r} - X$ sur $\mathbb{F}_p$. Réciproquement, toute extension finie de $\mathbb{F}_p$ est un corps de décomposition du polynôme $X^{p^{[k:\mathbb{F}_p]}} - X$ sur $\mathbb{F}_p$.*

Démonstration. Pour $x \in \overline{\mathbb{F}}_p$, on a $F^r(x) = x \Leftrightarrow$ (x racine de $X^{p^r} - X$). Ainsi $\overline{\mathbb{F}}_p^{F^r}$ est l'ensemble des racines de $X^{p^r} - X$ dans $\overline{\mathbb{F}}_p$. Comme c'est un corps, c'est donc en particulier un corps de décomposition de $X^{p^r} - X$.

Réciproquement, soit k une extension finie de $\mathbb{F}_p$. Notons $r := [k : \mathbb{F}_p]$ sa dimension sur $\mathbb{F}_p$. Alors k est fini de cardinal $|k| = p^r$, donc son groupe multiplicatif $k^\times$ est de cardinal $p^r - 1$ donc tout élément $x \in k^\times$ vérifie $x^{p^r-1} = 1$. Il s'ensuit que tout élément x de k est racine du polynôme $X(X^{p^r} - 1) = X^{p^r} - X$. En particulier, k est un corps de décomposition de ce polynôme. □

Comme tout corps fini est extension finie de son corps premier, ce théorème donne une recette pour "construire" tous les corps finis. Il dit aussi que, à isomorphisme près, il y a au plus un corps de cardinal p^r pour p premier et $r \in \mathbb{N}^*$. Pour compléter le théorème, il reste à calculer le cardinal de $\overline{\mathbb{F}}_p^{F^r}$, ce qui revient à compter les racines de $X^{p^r} - X$ (il y en a au plus p^r).

2.5 Polynômes et extensions séparables.

2.5.1 *Dérivation des polynômes.* Soit A une k-algèbre. Une *dérivation* ∂ de A est un endomorphisme k-linéaire de A qui vérifie l'axiome :

$$\forall f, g \in A, \;\; \partial(fg) = \partial(f)g + f\partial(g).$$

Ainsi, on constate par récurrence que $\partial(f^n) = n\partial(f)$ pour tout $n \in \mathbb{N}$ et en particulier $\partial(\lambda) = \lambda\partial(1) = 0$ pour tout $\lambda \in k$.

Sur l'algèbre $A = k[X]$, toute dérivation est donc uniquement déterminée par sa valeur en X. Notons ∂ l'unique dérivation de $k[X]$ telle que $\partial(X) = 1$. Pour un polynôme $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ on a donc

$$\partial f = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1.$$

On appelle ∂f le *polynôme dérivé* de f et on le note f' en l'absence d'ambiguïté.

Remarque. – Soit $\tau : k \to k'$ un morphisme de corps. Notons aussi $\tau : k[X] \longrightarrow k'[X]$ le morphisme d'anneaux qui prolonge τ et envoie X sur X. Alors $\forall f \in k[X]$, $\tau(f)' = \tau(f')$.

Lemme. – *Soit $f \in k[X]$ tel que $f' = 0$.*

i) Si k est de caractéristique nulle, alors $\deg(f) = 0$.

ii) Si k est de caractéristique $p > 0$, alors il existe un unique polynôme $g \in k[X]$ tel que $f = g(X^p)$.

Démonstration. i) est clair. ii) En écrivant $f = \sum_n a_nX^n$ et $f' = \sum_n na_nX^{n-1} = 0$, on voit que $a_n \neq 0 \Rightarrow p|n$ donc $f = \sum_{m\in\mathbb{N}} a_{pm}X^{pm} = g(X^p)$ pour $g = \sum_m a_{pm}X^m$. L'unicité de g est claire. □

2.5.2 *Polynômes séparables.*

Définition. – *Un polynôme $f \in k[X]$ est dit* séparable *si l'idéal (f, f') de $k[X]$ est l'idéal unité (ie f et f' sont premiers entre eux).*

Soit $f \in k[X]$. Si $\overline{k}$ est une clôture algébrique de k, alors f se scinde dans $\overline{k}[X]$ en $f = a_n(X - \alpha_1)^{v_1} \cdots (X - \alpha_m)^{v_m}$ où a_n est le terme dominant de f (ie $n = \deg(f)$), $\sum_{i=1}^m v_i = n$ et les $\alpha_i \in \overline{k}$ sont *supposés distincts*. Les α_i sont donc les racines de f dans $\overline{k}$ et v_i est la "*multiplicité*" de la racine α_i.

Proposition. – *Pour $f \in k[X]$, les propriétés suivantes sont équivalentes :*

i) f est séparable.

ii) f et f' n'ont pas de racine commune dans une clôture algébrique de k.

iii) Toutes les racines de f dans une clôture algébrique de k sont de multiplicité 1.

iii') f possède $\deg(f)$ *racines distinctes dans toute clôture algébrique.*

iii") Si $\overline{k}$ est une clôture algébrique de k, la $\overline{k}$-algèbre $\overline{k}[X]/(f)$ est réduite (auquel cas, elle est isomorphe à $\overline{k}^{\deg(f)} = \overline{k} \times \overline{k} \times \cdots \times \overline{k}$).

Démonstration. *i) ⇒ ii)*. Soit $\overline{k}$ une clôture algébrique de k. Si $g, h \in k[X]$ sont tels que $fg + f'h = 1$, alors la même égalité dans $\overline{k}[X]$ montre que f et f' n'y ont pas de diviseur irréductible commun, donc pas de racine commune.

ii) $\Rightarrow$ *iii)*. Montrons la contraposée. Supposons donc que f possède une racine double α dans une clôture algébrique $\overline{k}$. Il existe donc $g \in \overline{k}[X]$ tel que $f = (X-\alpha)^2 \cdot g$. Il s'ensuit que $f' = (X-\alpha)(2g + (X-\alpha)g')$, ce qui montre que α est une racine commune à f et f'.

iii) $\Rightarrow$ *i)*. Montrons encore la contraposée. Si (f, f') n'est pas l'idéal unité de $k[X]$ alors f et f' admettent un diviseur irréductible commun, disons $h \in k[X]$. Il existe donc $g \in k[X]$ tel que $f = hg$. En dérivant, on obtient $f' = h'g + hg'$. Comme $h|f'$, on en déduit que $h|h'g$. Deux choses peuvent se produire :

— Si $h' \neq 0$, alors h ne divise pas h' car $\deg(h') < \deg(h)$, donc d'après le lemme d'Euclide, h divise g. Il s'ensuit que h^2 divise f. Or h admet une racine dans $\overline{k}$ et celle-ci est donc une racine double de f.

— Si $h' = 0$, alors d'après le lemme précedent, k est de caractéristique $p > 0$ et $h = e(X^p)$ pour un $e \in k[X]$. Alors e admet une racine α dans $\overline{k}$ et donc $X^p - \alpha$ divise h dans $k[X]$. Mais α admet une racine p-ème β dans $\overline{k}$, donc $X^p - \alpha = (X-\beta)^p$ et β est racine multiple de h et donc de f.

L'équivalence entre *iii)* et *iii')* est évidente. Il reste à vérifier que *iii)* $\Leftrightarrow$ *iii'')*. Pour cela, on scinde $f = a_n(X-\alpha_1)^{v_1} \cdots (X-\alpha_m)^{v_m}$ dans $\overline{k}[X]$ avec les α_i distincts deux à deux, et on constate grâce aux restes chinois que

$$\overline{k}[X]/(f) = \prod_{i=1}^{m} \overline{k}[X]/(X-\alpha_i)^{v_i}.$$

Cet anneau est réduit si et seulement si chacun de ses facteurs $\overline{k}[X]/(X-\alpha_i)^{v_i}$ est réduit, ce qui équivaut à $v_i = 1$. Dans ce cas on a $m = \deg(f)$ et donc $\overline{k}[X]/(f) \simeq \overline{k}^{\deg(f)}$. □

Remarque. – On voit grâce à la propriété iii) que si f divise un polynôme séparable alors f est séparable.

Application. (Corps finis) – On peut maintenant compléter le théorème 2.4.4. Puisque le polynôme $X^{p^r} - X$ est séparable (son polynôme dérivé est $f' = -1$), il admet p^r racines distinctes dans $\overline{\mathbb{F}}_p$. Il s'ensuit, d'après le théorème 2.4.4, que son corps de décomposition $\overline{\mathbb{F}}_p^{F^r}$ est de cardinal p^r. On obtient ainsi le théorème de classification des corps finis :

2.5.3 THÉORÈME.– *Pour toute puissance p^r d'un nombre premier, il existe un corps $\mathbb{F}_{p^r}$ de cardinal p^r, unique à isomorphisme près. C'est un corps de décomposition du polynôme $X^{p^r} - X$ sur $\mathbb{F}_p$. Tout corps fini est de cette forme.*

Démonstration. Soit k un corps fini. Il est nécessairement de caractéristique non nulle, disons p. Il est de degré fini, disons r, sur son corps premier $\mathbb{F}_p$, donc, d'après le théorème 2.4.4, c'est le corps de décomposition de $X^{p^r} - X$. Voici pour l'unicité. L'existence vient du théorème 2.4.4 et de la séparabilité de $X^{p^r} - X$, comme expliqué ci-dessus. □

2.5.4 *Extensions séparables.*

DÉFINITION. – *Soit $K \supset k$ une extension algébrique. On dit que*

— *$\alpha \in K$ est séparable sur k, si son polynôme minimal $f_\alpha \in k[X]$ est séparable.*
— *K est séparable sur k si tout élément de K est séparable sur k.*

Afin de donner un analogue de la proposition 2.5.2 pour les extensions, il faut se demander quel est l'analogue, pour une extension, de la notion de racine d'un polynôme. Pour cela, il faut se rappeler la bijection suivante, pour $f \in k[X]$ irréductible :

$$\mathrm{Hom}_{k-\mathrm{alg}}(K[X]/(f), \overline{k}) \xrightarrow{\sim} \{\alpha \in \overline{k}, f(\alpha) = 0\}$$

donnée par $\iota \mapsto \iota(\overline{X})$ où $\overline{X}$ est l'image de X dans $K[X]/(f)$. Ainsi l'analogue de la notion de racine est la notion de plongement. Le lemme suivant nous dit que, tout comme un polynôme f possède au plus $\deg(f)$ racines, une extension finie $K \supset k$ admet au plus $[K : k]$ plongements.

Proposition. – *Soit $K \supset k$ une extension finie et $\overline{k}$ une clôture algébrique de k. Alors le nombre de k-plongements de K dans $\overline{k}$ vérifie l'inégalité*

$$|\mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k})| \leqslant [K : k].$$

Démonstration. La propriété universelle de l'extension des scalaires fournit une bijection

$$\mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k}) \xrightarrow{\sim} \mathrm{Hom}_{\overline{k}-\mathrm{alg}}(\overline{k} \otimes_k K, \overline{k}), \quad \iota \mapsto \tau,$$

caractérisée par l'égalité $\tau(\lambda \otimes \alpha) = \lambda\iota(\alpha)$. Posons $I := \mathrm{Hom}_{\overline{k}-\mathrm{alg}}(\overline{k} \otimes_k K, \overline{k})$ et considérons le morphisme produit

$$\Pi\tau : \ \overline{k} \otimes_k K \longrightarrow \overline{k}^I, \ \lambda \otimes \alpha \mapsto (\tau(\lambda \otimes \alpha))_{\tau \in I}.$$

Le lemme suivant nous dit que ce morphisme est surjectif, donc

$$[K : k] = \dim_{\overline{k}}(\overline{k} \otimes_k K) \geqslant \dim_{\overline{k}}(\overline{k}^I) = |\mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k})|.$$

Lemme. – *Soit A une $\overline{k}$-algèbre commutative de dimension finie. Alors le morphisme*

$$\Pi\tau : A \longrightarrow \overline{k}^{\mathrm{Hom}_{\overline{k}-\mathrm{alg}}(A, \overline{k})}, \quad a \mapsto (\tau(a))_{\tau \in \mathrm{Hom}_{\overline{k}-\mathrm{alg}}(A, \overline{k})}$$

est surjectif et son noyau est le nilradical de A.

Démonstration. Fixons un morphisme $\tau : A \longrightarrow \overline{k}$ de $\overline{k}$-algèbres. Alors τ est surjectif puisque $\tau(\lambda \cdot 1_A) = \lambda$ pour tout $\lambda \in \overline{k}$. Donc $\mathfrak{m} := \mathrm{Ker}(\tau)$ est un idéal maximal de A, et τ se factorise en $\tau : A \twoheadrightarrow A/\mathfrak{m} \xrightarrow{\overline{\tau}} \overline{k}$ avec $\overline{\tau}$ bijectif. En fait, $\overline{\tau}$ est déterminé par $\mathfrak{m}$. En effet, la composée $\iota_{\mathfrak{m}} : \overline{k} \longrightarrow A \longrightarrow A/\mathfrak{m}$ fait de $A/\mathfrak{m}$ une extension finie de $\overline{k}$, donc est un isomorphisme puisque $\overline{k}$ est algébriquement clos. Mais alors, $\overline{\tau} \circ \iota_{\mathfrak{m}}$ est un automorphisme de la $\overline{k}$-algèbre $\overline{k}$, donc est l'identité. Il s'ensuit que τ coïncide avec le morphisme $\tau_{\mathfrak{m}} : A \twoheadrightarrow A/\mathfrak{m} \xrightarrow{\iota_{\mathfrak{m}}^{-1}} \overline{k}$. On a donc montré que

$$\mathrm{Hom}_{\overline{k}-\mathrm{alg}}(A, \overline{k}) = \{\tau_{\mathfrak{m}}, \mathfrak{m} \in \mathrm{Max}(A)\}$$

et que l'application $\Pi\tau$ de l'énoncé se factorise en

$$A \longrightarrow \prod_{\mathfrak{m}\in \mathrm{Max}(A)} A/\mathfrak{m} \xrightarrow{\sim} \overline{k}^{\mathrm{Hom}_{\overline{k}-\mathrm{alg}}(A,\overline{k})}$$

où la première flèche est $a \mapsto (a \,(\mathrm{mod}\, \mathfrak{m}))_{\mathfrak{m}\in\mathrm{Max}(A)}$ et la seconde est le produit $\prod_{\mathfrak{m}} \iota_{\mathfrak{m}}^{-1}$. Le théorème des restes chinois nous dit alors que $\Pi\tau$ est surjective. De plus, son noyau est $\bigcap_{\mathfrak{m}\in\mathrm{Max}(A)} \mathfrak{m}$. Or, puisque A est de longueur finie comme A-module, on sait que A est annulé par un produit fini d'idéaux maximaux. Il est donc annulé par une puissance convenable de $\bigcap_{\mathfrak{m}\in\mathrm{Max}(A)} \mathfrak{m}$, ce qui signifie que $\bigcap_{\mathfrak{m}\in\mathrm{Max}(A)} \mathfrak{m}$ est nilpotent, donc inclus dans le nilradical $\mathcal{N}(A)$ de A. Réciproquement, puisque le quotient $A/\bigcap_{\mathfrak{m}\in\mathrm{Max}(A)} \mathfrak{m}$ est réduit, on a aussi $\mathcal{N}(A) \subset \bigcap_{\mathfrak{m}\in\mathrm{Max}(A)} \mathfrak{m}$, d'où l'égalité. □

□

Théorème. – *Soit $K \supset k$ une extension finie. On a équivalence entre :*

i) K est séparable sur k

ii) Pour toute clôture algébrique $\overline{k}$ de k on a l'égalité $|\mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k})| = [K:k]$.

iii) Pour toute clôture algébrique $\overline{k}$ de k, la $\overline{k}$-algèbre $\overline{k}\otimes_k K$ est réduite (auquel cas elle est isomorphe à $\overline{k}^{[K:k]} = \overline{k}\times\overline{k}\times\cdots\times\overline{k}$).

Démonstration. L'équivalence *ii*) ⇔ *iii*) découle immédiatement du lemme ci-dessus, via le raisonnement de la preuve de la proposition.

i) ⇒ *ii*). Commençons par la remarque suivante. Soit $K' \subset K$ une sous-k-extension de K, et considérons l'application de restriction

$$\mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k}) \longrightarrow \mathrm{Hom}_{k-\mathrm{alg}}(K',\overline{k}),\ \iota \mapsto \iota_{|K'}.$$

La proposition 2.2.3 nous dit que cette application est surjective. De plus, la fibre au-dessus de $\iota' : K' \hookrightarrow \overline{k}$ est l'ensemble $\mathrm{Hom}_{K'-\mathrm{alg},\iota'}(K,\overline{k})$ des plongements $K \hookrightarrow \overline{k}$ qui prolongent ι', *i.e.* des morphismes de K'-algèbres pour lesquels $\overline{k}$ est muni de la structure de K'-algèbre donnée par ι'. On a donc

$$|\mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k})| = \sum_{\iota'\in\mathrm{Hom}_{k-\mathrm{alg}}(K',\overline{k})} |\mathrm{Hom}_{K'-\mathrm{alg},\iota'}(K,\overline{k})|.$$

En particulier, si on sait que $|\mathrm{Hom}_{K'-\mathrm{alg},\iota'}(K,\overline{k})| = [K:K']$ pour tout ι et $|\mathrm{Hom}_{k-\mathrm{alg}}(K',\overline{k})| = [K':k]$, alors on obtient

$$(*) \qquad |\mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k})| = [K':k][K:K'] = [K:k].$$

Cette remarque nous permet de faire un raisonnement par récurrence sur le nombre de générateurs r de K sur k. Si $r=1$, K est de la forme $K = k[\alpha_1] = k[X]/(f_{\alpha_1})$ et on a vu ci-dessus que $\mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k})$ est en bijection avec l'ensemble des racines f_{α_1} qui est de cardinal $\deg(f_{\alpha_1}) = [K : k]$ puisque α_1 est séparable. Supposons K engendré par r éléments $\alpha_1, \cdots, \alpha_r$ et notons $K' := k[\alpha_1, \cdots, \alpha_{r-1}]$. Par récurrence, on peut supposer que $|\mathrm{Hom}_{k-\mathrm{alg}}(K', \overline{k})| = [K' : k]$. De plus, puisque K est engendrée sur K' par (au plus) 1 élément α_r, on a $|\mathrm{Hom}_{K'-\mathrm{alg},\iota'}(K, \overline{k})| = [K : K']$ pour tout plongement $\iota' : K' \hookrightarrow \overline{k}$ (un tel plongement fait de $\overline{k}$ une clôture algébrique de K'). On conclut par $(*)$.

iii) $\Rightarrow$ *i)*. Avant de prouver cette implication, remarquons que pour toute sous-extension $K' \subset K$, le morphisme canonique de $\overline{k}$-algèbre $\overline{k} \otimes_k K' \longrightarrow \overline{k} \otimes_k K$ est injectif. En effet, si $(e_i)_{i\in I}$ est une base du k-ev K telle que $(e_i)_{i\in I'}$ soit une base du k-ev K', alors $(1 \otimes e_i)_{i\in I}$ est une base du $\overline{k}$-ev $\overline{k} \otimes_k K$ et la sous-famille $(1 \otimes e_i)_{i\in I'}$ est une base du $\overline{k}$-ev $\overline{k} \otimes_k K'$. Il s'ensuit donc que si $\overline{k} \otimes_k K$ est réduite, alors $\overline{k} \otimes_k K'$ l'est aussi. Appliquons ceci à $K' = k[\alpha]$ pour $\alpha \in K$ quelconque. Alors $\overline{k} \otimes_k k[\alpha]$ est réduite, donc puisque $k[\alpha] \simeq k[X]/(f_\alpha)$, f_α est séparable d'après le iii") de la proposition 2.5.2. Comme α était quelconque, K est séparable sur k. $\square$

Application. – Si $f \in k[X]$ est séparable, $k[X]/(f)$ est une extension séparable de k. Cela découle en effet de l'implication *iii)* $\Rightarrow$ *i)*.

Corollaire. (De la preuve) – *Soit $k \subset K' \subset K$ une tour d'extensions finies. Si K est séparable sur K' qui est séparable sur k, alors K est séparable sur k.*

Démonstration. On répète l'argument utilisé pour l'implication *i)* $\Rightarrow$ *ii)* pour obtenir l'égalité $(*)$ de cette preuve, qui montre que K est séparable sur k. $\square$

Application. – Une extension finie K engendrée par des éléments séparables est séparable (récurrence sur le nombre de générateurs). En particulier, un corps de décomposition d'un polynôme séparable de $k[X]$ est séparable sur k.

Remarque. – Pour une extension algébrique $K \supset k$ *infinie*, l'assertion ii) du théorème n'a pas de sens. Mais le raisonnement utilisé donne l'équivalence :

$$K \text{ séparable sur } k \Leftrightarrow \overline{k} \otimes_k K \text{ est réduite.}$$

2.5.5 *Théorème de l'élément primitif.* Le corollaire suivant est assez spectaculaire pour qu'on lui donne un nom évocateur.

Corollaire. (Théorème de l'élément primitif) – *Toute extension finie séparable $K \supset k$ est monogène (i.e. engendrée par un seul élément).*

Démonstration. Soit $\alpha \in K$, et considérons l'application de restriction

$$\mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k}) \longrightarrow \mathrm{Hom}_{k-\mathrm{alg}}(k[\alpha], \overline{k}), \quad \iota \mapsto \iota_{|k[\alpha]}.$$

On a vu que cette application est surjective, que la source est de cardinal $[K : k]$ (puisque K est supposée séparable) et la cible de cardinal $[k[\alpha] : k] = \deg(f_\alpha)$ (puisque α est séparable). On a donc l'équivalence

$$K = k[\alpha] \Leftrightarrow [K : k] = [k[\alpha] : k] \Leftrightarrow (\iota \mapsto \iota_{|k[\alpha]} \text{ est injective}).$$

Par ailleurs, l'application $\iota' \mapsto \iota'(\alpha)$, est une injection de $\mathrm{Hom}_{k-\mathrm{alg}}(k[\alpha], \overline{k})$ dans $\overline{k}$ (puisque c'est même une bijection sur l'ensemble des racines de f_α dans $\overline{k}$). On a donc

$$K = k[\alpha] \Leftrightarrow (\iota \mapsto \iota(\alpha) \text{ est injective}) \Leftrightarrow \alpha \notin \bigcup_{\iota_1 \neq \iota_2} \mathrm{Ker}(\iota_1 - \iota_2).$$

Notons que chaque $\mathrm{Ker}(\iota_1 - \iota_2)$ est un k-sev propre de K. Lorsque k est infini, il nous suffira donc d'invoquer le lemme suivant :

LEMME. – *Soit k un corps infini et V un k-ev de dimension finie. Alors le complémentaire d'une union finie de k-sev propres est non-vide.*

Démonstration. On raisonne par récurrence sur $d = \dim_k(V)$. Pour $d = 1$, l'assertion est claire (et vraie pour k fini d'ailleurs). Supposons $d > 1$ et donnons-nous des k-sev propres $V_1, \cdots, V_r$. On peut supposer que les V_i sont des hyperplans deux à deux distincts. Alors $V_1 \cap V_i$ est un k-sev propre de V_1 pour tout $i > 1$ donc, par hypothèse de récurrence, il existe $v_1 \in V_1 \setminus \bigcup_{i>1} V_i$. Choisissons $w_1 \in V \setminus V_1$ et considérons la droite affine $D = w_1 + kv_1$. On a $D \cap V_1 = \emptyset$. De plus, pour $i > 1$ on a $|D \cap V_i| < 1$. En effet, si $w_1 + \lambda v_1$ et $w_1 + \mu v_1$ sont dans V_i, alors $(\mu - \lambda)v_1 \in V_i$ donc $\mu = \lambda$. Il s'ensuit que $D \cap \bigcup_{i=1}^r V_i$ est fini, donc de complémentaire non vide puisque la droite D est infinie. $\square$

Reste à traiter le cas où k est fini. Pour cela on peut supposer $k = \mathbb{F}_p$. Alors $K = \mathbb{F}_{p^r}$ pour $r = [K : k]$ et $K^\times$ est le groupe des racines $p^r - 1$-ème de l'unité (ie les racines des $X^{p^r} - 1$). Le lemme suivant nous dit que ce groupe est cyclique. Mais alors tout générateur α de ce groupe est aussi un générateur de $\mathbb{F}_{p^r}$ sur $\mathbb{F}_p$. $\square$

LEMME. – *Soit k un corps et $G \subset k^\times$ un sous-groupe fini de $k^\times$. Alors G est cyclique.*

Démonstration. Notons $n = |G|$. On veut montrer qu'il existe un élément d'ordre n dans G. Soit m le ppcm des ordres de tous les éléments de G. Le résultat de structure des groupes abéliens finis (modules de torsion sur l'anneau principal $\mathbb{Z}$) implique qu'il existe un élément $x \in G$ d'ordre m (en fait, cela se prouve directement et facilement : exercice). Il suffit donc de montrer $m = n$. Or, par définition on a $x^m = 1$ pour tout $x \in G$, donc G est formé de racine m-èmes de l'unité, et donc $|G| = n \leqslant m$. Comme $m|n$, on a donc $m = n$. $\square$

Remarque. – Une extension finie non séparable n'est pas nécessairement monogène. Prenons par exemple $K = \mathbb{F}_p(X, Y) \supset k = \mathbb{F}_p(X^p, Y^p)$. On vérifie assez facilement que la famille des $X^i Y^j$, $0 \leqslant i, j < p$ est une base de K sur k, de sorte que $[K : k] = p^2$. Et pourtant pour tout $\alpha \in K$, on a $\alpha^p \in k$ donc $[k[\alpha] : k] = \deg(f_\alpha) \leqslant p$.

Exemple. – On a vu que le corps $\mathbb{Q}(\sqrt[3]{2})$ n'est pas normal sur $\mathbb{Q}$, mais qu'il le devient si on lui adjoint j (on obtient alors le corps de décomposition de $X^2 - 3$, de degré 6 sur $\mathbb{Q}$). Le théorème de l'élément primitif nous dit que ce corps est monogène, mais pas comment trouver un générateur. Nous verrons plus loin comment en trouver, et montrerons que par exemple $j + \sqrt[3]{2}$ est de degré 6, et engendre donc $\mathbb{Q}(j, \sqrt[3]{2})$.

2.6 Corps parfaits et imparfaits

2.6.1 DÉFINITION.– *Un corps k est dit* parfait *si tout polynôme irréductible $f \in k[X]$ est séparable ou, ce qui est équivalent, si toutes ses extensions algébriques sont séparables.*

Soit $f \in k[X]$ irréductible. Alors, puisque (f) est maximal, on voit que $(f, f') = k[X]$ si et seulement si f ne divise pas f'. Puisque $\deg(f') < \deg(f)$, ceci équivaut encore à $f' \neq 0$. On a donc :

Pour f irréductible, f séparable $\Leftrightarrow f' \neq 0$.

On en déduit alors facilement le théorème suivant.

2.6.2 THÉORÈME.– *k est parfait si et seulement si k est de caractéristique* 0 *ou son endomorphisme de Frobenius est surjectif (et donc bijectif).*

Démonstration. Supposons d'abord k imparfait. Alors il existe $f \in k[X]$ irréductible tel que $f' = 0$. Puisque f est non constant, k doit être de caractéristique p et f de la forme $\sum_n a_{np} X^{np}$. Si le Frobenius de k était surjectif, on pourrait trouver $b_{np} \in k$ tel que $b_{np}^p = a_{np}$, et on aurait alors $f = (\sum_n b_{np} X^n)^p$, contredisant l'irréductibilité de f.

Réciproquement, supposons k de caractéristique p, de Frobenius non surjectif. Choisissons $\alpha \in k \setminus k^p$ et considérons le polynôme $f := X^p - \alpha$. On a $f' = 0$. Montrons que f est irréductible. Soit $f = f_1 f_2$ une factorisation non triviale de f dans $k[X]$. Si β désigne une racine p-ème de α dans une clôture algébrique $\overline{k}$ de k, alors $f = (X - \beta)^p$ dans $\overline{k}[X]$, et donc $f_i = (X - \beta)^{r_i}$ avec $0 < r_i < p$. Noter que r_1 et r_2 sont premiers entre eux, donc il existe u, v tels que $ur_1 + vr_2 = 1$. Par conséquent, on a l'égalité $f_1^u f_2^v = X - \beta$ dans $\overline{k}(X)$. Comme $k(X) \cap \overline{k}[X] = k[X]$ (intersection dans $\overline{k}(X)$), on en déduit que $X - \beta \in k[X]$ et donc que $\beta \in k$, ce qui contredit l'hypothèse sur α. □

Exemples. – i) Tout corps fini est parfait, puisque une application injective d'un ensemble fini dans lui-même est aussi bijective.

ii) Tout corps algébriquement clos est parfait, puisque l'équation $X^p - x$ possède une solution pour tout $x \in k$.

iii) Le corps $\mathbb{F}_p(T)$ n'est pas parfait, car T n'a pas de racine p-ème, donc n'est pas dans l'image du Frobenius. Mais le corps $\mathbb{F}_p(T, T^{\frac{1}{p}}, T^{\frac{1}{p^2}}, \cdots,)$ est parfait .

2.6.3 *Corps imparfaits, extensions purement inséparables.*

DÉFINITION. – *Soit $K \supset k$ une extension algébrique. On dit que*
— *Un élément $\alpha \in K$ est purement inséparable sur k si son polynôme minimal est de la forme $X^{p^r} - x$ pour un $x \in k$.*
— *K est purement inséparable sur k si tout $\alpha \in K \setminus k$ est purement inséparable sur k.*

Exemple. – L'extension $K = \mathbb{F}_p(T) \supset \mathbb{F}_p(T^p) = k$ est purement inséparable. En effet, $\forall \alpha \in K$ on a $\alpha^p \in k$ donc f_α divise $X^p - \alpha^p = (X - \alpha)^p$ et lui est donc égal si $\alpha \notin k$.

Plus généralement, si k est un corps de caractéristique positive et $x \in k$ n'est pas dans l'image du Frobenius, alors $K := k[X]/(X^p - x)$ est une extension purement inséparable.

LEMME. – *Soit $f \in k[X]$ irréductible sur k de caractéristique $p > 0$. Il existe un unique $g \in k[X]$ irréductible et* séparable *et un unique $r \in \mathbb{N}$ tels que $f = g(X^{p^r})$.*

Démonstration. Existence. Si f est séparable, c'est clair. Si f est inséparable, on a $f' = 0$ donc il existe f_1 tel que $f = f_1(X^p)$. Le polynôme f_1 est clairement irréductible aussi, donc on peut recommencer le processus inductivement : soit f_1 est séparable, soit il existe f_2 tel que $f_1 = f_2(X^p)$, etc. Comme le degré est divisé par p à chaque étape, il existe r tel que f_r est séparable.

Unicité. Supposons $f = g(X^{p^r})$ comme dans l'énoncé et regardons cette égalité dans $\overline{k}[X]$ où $\overline{k}$ est une clôture algébrique de k. On constate que p^r est la multiplicité de chaque racine de f, donc r ne dépend que de f. De plus, on constate que les racines de g sont les puissances p^r-èmes des racines de f, ce qui détermine entièrement g dans $\overline{k}[X]$ puisque celui-ci est séparable. $\square$

La proposition suivante décrit la structure d'une extension algébrique sur un corps non parfait, vis à vis de la notion de séparabilité.

PROPOSITION. – *Soit $K \supset k$ une extension algébrique. Alors l'ensemble K_{sep} des éléments séparables de K sur k est un sous-corps de K appelé* clôture séparable de k dans K*, et l'extension $K \supset K_{\mathrm{sep}}$ est purement inséparable.*

Démonstration. Soient $\alpha, \beta \in K_{\mathrm{sep}}$. L'extension $k \subset k[\alpha]$ est séparable. Le polynôme minimal de β sur $k[\alpha]$ divise f_β donc est séparable, donc l'extension $k[\alpha] \subset k[\alpha, \beta]$ est aussi séparable. D'après le corollaire 2.5.4, $k[\alpha, \beta]$ est séparable sur k et en particulier $\alpha - \beta$ et $\alpha\beta^{-1}$ sont séparables sur k. Il s'ensuit que K_{sep} est un corps.

Soit maintenant $\alpha \in K \setminus K_{sep}$ et g_α son polynôme minimal sur K_{sep}. Soit r tel que $g_\alpha = h_\alpha(X^{p^r})$ avec h_α séparable. Alors toute racine de h_α est séparable sur K_{sep}, donc aussi sur k (toujours par le corollaire 2.5.4), donc appartient à K_{sep}. Comme h_α est irréductible, on a $h_\alpha = X - \beta$ pour un $\beta \in K_{\mathrm{sep}}$. Il s'ensuit que $g_\alpha = X^{p^r} - \beta$. $\square$

DÉFINITION. – *i) Un corps k est dit séparablement clos si tout polynôme irréductible séparable de $k[X]$ est scindé.*

ii) On appelle clôture séparable (absolue) d'un corps k toute extension algébrique séparable et séparablement close de k.

PROPOSITION. – *Tout corps k admet une clôture séparable et celle-ci est unique à isomorphisme près. De plus, toute extension séparable s'y plonge.*

Démonstration. Soit $\overline{k}$ une clôture algébrique de k. Alors $\overline{k}_{\mathrm{sep}}$ est une clôture séparable de k (vérifier les détails). $\square$

2.7 Extensions Galoisiennes. Correspondance de Galois

2.7.1 Définition.– *Une extension finie $K \supset k$ est dite Galoisienne si elle est normale et séparable. On note alors* $\mathrm{Gal}(K/k) := \mathrm{Aut}(K/k)$ *le groupe des automorphismes de la k-algèbre K et on l'appelle* groupe de Galois *de K sur k.*

Le théorème suivant résume les caractérisations utiles des extensions Galoisiennes.

2.7.2 Théorème.– *Soit $K \supset k$ une extension finie. On a équivalence entre :*

i) K est Galoisienne sur k

ii) Pour tout $\alpha \in K$, on a $f_\alpha = \prod_{\beta \in \mathrm{Aut}(K/k)\cdot\alpha}(X-\beta)$ dans $K[X]$.

iii) K est le corps de décomposition d'un polynôme séparable.

iv) $|\mathrm{Aut}_{k-\mathrm{alg}}(K)| = [K:k]$

v) $K^{\mathrm{Aut}(K/k)} = k$ (points fixes dans K pour l'action de $\mathrm{Aut}(K/k)$*).*

Démonstration. $i) \Leftrightarrow ii)$. Par définition, K est Galoisienne sur k si et seulement si $\forall \alpha \in K$, f_α est séparable et scindé dans $K[X]$. Par ailleurs on a déjà vu que les racines de f_α dans une clôture algébrique $\overline{k}$ sont permutées transitivement par $\mathrm{Aut}(\overline{k}/k)$. Plongeons donc K dans $\overline{k}$. Comme $\mathrm{Aut}(\overline{k}/k)$ stabilise K, on en déduit que $\mathrm{Aut}(K/k)$ permute transitivement les racines de f_α dans K, de sorte que $\mathrm{Aut}(K/k)\alpha = \{\text{racines de } f_\alpha \text{ dans } K\}$.

$i) \Leftrightarrow iii)$. On a déjà vu qu'un corps de décomposition d'un polynôme séparable f est une extension normale (corollaire 2.3.5) et séparable (à la suite du corollaire 2.5.4). Réciproquement, si K est Galoisienne, elle est monogène puisque séparable, et contient toutes les racines du polynôme minimal f_α d'un générateur α. C'est donc un corps de décomposition de f_α.

$i) \Rightarrow iv)$. Soit $\overline{k}$ une clôture algébrique de k. Puisque K est séparable sur k on a $|\mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k})| = [K:k]$. Fixons un plongement $\iota_1 \in \mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k})$ et considérons l'application $\mathrm{Aut}_{k-\mathrm{alg}}(K) \longrightarrow \mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k})$, $\sigma \mapsto \iota_1 \circ \sigma$. Cette application est injective puisque ι_1 est injective. Elle est aussi surjective puisque tout autre plongement $\iota_2 : K \hookrightarrow \overline{k}$ a la même image K' dans $\overline{k}$ que ι_1, si bien que la composée $\sigma :\ \iota_1^{-1} \circ \iota_2$ est un automorphisme de K tel que $\iota_2 = \iota_1 \circ \sigma$. On a donc $|\mathrm{Aut}(K/k)| = [K:k]$.

$iv) \Rightarrow v)$. Notons $k' := K^{\mathrm{Aut}(K/k)}$, qui est évidemment un sous-corps de K contenant k. On a donc $\mathrm{Aut}(K/k') = \mathrm{Aut}(K/k)$. Choisissons un plongement $\iota : K \hookrightarrow \overline{k'}$ de K dans une clôture algébrique de k'. Alors l'application $\sigma \mapsto \iota \circ \sigma$ est une injection de $\mathrm{Aut}(K/k')$ dans $\mathrm{Hom}_{k'-\mathrm{alg}}(K,\overline{k'})$. D'après la proposition 2.5.4 on a donc $|\mathrm{Aut}(K/k')| \leqslant [K:k']$. Or, on a aussi $[K:k'] \leqslant [K:k] = |\mathrm{Aut}(K/k)| = |\mathrm{Aut}(K/k')|$. Donc $[K:k'] = [K:k]$, puis $[k':k] = 1$ et finalement $k' = k$.

$v) \Rightarrow ii)$. Soit $\alpha \in K$, et posons $g_\alpha := \prod_{\beta \in \mathrm{Aut}(K/k)\cdot\alpha}(X-\beta) \in K[X]$. On sait que g_α divise f_α puisque chaque $\beta \in \mathrm{Aut}(K/k)\alpha$ est une racine de f_α. Puisque f_α est irréductible dans $k[X]$, il nous suffira donc de montrer que $g_\alpha \in k[X]$. Pour cela, étendons l'action de $G := \mathrm{Aut}(K/k)$ à $K[X]$ comme d'habitude : G agit sur les coefficients des polynômes. Sous l'hypothèse $v)$, on voit qu'un polynôme $f \in K[X]$ est dans $k[X]$ si et seulement si il est fixe par G. Or pour tout $\sigma \in G$, on a

$$\sigma(g_\alpha) = \prod_{\beta \in G\alpha} (X - \sigma(\beta)) = \prod_{\gamma \in \sigma G\alpha} (X - \gamma) = \prod_{\gamma \in G\alpha} (X - \gamma) = g_\alpha.$$

Donc g_α est fixe par G et appartient à $k[X]$. □

2.7.3 *Exemple* (*Corps finis)*– L'extension $\mathbb{F}_{p^r} \supset \mathbb{F}_p$ est Galoisienne puisque c'est un corps de décomposition du polynôme séparable $X^{p^r} - X$. Soit F l'endomorphisme de Frobenius de $\mathbb{F}_{p^r}$, qui est un automorphisme, donc un élément de $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$. On a bien-sûr $F^r = \mathrm{id}$. De plus, pour $s < r$, on a vu que le sous-corps des points fixes $\mathbb{F}_{p^r}^{F^s}$ est l'ensemble des racines de $X^{p^s} - X$, donc de cardinal $< p^r$. Il s'ensuit que F est d'ordre r et donc que $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$ est cyclique d'ordre r, engendré par F.

2.7.4 *Exemple* (*Extensions cyclotomiques)*– L'extension n-cyclotomique d'un corps k est "le" corps de décomposition k_n du polynôme $X^n - 1$, c'est-à-dire "l'"extension engendrée par les racines n-èmes de l'unité. Si k est de caractéristique $p > 0$ et si $n = p^k n'$ avec $(n', p) = 1$, on a $X^n - 1 = (X^{n'} - 1)^{p^k}$ donc $k_n = k_{n'}$. On supposera donc que $(n, p) = 1$ sans perte de généralité. L'extension $k_n \supset k$ est Galoisienne puisque $X^n - 1$ est séparable. Cherchons à calculer $\mathrm{Gal}(k_n/k)$. Il est clair que tout $\sigma \in \mathrm{Gal}(k_n/k)$ stabilise le sous-groupe $\mu_n(k_n)$ des racines n-èmes de l'unité dans k_n, et est entièrement déterminé par son action sur $\mu_n(k_n)$ (puisque celui-ci engendre k_n sur k). De plus, σ agit par automorphismes de groupes sur $\mu_n(k_n)$, donc on obtient ainsi une injection

$$\mathrm{Gal}(k_n/k) \hookrightarrow \mathrm{Aut}_{\mathrm{grp}}(\mu_n(k_n)).$$

Maintenant, on a vu au cours de la preuve du théorème 2.5.5 que le groupe $\mu_n(k_n)$ est cyclique d'ordre n. On sait calculer le groupe des automorphismes d'un groupe cyclique d'ordre n : si ζ_n est un générateur de $\mu_n(k_n)$ (*i.e.* une racine n-ème "primitive" de l'unité), alors $\sigma(\zeta_n)$ en est un autre générateur, donc de la forme $\zeta_n^{a_\sigma}$ pour un $a_\sigma \in \mathbb{Z}$, uniquement déterminé modulo n, et tel que $(a_\sigma, n) = 1$. On obtient ainsi une injection

$$\chi_k : \mathrm{Gal}(k_n/k) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto (a_\sigma \pmod n).$$

On ne peut pas dire grand chose de plus sans information supplémentaire sur k. Voici quelques exemples :

— $k = \mathbb{F}_p$. Dans ce cas, on sait que k_n doit être de la forme $\mathbb{F}_{p^r} = k_{p^r-1}$. Donc r est le plus petit entier tel que $n | p^r - 1$, c'est-à-dire l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$. On a vu que $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$ est cyclique d'ordre r, engendré par le Frobenius F. Il en est donc de même de $\mathrm{Gal}(k_n/k)$ et, par définition du Frobenius et de χ, on a $\chi_{\mathbb{F}_p}(F) = (p \pmod n)$.

— $k = \mathbb{Q}$. On a donc $\mathbb{Q}_n = \mathbb{Q}(e^{2i\pi/n})$. Si c désigne la conjugaison complexe, un automorphisme de $\mathbb{C}$ qui préserve nécessairement le sous-corps algébriquement clos $\overline{\mathbb{Q}}$ et la sous-extension normale $\mathbb{Q}_n$, alors on voit que $\chi_{\mathbb{Q}}(c) = (-1 \pmod n)$ puisque c envoie $e^{2i\pi/n}$ sur $e^{-2i\pi/n}$. En fait nous allons démontrer :

THÉORÈME. – *$\chi_{\mathbb{Q}}$ est un isomorphisme* $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$.

D'après la discussion précédente, ceci équivaut à l'égalité

$$[\mathbb{Q}(e^{2i\pi/n}) : \mathbb{Q}] = \varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$$

(indicatrice d'Euler). Pour la prouver, notons

$$\Phi_n(X) := \prod_{0 \leqslant i < n,\, (a,n)=1} (X - e^{2\pi i.a/n}) = \prod_{\zeta \text{ d'ordre } n} (X - \zeta) \in \overline{\mathbb{Q}}[X],$$

où le second produit est indexé par les racines n-èmes primitives de 1. On a donc la factorisation

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \text{ dans } \overline{\mathbb{Q}}[X].$$

En fait, $\Phi_n(X) \in \mathbb{Q}_n[X]$ est invariant par $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ puisque tout conjugué d'une racine primitive n-ème est une racine primitive n-ème. On a donc, d'après le v) du théorème, $\Phi_n(X) \in \mathbb{Q}[X]$ (on peut aussi le voir par récurrence grâce au produit ci-dessus). Du coup, $\mathbb{Q}_n$ est aussi un corps de décomposition de Φ_n et, puisque $\deg(\Phi_n) = \varphi(n)$, il nous suffira de montrer que

LEMME. – Φ_n est irréductible dans $\mathbb{Q}[X]$.

Démonstration. Soit $\Phi_n = fg$ dans $\mathbb{Q}[X]$ avec f, g unitaires et $\deg(f) > 0$. Cette factorisation correspond à une partition de l'ensemble des racines primitives n-èmes de l'unité. On veut montrer que $f = \Phi_n$ et pour cela il suffit de montrer que l'ensemble des racines de f est stable par l'action de $(\mathbb{Z}/n\mathbb{Z})^\times$, c'est-à-dire par élévation à la puissance a pour tout a premier à n. Il suffit bien-sur de montrer la stabilité par élévation à la puissance p, pour tout premier p premier à n.
Avant cela, montrons que $\Phi_n \in \mathbb{Z}[X]$. On peut le voir par récurrence à partir de la formule du produit. On peut aussi remarquer que, ses coefficients appartiennent au sous anneau $\mathbb{Z}[e^{2\pi i/n}] \cap \mathbb{Q}$ de $\mathbb{Q}$. Or $\mathbb{Z}[e^{2i\pi/n}]$ est engendré, en tant que $\mathbb{Z}$-module par les $e^{2\pi i m/n}$, $0 \leqslant m < n$ (cf second corollaire de 1.4.3). Donc le sous-anneau $\mathbb{Z}[e^{2\pi i/n}] \cap \mathbb{Q}$ est de type fini en temps que $\mathbb{Z}$-module, et donc égal à $\mathbb{Z}$.
Montrons maintenant que $f, g \in \mathbb{Z}[X]$. Avec les notations de la preuve du théorème 1.6.3, il suffit de prouver que $\nu_p(f), \nu_p(g) \geqslant 0$ pour tout nombre premier p. Or on a $\nu_p(f), \nu_p(g) \leqslant 0$ puisque f, g sont unitaires, et aussi $\nu_p(f) + \nu_p(g) = 0$. Donc $\nu_p(f) = \nu_p(g) = 0$.
Fixons maintenant p premier et premier à n, et notons $\overline{\Phi}_n$, $\overline{f}$ et $\overline{g}$ les images de Φ_n, f et g dans $\mathbb{F}_p[X]$. L'ensemble des racines de $\overline{\Phi}_n$ dans $\overline{\mathbb{F}}_p$ est l'ensemble des racines primitives n-èmes de l'unité, et la factorisation $\overline{\Phi}_n = \overline{f}\overline{g}$ correspond encore à une partition de cet ensemble. En particulier, $\overline{f}$ et $\overline{g}^p$ sont premiers entre eux, et on peut donc trouver $\overline{u}$, $\overline{v} \in \mathbb{F}_p[X]$ tels que $\overline{u}\overline{f} + \overline{v}\overline{g}^p = 1$. En choissant des relèvements $u, v \in \mathbb{Z}[X]$ et en observant que $\overline{g(X^p)} = \overline{g}^p$, on voit qu'il existe $w \in \mathbb{Z}[X]$ tel que

$$uf(X) + vg(X^p) = 1 + pw.$$

Soit alors ζ une racine de f. On a $1+pw(\zeta)\neq 0$. En effet, sinon on aurait $w(\zeta)=-1/p\in\mathbb{Z}[\zeta]\cap\mathbb{Q}=\mathbb{Z}$, ce qui est absurde. Donc ζ^p ne peut pas être une racine de g, et doit être une racine de f, comme voulu. $\square$

2.7.5 *Exemple* (*Extensions radicales*)– Soit $a\in k^\times$ et $n\in\mathbb{N}$. Notons μ_n le groupe des racines n-èmes de l'unité et *supposons que* $|\mu_n|=n$ (ie k contient toutes les racines n-èmes de l'unité). Considérons une extension K de k engendrée par un élément α tel que $\alpha^n=a$ (ie $f_\alpha|X^n-a$). Alors K est le corps de décomposition du polynôme X^n-a sur k. En effet, toute autre racine de X^n-a est de la forme $\alpha\zeta$ avec $\zeta\in\mu_n$, donc appartient à K. Cette observation donne aussi des informations sur $\mathrm{Gal}(K/k)$. En effet, tout $\sigma\in\mathrm{Gal}(K/k)$ est déterminé par son action sur α, qui est de la forme $\alpha\zeta_\sigma$ pour un $\zeta_\sigma\in\mu_n$. Pour un autre σ', on a alors $(\sigma'\sigma)(\alpha)=\sigma'(\alpha\zeta_\sigma)=\sigma'(\alpha)\zeta_\sigma=\alpha\zeta_{\sigma'}\zeta_\sigma$, d'où l'on tire que l'application

$$\mathrm{Gal}(K/k)\longrightarrow\mu_n,\ \sigma\mapsto\zeta_\sigma$$

est un morphisme de groupes (injectif). Comme tout sous-groupe de μ_n est un μ_m pour $m|n$, on obtient ainsi un isomorphisme

$$\mathrm{Gal}(K/k)\xrightarrow{\sim}\mu_m$$

pour $m:=[K:k]$ qui montre en particulier que $\mathrm{Gal}(K/k)$ est cyclique. Cherchons à deviner m à partir de a. L'élément $N\alpha=\prod_\sigma\sigma(\alpha)$ est un élément de $K^{\mathrm{Gal}(K/k)}=k$. On a $N\alpha=\alpha^m\prod_\sigma\zeta_\sigma$, donc on voit que $\alpha^m\in k$. Comme le polynôme minimal f_α de α sur f est de degré $[K:k]=m$, on a $f_\alpha=X^m-\alpha^m$ et en particulier m est le plus petit entier $r\geqslant 1$ tel que $\alpha^r\in k^\times$. Il s'ensuit que m est le plus petit entier $r\geqslant 1$ tel que $a^r\in(k^\times)^n$, c'est-à-dire l'ordre de a dans le quotient $k^\times/(k^\times)^n$. En particulier, on voit que le polynôme X^n-a est irréductible dans $k[X]$ si et seulement si a est d'ordre n dans $k^\times/(k^\times)^n$. En résumé on a prouvé la première partie de :

Théorème. – *Soit k un corps tel que $|\mu_n(k)|=n$. Pour tout $a\in k$, l'extension $k[\sqrt[n]{a}]$ engendrée par une racine n-ème de a est Galoisienne de degré m égal à l'ordre de a dans $k^\times/(k^\times)^n$, et on a un isomorphisme*

$$\mathrm{Gal}(k[\sqrt[n]{a}]/k)\xrightarrow{\sim}\mu_m,\ \sigma\mapsto\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}.$$

Réciproquement, toute extension $K\supset k$ de groupe de Galois cyclique d'ordre n est de la forme $k[\sqrt[n]{a}]$ pour un $a\in k$.

Il nous reste à justifier la réciproque. Soit donc σ un générateur de $\mathrm{Gal}(K/k)$, de sorte que $\mathrm{Gal}(K/k)=\{1,\sigma,\sigma^2,\cdots,\sigma^{n-1}\}$, et soit $\zeta\in K$ une racine primitive n-ème de l'unité. Le lemme ... ci-dessous assure que les σ^i sont linéairement indépendants dans le k-ev $\mathrm{Hom}_{k-\mathrm{ev}}(K,K)$, de sorte que l'endomorphisme $\mathrm{id}+\zeta^{-1}\sigma+\cdots\zeta^{1-m}\sigma^{m-1}$ est non nul. Il existe donc $x\in K$ tel que $\alpha:=x+\zeta^{-1}\sigma(x)+\cdots+\zeta^{1-n}\sigma^{n-1}(x)$ est *non nul.* Alors

$\sigma(\alpha) = \zeta\alpha$, donc les $\sigma^i(\alpha) = \zeta^i\alpha$ pour $0 \leqslant i < n$ sont 2 à 2 distincts et

$$f_\alpha = \prod_{i=0}^{n-1}(X - \sigma^i(\alpha)) = \prod_{i=0}^{n-1}(X - \zeta^i\alpha) = X^n - \alpha^n.$$

En particulier, on a $\alpha^n \in k^\times$ et, puisque f_α est de degré n, on a $K = k[\alpha]$ comme voulu.
Le corollaire immédiat suivant nous sera utile :

Corollaire. – *Soit k un corps tel que $|\mu_n(k)| = n$ et soit $K \supset k$ une extension engendrée par des éléments $\alpha_1, \cdots, \alpha_r$ tels que $\alpha_i^n \in k$. Alors $K \supset k$ est Galoisienne de groupe de Galois abélien.*

Démonstration. L'extension est normale puisqu'elle contient tous les conjugués des générateurs α_i (qui sont de la forme $\alpha_i\zeta_n^j$). C'est donc un corps de décomposition du polynôme $(X^n - \alpha_1)\cdots(X^n - \alpha_r)$. Elle est séparable, puisqu'engendrée par des éléments séparables. Elle est donc galoisienne. Considérons l'application

$$\mathrm{Gal}(K/k) \longrightarrow \prod_{i=1}^{r} \mathrm{Gal}(k(\alpha_i)/k),\ \sigma \mapsto (\sigma_{|k(\alpha_1)}, \cdots, \sigma_{|k(\alpha_r)}).$$

Elle est bien définie puisque chaque extension $k(\alpha_i) \supset k$ est galoisienne, elle injective puisque les α_i engendrent K, et c'est un morphisme de groupes. Donc $\mathrm{Gal}(K/k)$ est un sous-groupe d'un produit de groupes cycliques et est donc abélien. □

Il nous reste à prouver le lemme général suivant.

2.7.6 Lemme.– *Soit $K \supset k$ une extension Galoisienne. Son groupe de Galois G est un sous-ensemble linéairement indépendant de* $\mathrm{Hom}_{k-ev}(K, K)$

Démonstration. Choisissons une énumération $(\sigma_i)_{i=1,\cdots,n}$ des éléments de G. Pour $\alpha \in K$ on peut former la matrice $M_\alpha = (\sigma_i(\alpha^j))_{i,j} \in \mathcal{M}_{n\times n}(K)$. Puisque $\sigma_i(\alpha^j) = \sigma_i(\alpha)^j$, c'est une matrice de Vandermonde et son déterminant est donc $\pm\prod_{i<j}(\sigma_i(\alpha) - \sigma_j(\alpha))$. Prenons pour α un élément primitif de K. Alors les $\sigma_i(\alpha)$ sont deux-à-deux distincts et on a donc $\det(M_\alpha) \neq 0$. Donnons-nous maintenant une relation de dépendence linéaire $\sum_{i=1}^n \lambda_i\sigma_i = 0$ dans $\mathrm{Hom}_k(K, K)$. Elle induit une dépendence linéaire $\sum_i \lambda_i L_i(M_\alpha)$ entre les lignes de M_α. Mais puisque $\det(M_\alpha) \neq 0$ on a donc $\lambda_i = 0$ pour tout i. □

Remarque. – Une autre approche, beaucoup moins élémentaire, consiste à se ramener à prouver que l'ensemble $\mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k}) = \mathrm{Hom}_{\overline{k}-\mathrm{alg}}(\overline{k}\otimes_k K, \overline{k})$ est linéairement indépendant dans le $\overline{k}$-ev $\mathrm{Hom}_{k-\mathrm{ev}}(K, \overline{k}) = \mathrm{Hom}_{\overline{k}-\mathrm{ev}}(\overline{k} \otimes_k K, \overline{k})$. Or, plus généralement, la surjectivité dans le lemme 2.5.4 nous dit que pour toute algèbre de dimension finie A sur $\overline{k}$, l'ensemble $\mathrm{Hom}_{\overline{k}-\mathrm{alg}}(A, \overline{k})$ est linéairement indépendant dans $\mathrm{Hom}_{\overline{k}-\mathrm{ev}}(A, \overline{k})$.

2.7.7 *Problèmes inverses.* Dans les exemples ci-dessus, tous les groupes de Galois étaient abéliens. L'énoncé suivant est un corollaire immédiat et utile de la caractérisation $v)$ du théorème 2.7.2, qui permet de voir que tout groupe fini est un groupe de Galois.

PROPOSITION. – *Soit G un groupe fini d'automorphismes d'un corps K. Alors K^G est un corps et l'extension $K \supset K^G$ est Galoisienne de groupe* $\mathrm{Gal}(K/K^G) = G$.

Démonstration. Si $\alpha \in K$ on remarque que le polynôme $g_\alpha := \prod_{\beta \in G\cdot\alpha}(X - \beta) \in K[X]$ est invariant sous G donc dans $K^G[X]$. Comme $g_\alpha(\alpha) = 0$, le polyôme minimal f_α de α sur K^G divise g_α, donc est séparable. Il s'ensuit que α est séparable et de degré $\leqslant |G|$. Le théorème de l'élément primitif nous assure alors que K est finie sur K^G et $[K : K^G] \leqslant |G|$. Puisque K est finie sur K^G on a aussi l'inégalité $|\mathrm{Aut}_{K^G-\mathrm{alg}}(K)| \leqslant [K : K^G]$. Or, on a par définition $G \subset \mathrm{Aut}_{K^G-\mathrm{alg}}(K)$, et on en déduit donc les égalités $[K : K^G] = |\mathrm{Aut}_{K^G-\mathrm{alg}}(K)| = |G|$. La première égalité montre que K/K^G est Galoisienne grâce au iv) du théorème 2.7.2. La deuxiéme égalité et l'inclusion $G \subset \mathrm{Aut}_{K^G-\mathrm{alg}}(K)$ montrent que $G = \mathrm{Gal}(K/K^G)$. □

Exemple. – Le groupe de permutations $\mathfrak{S}_n$ agit sur $K_n := k(X_1, \cdots, X_n)$ par permutation des indéterminées. Tout groupe fini G se plonge dans un $\mathfrak{S}_n$ (par exemple $n = |G|$ en faisant agir G sur lui-même par translations à gauche). Alors l'extension $K_n \supset K_n^G$ est Galoisienne de groupe G. On voit ainsi que tout groupe fini est un groupe de Galois. Le *problème de Galois inverse*, encore ouvert, demande quels groupes finis G peuvent être groupes de Galois d'une extension Galoisienne $K \supset \mathbb{Q}$ (on pense qu'ils le sont tous).

2.7.8 *Correspondance de Galois.* Nous allons établir une bijection remarquable entre sous-extensions d'une extension galoisienne et sous-groupes de son groupe de Galois. Commençons par le résultat suivant.

PROPOSITION. – *Soit $K \supset k$ une extension Galoisienne et $k \subset K' \subset K$ une sous-extension. Alors :*

i) K est Galoisienne sur K' et $K' = K^{\mathrm{Gal}(K/K')}$.

ii) Pour tout $\sigma \in \mathrm{Gal}(K/k)$, on a $\mathrm{Gal}(K/\sigma(K')) = \sigma\mathrm{Gal}(K/K')\sigma^{-1}$.

iii) K' est Galoisienne sur k si et seulement si $\mathrm{Gal}(K/K')$ est distingué dans $\mathrm{Gal}(K/k)$. Dans ce cas, l'application $\sigma \mapsto \sigma_{|K'}$ induit un isomorphisme

$$\mathrm{Gal}(K/k)/\mathrm{Gal}(K/K') \xrightarrow{\sim} \mathrm{Gal}(K'/k).$$

Démonstration. i) Si K est un corps de décomposition d'un polynôme séparable $f \in k[X]$ sur k, alors c'est aussi un corps de décomposition du même f sur K', lequel est toujours séparable. Donc K est Galoisienne sur K' et l'égalité $K' = K^{\mathrm{Gal}(K/K')}$ découle du $v)$ du théorème.

ii) Soit $\tau \in \mathrm{Gal}(K/k)$. On a $\tau \in \mathrm{Gal}(K/\sigma(K')) \Leftrightarrow (\forall \alpha \in K', \tau(\sigma(\alpha')) = \sigma(\alpha')) \Leftrightarrow (\forall \alpha \in K', \sigma^{-1}\tau\sigma(\alpha) = \alpha) \Leftrightarrow \sigma^{-1}\tau\sigma \in \mathrm{Gal}(K/K')$.

iii) Si $\mathrm{Gal}(K/K')$ est distingué dans $\mathrm{Gal}(K/k)$ alors d'après ii) on a

$$\forall \sigma \in \mathrm{Gal}(K/k),\ \sigma(K') = K^{\mathrm{Gal}(K/\sigma(K'))} = K^{\sigma\mathrm{Gal}(K/K')\sigma^{-1}} = K^{\mathrm{Gal}(K/K')} = K',$$

donc K' est normale sur k. Comme elle est aussi séparable, elle est bien Galoisienne. Réciproquement, supposons K' Galoisienne sur k. Alors tout automorphisme de K/k laisse K' stable et induit donc un automorphisme de K'/k. On obtient par restriction des automorphismes, un morphisme de groupes $\sigma \mapsto \sigma_{|K'}$

$$\mathrm{Gal}(K/k) \longrightarrow \mathrm{Gal}(K'/k)$$

dont le noyau est le sous-groupe des automorphismes de K/k qui sont l'identité sur K', c'est-à-dire $\mathrm{Gal}(K/K')$, qui est donc distingué. Pour voir que ce morphisme est surjectif, on peut plonger K dans une clôture algébrique $\overline{k}$ et rappeler que la restriction $\mathrm{Gal}(\overline{k}/k) \longrightarrow \mathrm{Gal}(K'/k)$ est surjective. On peut aussi remarquer que le cardinal de l'image est $[K:k][K:K']^{-1} = [K':k]$. □

Fixons maintenant une extension finie Galoisienne $K \supset k$. Notons $\mathcal{SE}(K)$ l'ensemble des sous-extensions $K' \supset k$ contenues dans K, ordonné par inclusion. Notons aussi $G := \mathrm{Gal}(K/k)$ et $\mathcal{SG}(G)$ l'ensemble des sous-groupes de G, lui aussi ordonné par inclusion. On a deux applications, manifestement décroissantes :

$$\begin{array}{rcl} \mathcal{SE}(K) & \to & \mathcal{SG}(G) \\ K' & \mapsto & \mathrm{Gal}(K/K') \end{array} \quad \text{et} \quad \begin{array}{rcl} \mathcal{SG}(G) & \to & \mathcal{SE}(K) \\ G' & \mapsto & K^{G'} \end{array}$$

THÉORÈME. – *Ces deux applications sont des bijections réciproques, qui échangent sous-extensions Galoisiennes et sous-groupes distingués.*

Démonstration. Découle de la proposition et du corollaire précédent. □

Exemple. – Le corps de décomposition K de X^3-2 sur $\mathbb{Q}$ est une extension Galoisienne de $\mathbb{Q}$. On a vu que $K = \mathbb{Q}(j, \sqrt[3]{2})$ est de degré 6 sur $\mathbb{Q}$, puisque de degré 2 sur $\mathbb{Q}(\sqrt[3]{2})$ qui est de degré 3 sur $\mathbb{Q}$. Donc $\mathrm{Gal}(K/\mathbb{Q})$ est un groupe d'ordre 6. Puisque $\mathrm{Gal}(K/\mathbb{Q})$ se plonge dans le groupe des permutations $\mathfrak{S}_3$ de l'ensemble $\{\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\}$ qui est aussi d'ordre 6, on voit que $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathfrak{S}_3$. Donnons une autre description susceptible de se généraliser. $\mathrm{Gal}(K/\mathbb{Q})$ contient le sous-groupe $\mathrm{Gal}(K/\mathbb{Q}(j))$ d'ordre 3, donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$, et le sous-groupe $\mathrm{Gal}(K/\mathbb{Q}(\sqrt[3]{2}))$, d'ordre 2 donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Le premier est distingué puisque $\mathbb{Q}(j)$ est Galoisien sur $\mathbb{Q}$, mais pas le second. Il s'ensuit que $\mathrm{Gal}(K/\mathbb{Q})$ est un produit semi-direct

$$\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q}(\sqrt[3]{2})) \ltimes \mathrm{Gal}(K/\mathbb{Q}(j)) \simeq \mathbb{Z}/2\mathbb{Z} \ltimes \mathbb{Z}/3\mathbb{Z}.$$

On peut en déduire la structure des extensions intermédiaires : il y a exactement trois sous-extensions de degré 3, à savoir $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$, correspondant aux trois sous-groupes d'ordre 2, et une sous-extension de degré 2, Galoisienne, à savoir $\mathbb{Q}(j)$.

On peut aussi maintenant montrer que $\alpha = j + \sqrt[3]{2}$ est un générateur de K sur $\mathbb{Q}$. En effet, soit σ le générateur de $\mathrm{Gal}(K/\mathbb{Q}(\sqrt[3]{2}))$ et soit τ le générateur de $\mathrm{Gal}(K/\mathbb{Q}(j))$ qui envoie $\sqrt[3]{2}$ sur $j\sqrt[3]{2}$. Alors on calcule que l'ensemble des conjugués de $j + \sqrt[3]{2}$

$$\{\alpha, \sigma(\alpha), \tau(\alpha), \tau^2(\alpha), \sigma\tau(\alpha), \sigma\tau^2(\alpha)\} = \{j+\sqrt[3]{2}, j^2+\sqrt[3]{2}, j+j\sqrt[3]{2}, j+j^2\sqrt[3]{2}, j^2+j^2\sqrt[3]{2}, j^2+j\sqrt[3]{2}\}$$

est de cardinal 6, donc $\deg(f_\alpha) = 6$ et α engendre K sur $\mathbb{Q}$.

Voici une généralisation de cet exemple :

2.7.9 *Exemple* (*Extensions de Kummer sur* $\mathbb{Q}$)– Soit $a \in \mathbb{Q}$. On s'intéresse au groupe de Galois du corps de décomposition K de $X^n - a$ sur $\mathbb{Q}$. Puisque le ratio de deux racines n-èmes de a est une racine de l'unité, on constate facilement que $K = \mathbb{Q}[\sqrt[n]{a}, \zeta_n]$ où $\zeta_n := e^{2\pi i/n}$ et $\sqrt[n]{a}$ désigne une racine n-ème de a dans $\overline{\mathbb{Q}} \subset \mathbb{C}$. Le groupe de Galois $G := \mathrm{Gal}(\mathbb{Q}[\zeta_n, \sqrt[n]{a}]/\mathbb{Q})$ contient donc deux sous-groupes remarquables,

$$H_1 := \mathrm{Gal}(\mathbb{Q}[\zeta_n, \sqrt[n]{a}]/\mathbb{Q}[\zeta_n]) \text{ et } H_a := \mathrm{Gal}(\mathbb{Q}[\zeta_n, \sqrt[n]{a}]/\mathbb{Q}[\sqrt[n]{a}]),$$

dont l'intersection $H_1 \cap H_a$ est égale à $\{\mathrm{id}\}$ puisque ses éléments fixent ζ_n et $\sqrt[n]{a}$.

Puisque $\mathbb{Q}[\zeta_n]$ est Galoisienne sur $\mathbb{Q}$ de groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, le sous-groupe H_1 est distingué de quotient $G/H_1 \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, en particulier on a $|G| = |H_1|\varphi(n)$. On a aussi, d'après l'exemple 2.7.5, un plongement $H_1 \hookrightarrow \mu_n$ et on sait que $n_1 := |H_1|$ est l'ordre de a dans le quotient $\mathbb{Q}(\zeta_n)^\times/(\mathbb{Q}(\zeta_n)^\times)^n$.

Par ailleurs, on a l'égalité $|G| = |H_a|[\mathbb{Q}[\sqrt[n]{a}] : \mathbb{Q}]$, et le caractère cyclotomique nous fournit un plongement $\chi_{n,\mathbb{Q}[\sqrt[n]{a}]} : H_a \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$.

Supposons que le polynôme cyclotomique Φ_n *reste irréductible dans* $\mathbb{Q}[\sqrt[n]{a}][X]$. Ceci équivaut à l'égalité $[\mathbb{Q}[\sqrt[n]{a}, \zeta_n] : \mathbb{Q}[\sqrt[n]{a}]] = \varphi(n)$, et donc à l'égalité $[\mathbb{Q}[\sqrt[n]{a}] : \mathbb{Q}] = n_1$ et aussi à l'égalité $|G| = |H_1||H_a|$. Ainsi, dans ce cas, G est produit semi-direct de H_1 par H_a. Utilisant les descriptions de H_1 et H_a on obtient l'isomorphisme

$$\mathrm{Gal}(\mathbb{Q}[\zeta_n, \sqrt[n]{a}]/\mathbb{Q}) \xrightarrow{\sim} \mu_{n_1} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times : \ \sigma \mapsto \left(\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}, \sigma_{|\mu_n}\right),$$

où le produit semi-direct est pris pour l'action de conjugaison de H_a sur H_1. Explicitons cette action ; pour $\sigma \in H_1$ et $\tau \in H_a$, on a $(\tau\sigma\tau^{-1})(\sqrt[n]{a}) = (\tau\sigma)(\sqrt[n]{a}) = \tau(\sqrt[n]{a}\zeta_\sigma) = \sqrt[n]{a}.\tau(\zeta_\sigma) = \sqrt[n]{a}.\zeta_\sigma^{a_\tau}$, donc c'est l'action naturelle $(a, \zeta) \mapsto \zeta^a$ de $(\mathbb{Z}/n\mathbb{Z})^\times$ sur μ_{n_1}.

Notons que l'on peut très bien avoir $n_1 = 1$ (par exemple lorsque a est une puissance n-ème dans $\mathbb{Q}$). A l'autre extrême, on a $n_1 = n$ si et seulement si $X^n - a$ est irréductible dans $\mathbb{Q}[\zeta_n][X]$ et, dans ce cas, notre hypothèse sur Φ_n est automatique puisqu'on a alors $[\mathbb{Q}[\sqrt[n]{a}, \zeta_n] : \mathbb{Q}[\sqrt[n]{a}]] = n\varphi(n)[\mathbb{Q}[\sqrt[n]{a}] : \mathbb{Q}]^{-1} = \varphi(n)$.

Enfin, sans hypothèse sur Φ_n, la même formule que ci-dessus nous donne toujours un plongement $G \hookrightarrow \mu_n \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ tel que la composée $G \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ avec la projection sur $(\mathbb{Z}/n\mathbb{Z})^\times$ soit surjective. Mais l'image de ce plongement peut être délicate à décrire.

Remarque. – Si l'on part de a tel que $X^n - a$ est irréductible dans $\mathbb{Q}[X]$, alors l'hypothèse sur Φ_n ci-dessus équivaut à l'hypothèse que $X^n - a$ *reste irréductible dans* $\mathbb{Q}[\zeta_n][X]$, ce qui n'est pas facile à vérifier en pratique. Néanmoins, si n et $\varphi(n)$ sont premiers entre eux (en particulier si n est premier), alors l'égalité $|H_1|\varphi(n) = n|H_a|$ et les relations $|H_a||\varphi(n)$ et $|H_1||n$ montrent que $|H_1| = n$ et $|H_a| = \varphi(n)$, donc l'hypothèse est vérifiée.

Voici un exemple où l'hypothèse n'est pas vérifiée : prenons $a = -3$ et $n = 6$. Le polynôme $X^6 + 3$ est irréductible dans $\mathbb{Q}[X]$ (par le critère d'Eisenstein par exemple) et le corps $\mathbb{Q}[\sqrt[6]{-3}]$ contient une racine carrée de -3 donc contient $\zeta_6 = -\zeta_3$. Dans ce cas, on a donc $K=\mathbb{Q}[\sqrt[6]{-3}]$, $H_a=\{1\}$ et H_1 d'ordre 3 de quotient G/H_1 d'ordre 2. Le groupe G est d'ordre 6 non-abélien car la sous-extension $\mathbb{Q}[\sqrt[3]{-3}]$ n'est pas normale. On a donc $G\simeq\mathfrak{S}_3$. Via le plongement $G\hookrightarrow\mu_6\rtimes(\mathbb{Z}/6\mathbb{Z})^\times$ considéré ci-dessus, G s'identifie au sous-groupe engendré par $(\zeta_3,1)$ et $(\zeta_2,-1)$.

2.7.10 *Sous-extensions étrangères et produits semi-directs.* Soit $K\supset k$ une extension algébrique séparable et soient K_1, K_2 des sous-extensions finies sur k. Voici un cadre général pour montrer qu'un groupe de Galois est un produit semi-direct.

Proposition. – *Notons K_{12} le sous-corps de K engendré par K_1 et K_2. Les 4 propriétés suivantes sont équivalentes :*

i) $[K_{12}:k]=[K_1:k][K_2:k]$

ii) $[K_{12}:K_1]=[K_2:k]$

iii) le morphisme canonique $K_1\otimes_k K_2\longrightarrow K_{12},\ \ x_1\otimes x_2\mapsto x_1x_2$ est un isomorphisme.

iv) $\forall\alpha\in K_2$, le polynôme minimal $f_\alpha\in k[X]$ de α sur k reste irréductible dans $K_1[X]$.

Si de plus K_1 ou K_2 est normale sur k, alors ces propriétés sont aussi équivalentes à

v) $K_1\cap K_2=k$

Démonstration. L'équivalence $i)\Leftrightarrow ii)$ découle de l'égalité $[K_{12}:k]=[K_{12}:K_1][K_1:k]$. L'équivalence $ii)\Leftrightarrow iii)$ découle de la surjectivité du morphisme considéré en $iii)$ (par définition du "corps engendré") et du fait que l'extension des scalaires (ici de k à K_1) conserve la dimension.

$iii)\Rightarrow iv)$ L'isomorphisme considéré en $iii)$ induit un isomorphisme de $K_1\otimes_k k[\alpha]$ sur son image, qui n'est autre que $K_1[\alpha]$, ce qui montre que le degré de α sur K_1 est le même que sur k.

$iv)\Rightarrow ii)$ Prenons α tel que $k[\alpha]=K_2$, et notons f_α son polynôme minimal sur k. On a donc $[K_2:k]=\deg(f_\alpha)$. Par ailleurs, on a $K_{12}=K_1[\alpha]$ et $iv)$ dit que f_α est aussi le polynôme minimal de α sur K_1. Donc $[K_{12}:K_1]=\deg(f_\alpha)=[K_2:k]$.

$iv)\Rightarrow v)$ ne nécessite aucune hypothèse supplémentaire. Si $\alpha\in K_1\cap K_2$ alors le polynôme minimal de α sur K_1 est $X-\alpha$. D'après $iv)$ il vit dans $k[X]$, donc $\alpha\in k$.

$v)\Rightarrow iv)$. Notons d'abord que l'équivalence entre $iv)$ et $i)$ montre que la propriété $iv)$ est symétrique si on échange les rôles de K_1 et K_2, ce qui n'est pas évident a priori. Supposons maintenant K_2 normale sur k, pour fixer les idées. Alors pour $\alpha\in K_2$, le polynôme minimal $f_\alpha\in k[X]$ de α sur k est scindé dans $K_2[X]$. Soit $g_\alpha\in K_1[X]$ le polynôme minimal de α sur K_1. Alors g_α divise f_α donc appartient à $K_2[X]$ puisque ses coefficients sont des polynômes en les racines de g_α dans K_2. Il s'ensuit que $g_\alpha\in(K_1\cap K_2)[X]=k[X]$ et donc que $g_\alpha=f_\alpha$. $\square$

Remarque. – L'hypothèse supplémentaire est nécessaire pour que $v)$ implique les autres propriétés. Par exemple, $\mathbb{Q}(\sqrt[3]{2})\cap\mathbb{Q}(j\sqrt[3]{2})=\mathbb{Q}$, mais $\mathbb{Q}(\sqrt[3]{2},j\sqrt[3]{2})=\mathbb{Q}(\sqrt[3]{2}],j)$ est de degré 6 et non 9.

Corollaire. – *Dans le contexte de la proposition, supposons K_{12} et K_1 galoisiennes sur k. Alors* $\mathrm{Gal}(K_{12}/k)$ *est le produit semi-direct de son sous-groupe distingué* $\mathrm{Gal}(K_{12}/K_1)$ *par son sous-groupe* $\mathrm{Gal}(K_{12}/K_2)$. *Plus précisément, l'application $(\sigma,\tau)\mapsto\sigma\tau$ est un isomorphisme*

$$\mathrm{Gal}(K_{12}/K_1)\rtimes\mathrm{Gal}(K_{12}/K_2)\xrightarrow{\sim}\mathrm{Gal}(K_{12}/k)$$

où le produit semi-direct est relatif à l'action de conjugaison.

Démonstration. $\mathrm{Gal}(K_{12}/K_2)$ est en effet distingué puisque K_2 est Galoisienne. L'intersection $\mathrm{Gal}(K_{12}/K_2)\cap\mathrm{Gal}(K_{12}/K_1)$ est le sous-groupe des automorphismes qui fixent K_1 et K_2 et donc aussi le corps K_{12} qu'ils engendrent. Cette intersection est donc $\{\mathrm{id}\}$. Il s'ensuit que l'application de l'énoncé est injective. Comme les deux ensembles sont de même cardinal, elle est bijective. Enfin, la formule $(\sigma\tau)(\sigma'\tau')=(\sigma.\tau\sigma'\tau^{-1})(\tau\tau')$ montre que c'est un morphisme de groupes. $\square$

2.7.11 *Clôture normale (Galoisienne) d'une extension.* La notion de corps de décomposition d'un polynôme a un analogue pour les extensions de corps : c'est la notion de *clôture normale.*

Définition. – *Soit $K\supset k$ une extension algébrique. On dit qu'une extension $\widetilde{K}\supset k$ est une clôture normale de K si elle est normale et engendrée par toutes les images $\iota(K)$ de k-plongements $\iota:\ K\hookrightarrow\tilde{K}$.*

Lorsque $K\supset k$ est une extension séparable finie, on dit aussi que $\widetilde{K}\supset k$ est une *clôture Galoisienne* de $K\supset k$. En effet dans ce cas, $\widetilde{K}$ est aussi séparable et finie sur k.

Exemple. – Le corps de décomposition d'un polynôme irréductible séparable $f\in k[X]$ est une clôture Galoisienne du corps de rupture de f.

Proposition. – *Toute extension admet une clôture normale, unique à isomorphisme près.*

Démonstration. Choisissons une clôture algébrique $\overline{k}$ et notons $\widetilde{K}$ le sous-corps de $\overline{k}$ engendré par toutes les images $\iota(K)$, où $\iota\in\mathrm{Hom}_{k-\mathrm{alg}}(K,\overline{k})$. C'est clairement une clôture normale de K, et si $\widetilde{K}'$ en est une autre, on peut la plonger dans $\overline{k}$, son image par ce plongement est nécessairement $\widetilde{K}$, et on obtient ainsi un isomorphisme $\widetilde{K}'\xrightarrow{\sim}\widetilde{K}$. $\square$

Alternativement, si K est plongé dans une clôture algébrique $\overline{k}$, sa clôture normale dans K est le corps engendré par les images $\sigma(K)$ où σ décrit $\mathrm{Aut}(\overline{k}/k)$.

Exemple. – Si $K=k(\alpha_1,\cdots,\alpha_n)$ avec $\alpha_i\in\overline{k}$, alors $\widetilde{K}=K(\{\alpha_i^{(j)}\}_{i=1,\cdots,n;j=1,\cdots r_j})$ où $\alpha_i^{(j)}$, $j=1,\cdots,r_i$ désignent les conjugués de α_i dans $\overline{k}$. En d'autres termes K est le corps de décomposition du polynôme $f_{\alpha_1}f_{\alpha_2}\cdots f_{\alpha_n}$.

Exemple. – La clôture Galoisienne de $\mathbb{Q}(\sqrt[3]{2},\sqrt[5]{3})$ dans $\overline{\mathbb{Q}}$ est $\mathbb{Q}(\sqrt[3]{2},\sqrt[5]{3},e^{2i\pi/15})$.

2.8 Résolubilité par radicaux des équations algébriques

Comme on l'a déjà mentionné dans l'introduction de ce chapitre, la théorie de Galois permet de résoudre le problème de la résolubilité par radicaux des équations algébriques. C'est ce que nous allons expliquer ici.

2.8.1 *Groupe de Galois d'un polynôme.* Soit $f \in k[X]$ un polynôme séparable. On appelle *groupe de Galois de* f le groupe de Galois G_f d'un corps de décomposition K_f de f sur k. Ce groupe permute les racines de f, et son action sur K_f est déterminée par celle sur les racines de f car celles-ci engendrent K_f. Ainsi G_f s'identifie à un sous-groupe du groupe des permutations des racines de f. Si on numérote les racines $\alpha_1, \cdots, \alpha_n$ de f dans K_f, alors G_f s'identifie à un sous-groupe de $\mathfrak{S}_n$.

LEMME. – *Le polynôme f est irréductible dans $k[X]$ si et seulement si G_f permute transitivement les racines de f dans K_f.*

Démonstration. On a déjà vu cela plusieurs fois. Répétons l'argument. Si f est irréductible et α, β sont deux racines, il existe un unique k-isomorphisme $k[\alpha] \xrightarrow{\sim} k[\beta]$ qui envoie α sur β et celui-ci se prolonge en un automorphisme $K_f \xrightarrow{\sim} K_f$ car K_f est normale. Réciproquement, la propriété ii) des extensions Galoisiennes nous dit que si G_f agit transitivement sur les racines de f, alors f est le polynôme minimal de chacune de ses racines, et en particulier est irréductible. $\square$

Si on a au contraire une factorisation $f = f_1 f_2$ dans $k[X]$, alors soit K_{f_i} le sous-corps de K_f engendré par les racines de f_i. Puisque K_{f_i} est galoisienne sur k, on a un morphisme surjectif $G_f \twoheadrightarrow G_{f_i}$ de noyau $\mathrm{Gal}(K_f/K_{f_i})$. Le morphisme produit $G_f \longrightarrow G_{f_1} \times G_{f_2}$ est lui injectif puisque K_f est engendré par $K_{f_1}.K_{f_2}$.

2.8.2 *Résolubilité par radicaux et groupes résolubles.* Rappelons qu'un polynôme $f \in \mathbb{Q}[X]$ est dit "résoluble par radicaux" si ses racines peuvent s'exprimer en appliquant successivement des opérations parmi $+, -, \cdot, \div$ et $\sqrt[n]{x}$ à des nombres rationnels.

DÉFINITION. – *Un groupe fini G est dit résoluble s'il admet une suite décroissante $G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$ de sous-groupes tels que G_{i+1} est distingué dans G_i et G_i/G_{i+1} est abélien.*

Exercice. – Soit H un sous-groupe de G. Montrer que :
— G résoluble $\Rightarrow$ H résoluble.
— Si H est distingué, G résoluble $\Leftrightarrow$ (H et G/H résolubles).

Le théorème de Galois s'exprime ainsi :

THÉORÈME. – *Le polynôme f est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.*

Démonstration. Supposons d'abord f résoluble par radicaux. Ceci équivaut à ce que K_f soit inclus dans le "dernier étage" K_r d'une tour d'extensions $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r$, telle que pour tout $i = 1, \cdots, r$, on a $K_i = K_{i-1}(\alpha_i)$ avec $\alpha_i^{n_i} \in K_{i-1}$ pour un $n_i \in \mathbb{N}$. On peut choisir cette tour de sorte que K_1 soit n-cyclotomique avec n le ppcm des n_i. Alors chaque extension $K_i \supset K_{i-1}$ est Galoisienne de groupe de Galois abélien, d'après 2.7.5 et 2.7.4. Malheureusement K_i n'est pas nécessairement Galoisienne sur $\mathbb{Q}$ pour $i > 2$. Remplaçons donc K_i par sa clôture Galoisienne K_i' dans $\overline{\mathbb{Q}}$. On a donc une tour $\mathbb{Q} = K_0 \subset K_1 = K_1' \subset K_2' \subset \cdots \subset K_r'$ d'extensions Galoisiennes avec $K_i' = K_{i-1}'(\alpha_i^{(j)}, j = 1, \cdots, r_i)$ où les $\alpha_i^{(j)}$ désignent les conjugués de α_i dans $\overline{\mathbb{Q}}$. Alors $(\alpha_i^{(j)})^{n_i}$ est un conjugué de $\alpha_i^{n_i}$ donc appartient à K_{i-1}', et le corollaire 2.7.5 nous dit que $\mathrm{Gal}(K_i'/K_{i-1}')$ est abélien.

Traduisons cela via la correspondance de Galois. Notons $G_i' := \mathrm{Gal}(K_r'/K_i')$, qui est un sous-groupe de $G_0' = \mathrm{Gal}(K_r'/\mathbb{Q})$. Alors les G_i' sont distingués dans G_0', et les quotients successifs G_i'/G_{i+1}' sont abéliens. Le groupe G_0' est donc résoluble. Il s'ensuit que le groupe $G_f := \mathrm{Gal}(K_f/\mathbb{Q})$, qui est un quotient de G_0 puisque $K_f \subset K_r'$, est aussi résoluble. En effet, si $G_{f,i}$ désigne l'image de G_i' dans G_f, alors chaque $G_{f,i}$ est distingué dans G_f et les quotients successifs $G_{f,i}/G_{f,i+1}$ sont abéliens, puisque quotients de G_i/G_{i+1}.

Réciproquement, supposons maintenant que $G_f = \mathrm{Gal}(K_f/\mathbb{Q})$ est résoluble. Notons K_f' le corps engendré par K_f et les racines n-èmes de l'unité où $n = [K_f : \mathbb{Q}]$. C'est aussi une extension Galoisienne de $\mathbb{Q}$, dont le groupe de Galois G_f' se surjecte sur G_f avec noyau $\mathrm{Gal}(K_f'/K_f)$ abélien (d'ordre divisant $\varphi(n)$). Donc G_f' est aussi un groupe résoluble. Notons $G_{f,1}' := \mathrm{Gal}(K_f'/\mathbb{Q}(e^{2i\pi/n}))$, qui est un sous-groupe distingué de G_f' de quotient $G_f'/G_{f,1}'$ abélien (isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$). Puisque G_f' est résoluble, il existe des sous-groupes $G_{f,1}' \supset G_{f,2}' \supset \cdots \supset G_{f,r}' = \{1\}$ tels que $G_{f,i+1}'$ soit distingué dans $G_{f,i}'$ de quotient abélien. En fait, puisque tout groupe abélien fini est produit de groupes cycliques, on peut même supposer que $G_{f,i}'/G_{f,i+1}'$ est cyclique. Notons que pour $i \geqslant 1$, l'ordre de $G_{f,i}'/G_{f,i+1}'$ divise celui de $G_f'/G_{f,1}'$ qui est égal au degré $[K_f' : \mathbb{Q}(e^{2i\pi/n})]$, lequel divise $[K_f : \mathbb{Q}] = n$. Soit alors $K_{f,i}' := (K_f')^{G_i}$. La correspondance de Galois nous dit que la tour

$$\mathbb{Q} \subset \mathbb{Q}(e^{2i\pi/n}) = K_{f,1}' \subset K_{f,2}' \subset \cdots \subset K_{f,r}' = K_f'$$

est formée d'extensions Galoisiennes telles que $K_{f,i}'/K_{f,i-1}'$ est de groupe de Galois cyclique d'ordre n_i divisant n. D'après le théorème 2.7.5, une telle extension est de la forme $K_{f,i}' = K_{f,i-1}'(\sqrt[n_i]{a_i})$. Il s'ensuit que f est résoluble par radicaux. □

2.8.3 *Résolubilité des équations de degré au plus* 4. À l'époque de Galois, on savait déjà depuis longtemps que les polynômes de degré au plus 4 étaient résolubles par radicaux. En voici une explication conceptuelle. Soit $n := \deg(f)$. On a vu que l'action de permutation de $G_f := \mathrm{Gal}(K_f/K)$ sur l'ensemble des racines de f fournit un plongement $G_f \hookrightarrow \mathfrak{S}_n$ (une fois qu'on a numéroté les racines). Or, pour $n \leqslant 4$, le groupe $\mathfrak{S}_n$ est résoluble. En effet, $\mathfrak{S}_2 = \mathbb{Z}/2\mathbb{Z}$ est abélien, $\mathfrak{S}_3$ se surjecte sur $\mathbb{Z}/2\mathbb{Z}$ (signature) avec pour noyau $\mathfrak{A}_3 = \mathbb{Z}/3\mathbb{Z}$, et $\mathfrak{S}_4$ se surjecte sur $\mathbb{Z}/2\mathbb{Z}$ avec pour noyau $\mathfrak{A}_4$ dont le sous-groupe $\{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ est distingué de quotient isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Comme tout sous-groupe d'un groupe résoluble est résoluble (exercice), il s'ensuit que G_f est bien résoluble dès que $\deg(f) \leqslant 4$.

2.8.4 *Non-résolubilité d'une équation de degré* 5. C'est à Abel qu'est attribué le premier exemple d'équation algébrique non résoluble par radicaux. Mais la théorie de Galois donne une explication plus conceptuelle aux exemples d'Abel.

LEMME. – *Le groupe $\mathfrak{S}_n$, $n \geqslant 5$ n'est pas résoluble.*

Démonstration. Il suffit de montrer que $\mathfrak{A}_n$ n'est pas résoluble. Pour cela, il suffit de montrer que $\mathfrak{A}_n$ ne possède aucun quotient abélien. Ceci équivaut à montrer que le sous-groupe $[\mathfrak{A}_n, \mathfrak{A}_n]$ engendré par les commutateurs $xyx^{-1}y^{-1}$ d'éléments de $\mathfrak{A}_n$ est égal à $\mathfrak{A}_n$. En effet, tout morphisme $\mathfrak{A}_n \longrightarrow G$ avec G abélien est trivial sur $[\mathfrak{A}_n, \mathfrak{A}_n]$.

Rappelons que $\mathfrak{A}_n$ est engendré par les 3-cycles. En effet, il suffit de voir que le produit de deux transpositions $\tau = (i,j)(k,l)$ est un produit de 3-cycles. Si $\{i,j\} = \{k,l\}$ on a $\tau = \mathrm{id}$, si $|\{i,j\} \cap \{k,l\}| = 1$, alors, en supposant que $j = k$ par exemple, on a $\tau = (i,j,l)$, et si $\{i,j\} \cap \{k,l\} = \emptyset$ alors $\tau = (i,j)(j,k)(j,k)(k,l) = (i,j,k)(j,k,l)$.

Il nous suffit donc de voir que tout 3-cycle est un commutateur dans $\mathfrak{A}_n$. On a la formule $(i,j,k) = (i,j)(j,k) = (i,j)(i,k)(i,j)^{-1}(i,k)^{-1}$ qui montre que (i,j,k) est un commutateur dans $\mathfrak{S}_n$. Pour passer à un commutateur dans $\mathfrak{A}_n$, choisissons, $l \neq m$ distincts de (i,j,k), ce qui est possible car $n \geqslant 5$. Alors, (l,m) commute à (i,j) et (i,k), donc en posant $\tau = (i,j)(l,m)$ et $\sigma = (i,k)(l,m)$, on a $\tau\sigma\tau^{-1}\sigma^{-1} = (i,j,k)$, et $\tau, \sigma \in \mathfrak{A}_n$. □

Remarque. – En fait, on a beaucoup mieux : pour $n \geqslant 5$, le groupe $\mathfrak{A}_n$ est *simple*, i.e. ne possède aucun sous-groupe distingué propre et non trivial.

Notre but est maintenant de produire un polynôme de degré 5 dont le groupe de Galois est $\mathfrak{S}_5$. Pour cela, le lemme suivant sera utile :

LEMME. – *Si n est premier, le groupe $\mathfrak{S}_n$ est engendré par toute paire d'éléments (σ, τ) formée d'un n-cycle et d'une transposition.*

Démonstration. Soit $\tau = (i,j)$ avec $i \neq j$. Comme n est premier, l'unique puissance de σ qui envoie i sur j est encore un n-cycle. On peut donc supposer que $j = \sigma(i)$. On a alors $\sigma^s\tau\sigma^{-s} = (\sigma^s(i), \sigma^{s+1}(i))$ pour tout $s = 0, \cdots, n-1$. Soit alors $r > s$. On a

$$\begin{aligned} & (\sigma^{r-1}(i),\sigma^r(i))\cdots(\sigma^{s+1}(i),\sigma^{s+2}(i))(\sigma^s(i),\sigma^{s+1}(i))(\sigma^{s+1}(i),\sigma^{s+2}(i))\cdots(\sigma^{r-1}(i),\sigma^r(i)) \\ = \; & (\sigma^s(i),\sigma^r(i)), \end{aligned}$$

ce qui montre que le sous-groupe engendré par σ et τ contient toutes les transpositions, donc est égal à $\mathfrak{S}_n$. □

Nous voulons donc trouver un polynôme de degré 5 dont le groupe de Galois contient un 5-cycle et une transposition. Remarquons alors :

LEMME. – *Soit $f \in k[X]$ séparable. Si f est irréductible de degré premier p, alors G_f contient un p-cycle du groupe des permutations des racines de f.*

Démonstration. Tout corps de rupture de f est de degré p (isomorphe à $k[X]/(f)$ puisque f est irréductible), donc $p | [K_f : k]$ et G_f contient donc un élément d'ordre p. Mais les seuls éléments d'ordre p de $\mathfrak{S}_p$ sont les p-cycles. □

Pour trouver des polynômes irréductibles, le critère suivant est très utile.

PROPOSITION. (Critère d'Eisenstein) – *Soit* $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. *Supposons qu'il existe un nombre premier* p *tel que* p *divise* a_i *pour tout* i*, mais* p^2 *ne divise pas* a_0*. Alors* f *est irréductible dans* $\mathbb{Q}[X]$.

Démonstration. Soit $f = gh$ une factorisation dans $\mathbb{Q}[X]$ avec g et h unitaires. On a déjà expliqué qu'on a alors $g, h \in \mathbb{Z}[X]$. Ecrivons $g = X^m + b_{m-1}X^{m-1} + \cdots + b_0$ et $h = X^r + c_{r-1}X^{r-1} + \cdots + c_0$. Alors $b_0c_0 = a_0$ donc p ne divise pas b_0 ou ne divise pas c_0. Supposons que p ne divise pas c_0 et soit k le plus petit entier tel que p ne divise pas b_k (qui existe bien puisque $b_m = 1$). Alors l'égalité $a_k = \sum_{i+j=k} b_ic_j$ montre que p ne divise pas a_k, donc $k = n$ et $h(X) = 1$. □

On voudrait maintenant un moyen de produire une transposition dans le groupe de Galois d'un polynôme irréductible de $\mathbb{Q}[X]$. L'astuce pour cela est d'utiliser la conjugaison complexe, qui au moins fournit un automorphisme d'ordre 2. Supposons en effet que f possède exactement 2 racines dans $\mathbb{C} \setminus \mathbb{R}$. Alors la conjugaison complexe permute ces deux racines et fixe toutes les autres. Elle fournit donc une transposition dans G_f.

COROLLAIRE. – *Le groupe de Galois du polynôme* $f = X^5 - 10X + 5 \in \mathbb{Q}[X]$ *est* $\mathfrak{S}_5$*. En particulier,* f *n'est pas résoluble par radicaux.*

Démonstration. Le critère d'Eisenstein avec $p = 5$ montre que f est irréductible dans $\mathbb{Q}[X]$, donc le dernier lemme assure que G_f contient un 5-cycle. Par ailleurs, le tableau des variations de la fonction $\mathbb{R} \longrightarrow \mathbb{R}$, $x \mapsto f(x)$ montre que f a trois racines réelles, donc G_f contient une transposition. Il s'ensuit que $G_f \simeq \mathfrak{S}_5$. □

2.9 Nombres constructibles à la règle et au compas

Voici une autre illustration des implications de la théorie de Galois sur des problèmes classiques de l'antiquité.

DÉFINITION. – *Dans le plan euclidien* $\mathbb{R}^2$*, un point* P *est dit :*

— 0*-constructible si* $P \in \{(0,0), (1,0)\}$

— n*-constructible s'il est* $(n-1)$*-constructible ou s'il existe des points* $n-1$*-constructibles* $A \neq B$ *et* $C \neq D$ *tels que* P *soit dans l'une des intersections suivantes, supposée transverse :*

  — *des droites* (AB) *et* (CD)

  — *ou de la droite* (AB) *et du cercle de centre* C *passant par* D

  — *ou des cercles de centres respectifs* C *et* A*, passant respectivement par* D *et* B*.*

Un nombre complexe $z \in \mathbb{C}$ *est dit* constructible *si le point correspondant est* n*-constructible pour un* $n \in \mathbb{N}$*.*

La géométrie élémentaire classique nous apprend à projeter un point orthogonalement sur une droite à la règle et au compas, ce dont on déduit :

Lemme. – *Un complexe est constructible si et seulement si ses parties réelles et imaginaires le sont.*

Notons $E \subset \mathbb{C}$ l'ensemble des nombres constructibles.

Théorème. – *E est un sous-corps de $\mathbb{C}$ stable par extraction de racine carrée.*

Démonstration. Exercice. La stabilité par soustraction est claire, utiliser Thalès pour la multiplication de réels, la construction de l'inversion géométrique pour le passage à l'inverse, puis Pythagore pour la racine carrée d'un réel positif. □

L'équation d'un cercle et celle d'une droite montrent que les coordonnées de leurs point(s) d'intersection sont solutions d'une équation du second degré en les coordonnées des points utilisés pour définir le cercle et la droite. Les nombres constructibles sont donc algébriques. Plus précisément, on a :

Théorème. (Wantzen) – *Un complexe z est constructible si et seulement si il existe une suite de corps $K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_r$ tels que $[K_i : K_{i-1}] = 2$ et $z \in K_r$.*

Démonstration. Exercice. On remarquera que toute extension quadratique est obtenue par extraction d'une racine carrée. □

Ici intervient la théorie de Galois, et notamment la notion de conjugué.

Théorème. – *Un nombre algébrique $z \in \overline{\mathbb{Q}}$ est constructible si et seulement si l'extension algébrique de $\mathbb{Q}$ engendrée par ses conjugués est de degré une puissance de 2.*

Démonstration. Remarquons tout d'abord que si z est constructible alors ses conjugués le sont aussi. En effet, si $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ et si $K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_r$ est une tour d'extensions quadratiques contenant z, alors $\sigma(K_0) = \mathbb{Q} \subset \sigma(K_1) \subset \cdots \subset \sigma(K_r)$ est une tour d'extensions quadratiques contenant $\sigma(z)$. Soit alors K_z le corps engendré par les conjugués de z. Il est contenu dans E et engendré par un élément primitif α. Puisque α est constructible, il est contenu dans une tour d'extensions quadratiques, donc K_z aussi, et K_z est bien de degré une puissance de 2.

Réciproquement, supposons que le corps K_z est de degré une puissance de 2. Comme c'est le corps de décomposition du polynôme minimal f_z de z, c'est une extension Galoisienne dont le groupe de Galois G_z est un 2-groupe. Or, tout 2-groupe possède un sous-groupe (distingué) d'indice 2. Inductivement, il existe donc une suite décroissante $G_0 = G_z \supset G_1 \supset \cdots \supset G_r = \{1\}$ de sous-groupes de G_z telle que $[G_i : G_{i+1}] = 2$. En prenant les corps de points fixes $K_i = K_z^{G_i}$, on obtient une tour d'extensions quadratiques comme dans le théorème précédent. □

Ce résultat s'applique au problème classique de savoir quels polygones réguliers peuvent être construits à la règle et au compas. Si n est le nombre de côtés, c'est équivalent à déterminer si $\exp(2i\pi/n)$ est constructible. Par le théorème précédent, c'est encore équivalent à ce que $[\mathbb{Q}(\exp(2i\pi/n)) : \mathbb{Q}]$ soit de degré une puissance de 2. Or on a vu que $[\mathbb{Q}(\exp(2i\pi/n)) : \mathbb{Q}] = \varphi(n)$. Par la formule usuelle de $\varphi(n)$, on obtient donc :

Corollaire. – *Un polygone régulier à n côtés est constructible à la règle et au compas si et seulement si $n = 2^a p_1 p_2 \cdots p_r$ avec p_i des premiers distincts de la forme $p_i = 1 + 2^{a_i}$.*

Remarquons que pour que $p = 1 + 2^a$ soit premier, il faut que a soit lui-même une puissance de 2. En effet, si on écrit $a = 2^b m$ avec m impair, on a $1 + 2^a = 1 - (-2^{2^b})^m$ qui est divisible par $1 + 2^{2^b}$. Les nombres de la forme $p = 1 + 2^{2^b}$ sont appelés “nombres de Fermat” car Fermat avait émis l'hypothèse qu'ils soient tous premiers, ce qui est vrai jusqu'à $b = 4$, mais faux pour $5 \leqslant b \leqslant 23$ et inconnu au-delà. En particulier, 17 est un nombre de Fermat premier, et la constructibilité du polygone régulier à 17 côtés avait été établie par Gauss.

2.10 Spécialisation du groupe de Galois

2.10.1 Soit A un anneau principal de corps des fractions K. Fixons un élément irréductible $p \in A$ et notons $k = A/pA$ le corps résiduel.

Soit maintenant $f \in A[X]$ un polynôme unitaire et soit K_f “son” corps de décomposition sur K. On a donc une décomposition $f = (X - \alpha_1) \cdots (X - \alpha_n)$ dans $K_f[X]$.

Notons $A_f := A[\alpha_1, \cdots, \alpha_n]$ la sous-A-algèbre de K_f engendrée par les racines α_i de f.

Lemme. – *En tant que A-module, A_f est libre de rang $[K_f : K]$.*

Démonstration. Manifestement A_f engendre K_f comme K-espace vectoriel. Vu le i) du corollaire 1.9.5, il suffit donc de montrer que A_f est de type fini comme A-module. Or, puisque f annule chaque α_i, il est engendré par les éléments $\alpha_1^{n_1} \cdots \alpha_n^{n_n}$ avec $n_1, \cdots, n_n \leqslant n$. □

Notons $\overline{f}$ l'image de f dans $k[X]$. Soit $\mathfrak{m} \subset A_f$ un idéal maximal de A_f qui contient p, et soit $k_f := A_f/\mathfrak{m}$ le corps résiduel. C'est une extension finie de $A/pA = k$, engendrée par les images $\overline{\alpha}_i$ des α_i. La factorisation $\overline{f} = (X - \overline{\alpha}_1) \cdots (X - \overline{\alpha}_n)$ montre donc que k_f est un corps de décomposition de $\overline{f}$ sur k.

Lemme. – *Si $\overline{f}$ est séparable dans $k[X]$, alors f est séparable dans $K[X]$.*

Démonstration. Si $\overline{f}$ est séparable, les $\overline{\alpha}_i$ sont tous distincts, donc les α_i aussi et f est séparable aussi. □

Nous supposons dorénavant que $\overline{f}$ est séparable. Notons $G_f = \mathrm{Gal}(K_f/K)$ et $G_{\overline{f}} := \mathrm{Gal}(k_f/k)$ les groupes de Galois correspondants. Notre but est de comparer G_f et $G_{\overline{f}}$.

L'action de G_f sur K_f stabilise manifestement A_f puisqu'elle permute les α_i. Cette action induit à son tour une action sur l'ensemble des idéaux de A_f qui stabilise l'ensemble $\mathrm{Max}(A_f)$ des idéaux maximaux, ainsi que le sous-ensemble $\mathrm{Max}(A_f/p)$ des idéaux maximaux contenant p. Notons alors $G_{f,\mathfrak{m}}$ le fixateur de l'élément $\mathfrak{m} \in \mathrm{Max}(A_f/p)$. On a donc $G_{f,\mathfrak{m}} = \{\sigma \in G_f, \sigma(\mathfrak{m}) = \mathfrak{m}\}$, donc $G_{\mathfrak{m},f}$ est aussi le stabilisateur de $\mathfrak{m}$ dans G_f. L'action de $G_{f,\mathfrak{m}}$ sur A_f par automorphismes de A-algèbre passe alors au quotient pour donner une action sur k_f par automorphismes de A/p-algèbres. On a donc un morphisme $G_{f,\mathfrak{m}} \longrightarrow G_{\overline{f}}$, $\sigma \mapsto \overline{\sigma}$ caractérisé par $\forall a \in A_f, \overline{\sigma}(\overline{a}) = \overline{\sigma(a)}$ où $\overline{a}$ désigne la réduction de a modulo $\mathfrak{m}$.

THÉORÈME. – *Le morphisme $G_{f,\mathfrak{m}} \longrightarrow G_{\overline{f}}$ est un isomorphisme.*

Démonstration. En suivant l'action sur les racines, on constate que ce morphisme s'inscrit dans le diagramme commutatif suivant :

$$\begin{tikzcd} G_{f,\mathfrak{m}} \arrow[r, hook] \arrow[dr, "\sigma\mapsto\overline{\sigma}"'] & G_f \arrow[r, hook] & \mathfrak{S}_{\{\alpha_1,\cdots,\alpha_n\}} = \mathfrak{S}_n \arrow[d, equal] \\ & G_{\overline{f}} \arrow[r, hook] & \mathfrak{S}_{\{\overline{\alpha}_1,\cdots,\overline{\alpha}_n\}} = \mathfrak{S}_n \end{tikzcd}$$

Son injectivité en découle immédiatement, et en particulier l'inégalité $|G_{f,\mathfrak{m}}| \leqslant |G_{\overline{f}}|$.

Par ailleurs, soit $M := G_f \cdot \mathfrak{m} \subset \mathrm{Max}(A_f/pA_f)$ l'orbite de l'idéal maximal $\mathfrak{m}$ sous G_f. Le théorème des restes chinois nous donne un morphisme surjectif de k-algèbres

$$A_f/pA_f \twoheadrightarrow \prod_{\mathfrak{n}\in M} A_f/\mathfrak{n},$$

d'où l'inégalité $\dim_k(A_f/pA_f) = [K_f : K] = |G_f| \geqslant \sum_{\mathfrak{n}\in M} \dim_k(A_f/\mathfrak{n})$. Or chaque $A_f/\mathfrak{n}$ est un corps de décomposition de f, donc $\dim_k(A_f/\mathfrak{n}) = [k_f : k] = |G_{\overline{f}}|$. Puisque $|M| = [G_f : G_{f,m}]$, l'inégalité devient $|G_f| \geqslant [G_f : G_{f,m}]|G_{\overline{f}}|$, et implique donc l'inégalité $|G_{f,m}| \geqslant |G_{\overline{f}}|$. Puisqu'on a déjà vu l'autre inégalité, on a $|G_f| = |G_{f,\mathfrak{m}}|$, et donc le morphisme de l'énoncé est aussi bijectif. □

Remarque. – Sous l'hypothèse $\overline{f}$ séparable, le théorème nous fournit donc un plongement $i_{\mathfrak{m}} : G_{\overline{f}} \hookrightarrow G_f$. Ce plongement dépend a priori de deux choix : d'une part le choix de $\mathfrak{m}$ et d'autre part celui d'un isomorphisme de k-extensions $A_f/\mathfrak{m} \xrightarrow{\sim} k_{\overline{f}}$. Si l'on fixe $\mathfrak{m}$, le plongement $i_{\mathfrak{m}}$ n'est donc bien défini qu'à "conjugaison à la source près". Que se passe-t-il si maintenant on choisit un autre $\mathfrak{m}'$? La preuve ci-dessus implique que le morphisme $A_f/pA_f \twoheadrightarrow \prod_{\mathfrak{n}\in M} A_f/\mathfrak{n}$ est un isomorphisme, ce qui signifie que $M = \mathrm{Max}(A_f/pA_f)$, i.e. que G_f agit transitivement sur $\mathrm{Max}(A_f/pA_f)$. Il existe donc $\sigma \in G_f$ tel que $\sigma(\mathfrak{m}) = \mathfrak{m}'$. On a alors $\sigma G_{f,\mathfrak{m}}\sigma^{-1} = G_{f,\mathfrak{m}'}$, et les plongements $i_{\mathfrak{m}'}$ et $\tau \mapsto \sigma i_{\mathfrak{m}}(\tau)\sigma^{-1}$ de $G_{\overline{f}}$ dans G_f sont conjugués "à la source". En d'autre termes, on a construit une *classe de conjugaison canonique* de plongements $G_{\overline{f}} \hookrightarrow G_f$.

2.10.2 *Application aux polynômes dans* $\mathbb{Z}[X]$. Supposons ici $A = \mathbb{Z}$. Dans ce cas $k = \mathbb{F}_p$ et on sait que $G_{\overline{f}}$ est cyclique engendré par le Frobenius F. Soit alors $\overline{f} = \overline{f}_1\overline{f}_2\cdots\overline{f}_r$ la décomposition de $\overline{f}$ en produit d'irréductibles dans $\mathbb{F}_p[X]$, et soit $n_i := \deg(\overline{f}_i)$. Cela correspond à une partition de l'ensemble des racines

$$R(\overline{f}) = \{\overline{\alpha}_1, \cdots, \overline{\alpha}_n\} = \bigsqcup_{i=1}^{r} R(\overline{f}_i).$$

Cette partition est respectée par F, et F agit transitivement sur chaque $R(\overline{f}_i)$. Ainsi, l'image de F dans $\mathfrak{S}_n$ est un produit $c_1\cdots c_r$ de cycles disjoints de longueurs respectives $n_1, \cdots, n_r$. On a donc prouvé :

Corollaire. – *Soit $f \in \mathbb{Z}[X]$ de degré n et p premier tel que $\overline{f} \in \mathbb{F}_p[X]$ est séparable et de décomposition en irréductibles $\overline{f} = \overline{f}_1\overline{f}_2 \cdots \overline{f}_r$. Alors G_f, vu comme sous-groupe de $\mathfrak{S}_n$, contient un produit $c_1 \cdots c_r$ de cycles disjoints de longueurs respectives* $\deg(\overline{f}_i)$.

Pour appliquer cet énoncé, il faut donc être capable de factoriser $\overline{f}$. Pour cela, il est utile de remarquer que $\overline{f}$ possède un facteur irréductible de degré r si et seulement si il admet une racine dans $\mathbb{F}_{p^r}$ qui n'est dans aucun $\mathbb{F}_{p^s}$ pour $s|r$, $s \neq r$. Par ailleurs, $\overline{f}$ admet une racine dans $\mathbb{F}_{p^r}$ si et seulement si il n'est pas premier à $X^{p^r} - X$, ce qui peut se vérifier par divisions euclidiennes successives et/ou un peu d'astuce.

Exemple. – Condidérons le polynôme $f = X^5 - X - 1$.

– Modulo 2. On vérifie que $\overline{f}$ n'a pas de racine dans $\mathbb{F}_2$, mais il en a deux dans $\mathbb{F}_4$ puisque $\overline{f} \equiv X^2 - X - 1 \,(\mathrm{mod}\,(\mathrm{X}^4 - \mathrm{X}))$ et $\overline{f}_1 := X^2 - X - 1 = X^2 + X + 1 | X^4 - X$. Il s'ensuit que $\overline{f} = \overline{f}_1\overline{f}_2$ avec $\overline{f}_2$ irréductible de degré 3. Le corollaire nous dit que G_f contient une permutation de type $(2, 3)$, et le cube de cette permutation est donc une transposition.

– Modulo 3. On vérifie que $\overline{f}$ n'a pas de racine dans $\mathbb{F}_3$, donc pas de facteur de degré 1. Puis on calcule le pgcd avec $X^9 - X$ (d'abord avec $X^4 - 1$ puis avec $X^4 + 1$) pour constater que $\overline{f}$ n'a pas de racine dans $\mathbb{F}_9$, donc pas de facteur de degré 2. Il s'ensuit que $\overline{f}$ est irréductible et G_f contient donc un 5-cycle.

– Conclusion. $G_f \simeq \mathfrak{S}_5$.

Exemple. (Corps cyclotomiques) – Considérons le polynôme cyclotomique $f = \Phi_n$. Le polynôme $f \bmod p$ est séparable si et seulement si p ne divise pas n. Comme le groupe de Galois $G_f = (\mathbb{Z}/n\mathbb{Z})^\times$ est abélien, le plongement $\iota : G_{\overline{f}} \hookrightarrow G_f$ construit dans le théorème est canonique (et pas seulement à conjugaison près). On voudrait calculer l'image du Frobenius $\iota(F)$ à travers l'isomorphisme $G_f \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$ donné par le caractère cyclotomique $\chi_{n,\mathbb{Q}}$. Pour cela, on constate sur la construction de ι et les définitions de $\chi_{n,\mathbb{Q}}$ et $\chi_{n,\mathbb{F}_p}$ que le diagramme suivant est commutatif

$$\begin{tikzcd}
G_f \arrow[r, hook, "\chi_{n,\mathbb{Q}}"] & (\mathbb{Z}/n\mathbb{Z})^\times = \mathrm{Aut}(\mu_n) \subset \mathfrak{S}_{\{\text{rac. prim. } n^{emes} \text{ de } 1\}} \arrow[d, equal] \\
G_{\overline{f}} \arrow[u, hook, "\iota"] \arrow[r, hook, "\chi_{n,\mathbb{F}_p}"] & (\mathbb{Z}/n\mathbb{Z})^\times = \mathrm{Aut}(\mu_n) \subset \mathfrak{S}_{\{\text{rac. prim. } n^{emes} \text{ de } 1\}}
\end{tikzcd}$$

On a donc $\chi_{n,\mathbb{Q}}(\iota(F)) = \chi_{n,\mathbb{F}_p}(F) = p \in (\mathbb{Z}/n\mathbb{Z})^\times$. On peut en déduire la forme de la factorisation de la réduction $\bar{\Phi}_n$ dans $\mathbb{F}_p[X]$ (toujours sous l'hypothèse $(p, n) = 1$). En effet, soit r l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Alors les orbites de l'action de p sur les racines primitives n-èmes de l'unité donnée par $\xi \mapsto \xi^p$ sont de cardinal r et il y en a $s := \varphi(n)/r$. Il s'ensuit que $\bar{\Phi}_n = f_1 \cdots f_s$ dans $\mathbb{F}_p[X]$ avec f_i irréductibles de degré r premiers entre eux deux à deux. En particulier :

- $\bar{\Phi}_n$ est scindé dans $\mathbb{F}_p[X]$ si et seulement si $p \equiv 1[n]$.
- $\bar{\Phi}_n$ est irréductible dans $\mathbb{F}_p[X]$ si et seulement si p est un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$ (et on voit donc que Φ_n n'est jamais irréductible dans $\mathbb{F}_p[X]$ si $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique).

Exemple. (Corps quadratiques) – Soit $d \in \mathbb{Z}$ sans facteur carré et $f = X^2 - d$. Si l'on choisit une racine carrée $\sqrt{d}$ dans $\overline{\mathbb{Q}}$, alors $K_f = \overline{\mathbb{Q}}[\sqrt{d}]$ et l'application $\varepsilon_{d,\mathbb{Q}} : \sigma \mapsto \frac{\sigma(\sqrt{d})}{\sqrt{d}}$ est un isomorphisme $G_f \xrightarrow{\sim} \{\pm 1\}$ qui ne dépend pas du choix de $\sqrt{d}$. On voit que $\overline{f} = f \bmod p$ est séparable si et seulement si $(p, 2d) = 1$. Dans ce cas, puisque G_f est abélien, le plongement $\iota : G_{\overline{f}} \hookrightarrow G_f$ est encore canonique et on aimerait calculer $\iota(F)$. Pour cela, on vérifie sur la construction que le diagramme suivant est commutatif

$$\begin{tikzcd} G_f \arrow[r, hook, "\varepsilon_{d,\mathbb{Q}}"] & \{\pm 1\} \arrow[d, equal] \\ G_{\overline{f}} \arrow[u, hook, "\iota"] \arrow[r, hook, "\varepsilon_{d,\mathbb{F}_p}"] & \{\pm 1\} \end{tikzcd}.$$

On a donc $\varepsilon_{d,\mathbb{Q}}(\iota(F)) = \varepsilon_{d,\mathbb{F}_p}(F)$. Concrètement, on a $\varepsilon_{d,\mathbb{F}_p}(F) = -1$ si et seulement si $\overline{f} = X^2 - \overline{d}$ est irréductible, c'est-à-dire si et seulement si d n'est pas un carré modulo p. Il s'ensuit que le signe $\varepsilon_{d,\mathbb{F}_p}(F)$ n'est autre que le symbole de Legendre $\left(\frac{d}{p}\right)$.

Application. (Loi de réciprocité quadratique) – Soit q un premier impair. Un calcul élémentaire montre que

$$\prod_{0 \leqslant i < j < q} (\zeta_q^i - \zeta_q^j)^2 = (-1)^{\frac{q(q-1)}{2}} q^q = (-1)^{\frac{q-1}{2}} q^q.$$

Il s'ensuit que $\mathbb{Q}(\zeta_q) \supset \mathbb{Q}(\sqrt{q^*})$ où on a posé $q^* = (-1)^{\frac{q-1}{2}} q$. Par la correspondance de Galois, on a donc un morphisme surjectif $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{q^*})/\mathbb{Q})$. Via le caractère cyclotomique $\chi_{q,\mathbb{Q}}$ et le caractère quadratique $\varepsilon_{q^*,\mathbb{Q}}$, ce morphisme devient un morphisme surjectif $(\mathbb{Z}/q\mathbb{Z})^\times \twoheadrightarrow \{\pm 1\}$. Mais puisque q est premier, le groupe $(\mathbb{Z}/q\mathbb{Z})^\times$ est cyclique, donc il existe un unique tel morphisme surjectif, et de plus, son noyau est le sous-groupe des carrés dans $(\mathbb{Z}/q\mathbb{Z})^\times$ (ie l'image de $x \mapsto x^2$).

Notons maintenant $f = \Phi_q$ et $g = X^2 - q^*$, fixons p premier impair différent de q, et notons $\overline{f}, \overline{g} \in \mathbb{F}_p[X]$ les réductions de f et g. Alors $\overline{f}$ et $\overline{g}$ sont séparables et $k_{\overline{f}}$ contient un corps de décomposition $k_{\overline{g}}$ de $\overline{g}$ (puisqu'on a toujours $(\prod_{i<j}(\zeta_q^i - \zeta_q^j))^2 = (q^*)^q$). D'où un morphisme surjectif $G_{\overline{f}} \twoheadrightarrow G_{\overline{g}}$. On vérifie à nouveau sur leur construction que les plongements ι sont compatibles à ces morphismes surjectifs, i.e. que le diagramme suivant est commutatif

$$\begin{tikzcd} G_f \arrow[r, two heads] & G_g \\ G_{\overline{f}} \arrow[u, "\iota_f"] \arrow[r, two heads] & G_{\overline{g}} \arrow[u, "\iota_g"'] \end{tikzcd}.$$

(pour cela, on remarque que $A_f = \mathbb{Z}[\zeta_q]$ contient $A_g = \mathbb{Z}[\delta_q]$ où $\delta_q = \prod_{i<j}(\zeta_q^i - \zeta_q^j)$ et que si $\mathfrak{m}_f \in \mathrm{Max}(A_f)$ contient p alors $\mathfrak{m}_g := \mathfrak{m} \cap A_g \in \mathrm{Max}(A_g)$ et contient toujours p, de sorte que la surjection $G_f \longrightarrow G_g$ envoie $G_{f,\mathfrak{m}_f}$ dans $G_{g,\mathfrak{m}_g}$.)

Il s'ensuit que la surjection $(\mathbb{Z}/q\mathbb{Z})^\times \twoheadrightarrow \{\pm 1\}$ envoie $\overline{p}$ sur $\left(\frac{q^*}{p}\right)$. On en déduit la propriété remarquable suivante : q^* *est un carré dans* $\mathbb{F}_p^\times$ *si et seulement si* p *est un carré dans* $\mathbb{F}_q^\times$. Autrement dit $\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$. Un petit calcul utilisant la multiplicativité $\left(\frac{d_1 d_2}{p}\right) = \left(\frac{d_1}{p}\right)\left(\frac{d_2}{p}\right)$ et le fait (élémentaire) que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ montre alors la fameuse "loi de réciprocité quadratique"

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Remarque culturelle. (Le théorème de Chebotarev) – Comme remarqué plus haut, le théorème de spécialisation nous fournit, pour chaque premier p tel que $\overline{f} := f \bmod p$ est séparable, une *classe de conjugaison canonique* de plongements $G_{\overline{f}} \hookrightarrow G_f$. Les images du Frobenius $F \in G_{\overline{f}}$ dans G_f sont appelées *substitutions de Frobenius* et forment une classe de conjugaison C_p dans G_f. Le théorème de Chebotarev (conjecturé par Frobenius qui avait prouvé un résultat un peu plus faible) affirme que pour toute classe de conjugaison C de G_f, l'ensemble des premiers p tels que $C = C_p$ est infini, et a même pour densité "naturelle" $|C|/|G|$, ce qui signifie que la suite

$$\frac{|\{p \leqslant N, C = C_p\}|}{|\{p \leqslant N\}|} \underset{N\mapsto\infty}{\longrightarrow} \frac{|C|}{|G|}.$$

Dans le cas particulier de $f = \Phi_n$, on a $G_f \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ abélien, donc une classe de conjugaison est un singleton $C = \{\bar{a}\}$ pour un $a \in \mathbb{Z}$ premier à n. Alors, vu le calcul de $\iota(F)$ ci-dessus, on a $C = C_p$ si et seulement si $p \equiv a[n]$. On retrouve ainsi le théorème de densité de Dirichlet, qui affirme que l'ensemble des premiers congrus à a modulo n est infini, de densité $1/\varphi(n)$. En fait, les idées de Dirichlet sont utilisées dans la preuve de Chebotarev.

Dans le cas particulier $f = X^2 - d$, le théorème de Chebotarev nous dit que d est un carré dans $\mathbb{F}_p$ pour "la moitié" des nombres premiers p (ie pour p dans un sous-ensemble de densité 1/2).

2.10.3 *Un théorème de Hilbert.* Supposons ici $A = \mathbb{Q}[T]$. Tout élément $t \in \mathbb{Q}$ fournit une spécialisation de $f_T(X) \in A[X]$ en un polynôme $f_t(X) \in \mathbb{Q}[X]$, et le théorème précédent nous fournit un plongement $G_{f_t} \hookrightarrow G_{f_T}$, unique à conjugaison près. Hilbert a prouvé le théorème suivant, que nous citons pour la culture.

THÉORÈME. – *Supposons* f_T *irréductible dans* $\mathbb{Q}(T)[X]$. *Alors l'ensemble des* $t \in \mathbb{Q}$ *pour lesquels* $G_{f_t} \xrightarrow{\sim} G_{f_T}$ *est infini.*

Notons que pour un t comme dans le théorème, f_t est irréductible puisque l'action de G_{f_t} sur les racines est transitive comme celle de G_{f_T}. Notons aussi que le même énoncé est trivialement faux si on remplace $\mathbb{Q}$ par $\mathbb{C}$ ou $\mathbb{F}_p$. La motivation de Hilbert pour prouver ce théorème venait du problème de Galois inverse. On peut en déduire assez facilement que pour tout $n \in \mathbb{N}$, les groupes $\mathfrak{S}_n$ et $\mathfrak{A}_n$ sont des groupes de Galois sur $\mathbb{Q}$.

2.11 Polynômes symétriques

Considérons maintenant le corps $K = k(a_1, \cdots, a_n)$ des fractions rationnelles en n indéterminées, et le polynôme $f = X^{n-1} + a_1 X^{n-1} + \cdots + a_n \in K[X]$. Nous allons montrer que ce polynôme est séparable sur K et son groupe de Galois est $G_f = \mathfrak{S}_n$.

2.11.1 *Actions du groupe symétrique.* Faisons agit $\mathfrak{S}_n$ sur $\mathbb{N}^n$ par la formule

$$\sigma \cdot \nu = ((\sigma \cdot \nu)_1, \cdots, (\sigma \cdot \nu)_n) \text{ avec } (\sigma \cdot \nu)_i := \nu_{\sigma^{-1}(i)} \text{ si } \nu = (\nu_1, \cdots, \nu_n).$$

On a alors l'égalité $(\sigma\sigma') \cdot \nu = \sigma \cdot (\sigma' \cdot \nu)$ qui montre qu'on a ainsi défini une action à gauche de $\mathfrak{S}_n$ sur $\mathbb{N}^n$.

Par la propriété universelle de l'algèbre de monoïde $\mathbb{Z}[\mathbb{N}^n]$ cette action s'étend en une action de $\mathfrak{S}_n$ sur $\mathbb{Z}[\mathbb{N}^n]$ par automorphisme d'anneaux. Explicitement, on a

$$\sigma(f) = \sum_{\nu \in \mathbb{N}^n} a_\nu X^{\sigma \cdot \nu} = \sum_{\nu \in \mathbb{N}^n} a_{\sigma^{-1} . \nu} X^\nu \quad \text{pour } f = \sum_{\nu \in \mathbb{N}^n} a_\nu X^\nu.$$

Identifions $\mathbb{Z}[\mathbb{N}^n]$ à $\mathbb{Z}[X_1, \cdots, X_n]$ comme dans ..... On a donc $X^\nu = X_1^{\nu_1} \cdots X_n^{\nu_n}$ et

$$X^{\sigma \cdot \nu} = X_1^{\nu_{\sigma^{-1}(1)}} \cdots X_n^{\nu_{\sigma^{-1}(n)}} = X_{\sigma(1)}^{\nu_1} \cdots X_{\sigma(n)}^{\nu_n}.$$

Il s'ensuit que $\sigma(X_i) = X_{\sigma(i)}$ pour tout i. En d'autres termes, l'automorphisme $f \mapsto \sigma(f)$ de l'anneau $\mathbb{Z}[X_1, \cdots, X_n]$ est l'unique automorphisme tel que $\sigma(X_i) := X_{\sigma(i)}$.

2.11.2 *Polynômes symétriques élémentaires.* Pour $j = 1, \cdots, n$, on pose

$$\Sigma_j := \sum_{1 \leqslant i_1 < \cdots < i_j \leqslant n} X_{i_1} X_{i_2} \cdots X_{i_j} = \sum_{\substack{I \subset \{1, \cdots, n\} \\ |I| = j}} X_I \text{ avec } X_I := \prod_{i \in I} X_i.$$

Par exemple on a $\Sigma_1 = X_1 + X_2 + \cdots + X_n$ et $\Sigma_n = X_1 X_2 \cdots X_n$. Noter que $\mathfrak{S}_n$ agit sur les sous-ensembles de $\{1, \cdots, n\}$ par $(\sigma, I) \mapsto \sigma(I)$, et que cette action préserve évidemment le cardinal. Comme on a aussi $\sigma(X_I) = X_{\sigma(I)}$, il s'ensuit que $\sigma(\Sigma_n) = \Sigma_n$ pour toute permutation $\sigma \in \mathfrak{S}_n$. En d'autres termes, on a

$$\Sigma_1, \cdots, \Sigma_n \in \mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n},$$

on dit que ce sont des polynômes "symétriques". Ces polynômes encodent les relations entre racines et coefficients des polynômes.

Lemme. – *On a dans $\mathbb{Z}[X_1, \cdots, X_n][T]$ l'égalité*

$$(T - X_1)(T - X_2) \cdots (T - X_n) = T^n - \Sigma_1 T^{n-1} + \Sigma_2 T^{n-2} + \cdots + (-1)^n \Sigma_n$$

Démonstration. On laisse au lecteur le soin de faire une récurrence sur n. □

Si on se donne un n-uplet $\alpha_1, \cdots, \alpha_n$ d'éléments d'un anneau commutatif A, alors en “spécialisant” l'identité du lemme par le morphisme $\mathbb{Z}[X_1, \cdots, X_n][T] \longrightarrow A[X]$ qui envoie T sur X et α_i sur X_i, on obtient dans $A[X]$ l'égalité

$$(X - \alpha_1) \cdots (X - \alpha_n) = X^n - \Sigma_1(\alpha_1, \cdots, \alpha_n) X^{n-1} + \cdots + (-1)^n \Sigma_n(\alpha_1, \cdots, \alpha_n).$$

Le spectaculaire théorème suivant justifie la terminologie de “polynôme symétrique *élémentaire*”.

2.11.3 Théorème.– *Les Σ_i sont algébriquement indépendants dans $\mathbb{Z}[X_1, \cdots, X_n]$ et engendrent le sous-anneau $\mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n}$. En d'autres termes, l'unique morphisme d'anneaux $\mathbb{Z}[Y_1, \cdots, Y_n] \longrightarrow \mathbb{Z}[X_1, \cdots, X_n]$ qui envoie Y_i sur Σ_i est injectif et son image est $\mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n}$, ce que l'on écrit de manière un peu imprécise :*

$$\mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n} = \mathbb{Z}[\Sigma_1, \cdots, \Sigma_n].$$

Voici une preuve combinatoire et élémentaire de ce théorème. Nous en donnons une plus courte, et qui illustre plusieurs notions introduites dans ce cours, au paragraphe 2.12.4.

Démonstration. Pour $\nu \in \mathbb{N}^n$, posons $\Sigma^\nu := \Sigma_1^{\nu_1} \Sigma_2^{\nu_2} \cdots \Sigma_n^{\nu_n}$. Nous devons donc montrer que la famille $(\Sigma^\nu)_{\nu \in \mathbb{N}^n}$ est une $\mathbb{Z}$-base de $\mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n}$.

Pour cela, nous allons d'abord exhiber une $\mathbb{Z}$-base agréable de $\mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n}$, puis nous exprimerons les Σ^ν dans cette base agréable. Soit $f = \sum_{\nu \in \mathbb{N}^n} a_\nu X^\nu$ invariant sous $\mathfrak{S}_n$. Alors $a_\nu = a_{\sigma \cdot \nu}$ pour tout $\sigma \in \mathfrak{S}_n$, et on peut donc écrire, de manière unique,

$$f = \sum_{\overline{\nu} \in \mathbb{N}^n / \mathfrak{S}_n} a_{\overline{\nu}} S^{\overline{\nu}}, \quad \text{où} \quad S^{\overline{\nu}} = \sum_{\nu \in \overline{\nu}} X^\nu.$$

La famille $(S^{\overline{\nu}})_{\overline{\nu} \in \mathbb{N}^n / \mathfrak{S}_n}$ est donc une $\mathbb{Z}$-base de $\mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n}$. Néanmoins, la paramétrisation de cette base par l'ensemble quotient $\mathbb{N}^n / \mathfrak{S}_n$ n'est pas pratique pour y exprimer Σ^ν.

Définition. – *On dit que $\nu \in \mathbb{N}^n$ est* dominant *si $\nu_1 \geqslant \nu_2 \geqslant \cdots \geqslant \nu_n$. On note $\Lambda \subset \mathbb{N}^n$ l'ensemble des n-uplets dominants.*

Il est clair que toute $\mathfrak{S}_n$-orbite $\overline{\nu}$ contient exactement 1 n-uplet dominant. L'ensemble Λ est donc un ensemble de représentants des $\mathfrak{S}_n$-orbites dans $\mathbb{N}^n$. Pour $\lambda \in \Lambda$, on notera simplement

$$S^\lambda := S^{\overline{\lambda}} = \sum_{\nu \in \mathfrak{S}_n \cdot \lambda} X^\nu.$$

Exemple. – Pour $j = 1, \cdots, n$ notons $\mu^j = (1, \cdots, 1, 0, \cdots, 0) \in \Lambda$ avec j termes égaux à 1. Alors $\mu^j \in \Lambda$ et $S^{\mu^j} = \Sigma_j$.

Si $\lambda' \in \Lambda$, on peut écrire

$$(*) \qquad S^\lambda S^{\lambda'} = \sum_{\mu \in \Lambda} c_{\lambda, \lambda'; \mu} S^\mu$$

pour des coefficients $c_{\lambda,\lambda';\mu} \in \mathbb{Z}$ uniquement déterminés. Afin d'étudier ces coefficients, il est utile de remarquer que Λ est stable par addition, et de munir $\mathbb{N}^n$ de l'ordre suivant :

DÉFINITION. – *Pour $\nu \in \mathbb{N}^n$, posons $|\nu| := \sum_{i=1}^n \nu_i$ et $\tilde{\nu} := (|\nu|, \nu_1, \cdots, \nu_n) \in \mathbb{N}^{n+1}$. On munit alors $\mathbb{N}^n$ de la relation d'ordre*

$$\nu \preccurlyeq \nu' \Leftrightarrow \tilde{\nu} \leqslant \tilde{\nu}'$$

où $\leqslant$ désigne l'ordre lexicographique sur $\mathbb{N}^{n+1}$.

L'ordre $\preccurlyeq$ est total et compatible à l'addition : $\nu \preccurlyeq \nu'$ et $\mu \preccurlyeq \mu' \Rightarrow \nu + \mu \preccurlyeq \nu' + \mu'$.

LEMME. – *Dans l'expansion $(*)$ on a $c_{\lambda,\lambda';\mu} \neq 0 \Rightarrow \mu \preccurlyeq \lambda + \lambda'$ et $c_{\lambda,\lambda',\lambda+\lambda'} = 1$. En d'autres termes, on a*

$$S^\lambda S^{\lambda'} \in S^{\lambda+\lambda'} + \sum_{\mu \prec \lambda+\lambda'} \mathbb{Z}.S^\mu$$

Démonstration. Pour $\nu \in \mathbb{N}^n$, notons $A_{\prec\nu} := \sum_{\nu' \prec \nu} \mathbb{Z}X^{\nu'}$. Puisque $\preccurlyeq$ est compatible à l'addition, on a $A_{\prec\nu}A_{\preccurlyeq\nu'} \subset A_{\prec\nu+\nu'}$. De plus, si $\lambda \in \Lambda$, on a $\sigma\cdot\lambda \prec \lambda$ pour tout $\sigma \in \mathfrak{S}_n \backslash \{\mathrm{id}\}$. On en déduit que $S^\lambda \in X^\lambda + A_{\prec\lambda}$ et

$$S^\lambda S^{\lambda'} \in X^{\lambda+\lambda'} + A_{\prec\lambda+\lambda'}.$$

Il s'ensuit que

$$S^\lambda S^{\lambda'} = S^{\lambda+\lambda'} + P, \quad \text{avec} \quad P \in (A_{\prec\lambda+\lambda'})^{\mathfrak{S}_n}.$$

Écrivons $P = \sum_{\mu\in\Lambda} c_\mu S^\mu$. Comme c_μ est aussi le coefficient de X^μ dans le développement de P dans la base des X^ν, on voit que $c_\mu \neq 0 \Rightarrow \mu \prec \lambda + \lambda'$ comme voulu. □

Écrivons maintenant les Σ^ν dans la base des S^λ. On a

$$\Sigma^\nu = \Sigma_1^{\nu_1} \cdots \Sigma_n^{\nu_n} = (S^{\mu^1})^{\nu_1} \cdots (S^{\mu^n})^{\nu_n}.$$

Posons alors

$$\lambda_\nu := \nu_1\mu^1 + \cdots + \nu_n\mu^n \in \Lambda.$$

Le lemme nous dit que

$$\Sigma^\nu \in S^{\lambda_\nu} + \sum_{\lambda \prec \lambda_\nu} \mathbb{Z}.S^\lambda.$$

Or l'application

$$\mathbb{N}^n \longrightarrow \Lambda, \ \ \nu \mapsto \lambda_\nu$$

est *bijective*, d'inverse $\lambda \mapsto (\lambda_1 - \lambda_2, \cdots, \lambda_{n-1} - \lambda_n, \lambda_n)$. Munissons donc $\mathbb{N}^n$ d'une nouvelle relation d'ordre (total et compatible à l'addition) :

$$\nu \trianglelefteq \nu' \Leftrightarrow \lambda_\nu \preccurlyeq \lambda_{\nu'},$$

et posons $S_\nu := S^{\lambda_\nu}$. Alors la famille $(S_\nu)_{\nu\in\mathbb{N}^n}$ est une $\mathbb{Z}$-base de $\mathbb{Z}[X_1,\cdots,X_n]^{\mathfrak{S}_n}$, et on a

$$\forall \nu \in \mathbb{N}^n, \quad \Sigma^\nu \in S_\nu + \sum_{\nu' \lhd \nu} \mathbb{Z}.S_{\nu'}.$$

On en déduit que la famille $(\Sigma^\nu)_{\nu\in\mathbb{N}^n}$ est libre sur $\mathbb{Z}$; en effet, soit $\sum_\nu a_\nu \Sigma^\nu = 0$ une relation de dépendance linéaire, si $\{\nu, a_\nu \neq 0\}$ est non vide il possède un plus grand élement ν_0, mais alors on obtient la relation $0 \in a_{\nu_0} S_{\nu_0} + \sum_{\nu \lhd \nu_0} S_\nu$ qui contredit la liberté des S_ν.

On en déduit aussi que la famille $(\Sigma^\nu)_{\nu\in\mathbb{N}^n}$ est génératrice sur $\mathbb{Z}$. Plus précisément, on montre que

$$\forall \nu \in \mathbb{N}^n, \quad S_\nu \in \Sigma^\nu + \sum_{\nu' \lhd \nu} \mathbb{Z}.\Sigma^{\nu'}$$

par récurrence sur l'entier $n(\nu) = |\{\nu' \lhd \nu\}|$ par exemple.

□

2.11.4 *Application : discriminant d'un polynôme.* D'après le théorème, il existe un unique polynôme $\Delta \in \mathbb{Z}[\Sigma_1,\cdots,\Sigma_n]$ tel que

$$\prod_{i<j}(X_i - X_j)^2 = (-1)^{n(n-1)/2}\prod_{i\neq j}(X_i - X_j) = \Delta(\Sigma_1,\cdots,\Sigma_n).$$

En effet, le terme de gauche est manifestement un polynôme symétrique en les X_i.

DÉFINITION. – *Soit A un anneau et $f = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in A[X]$ un polynôme unitaire. On définit le* discriminant *de f par*

$$\operatorname{disc}(f) := \Delta\left(-a_1,\cdots,(-1)^n a_n\right) \in A.$$

Exemple. – Soit $A = \mathbb{Z}[X_1,\cdots,X_n]$ et f_{univ} le polynôme scindé de degré n “universel”

$$f_{\mathrm{univ}} := (T - X_1)(T - X_2)\cdots(T - X_n) \in \mathbb{Z}[X_1,\cdots,X_n][T].$$

Alors $\operatorname{disc}(f_{\mathrm{univ}}) = \Delta$, puisque $f_{\mathrm{univ}} = T^n - \Sigma_1 T^{n-1} + \cdots + (-1)^n\Sigma_n$. On remarque aussi (calcul) que

$$\operatorname{disc}(f_{\mathrm{univ}}) = (-1)^{n(n-1)/2}\prod_{i=1}^n f'(X_i).$$

PROPOSITION. – *Soit k un corps et $f \in k[X]$ unitaire. Pour toute extension K pour laquelle f se scinde $f = (X - \alpha_1)\cdots(X - \alpha_n)$ dans $K[X]$, on a*

$$\operatorname{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2}\prod_{i=1}^n f'(\alpha_i).$$

En particulier, f est séparable si et seulement si $\operatorname{disc}(f) \neq 0$.

Démonstration. Découle de l'exemple universel par le morphisme $\mathbb{Z}[X_1, \cdots, X_n][T] \longrightarrow K[X]$ qui envoie T sur X et X_i sur α_i. $\square$

Exercice. – Montrer que $\mathrm{disc}(X^n + aX + b) = (-1)^{n(n-1)/2}((1-n)^{n-1}a^n + n^n b^{n-1})$.

Voici un autre exemple d'utilisation du discriminant :

PROPOSITION. – *Soit $f \in k[X]$ séparable et G_f son groupe de Galois, vu comme un sous-groupe du groupe de permutation $\mathfrak{S}_n$ des racines de f dans un corps de décomposition K_f de f. Alors, si* $\mathrm{car}(k) \neq 2$ *on a* $G_f \subset \mathfrak{A}_n \Leftrightarrow \mathrm{disc}(f) \in (k^\times)^2$.

Démonstration. Soit $\alpha_1, \cdots, \alpha_n$ les racines de f dans K_f. Notons $\tau \mapsto \sigma_\tau$ l'injection de G_f dans $\mathfrak{S}_n$ associée à cette numérotation des racines. On a donc $\tau(\alpha_i) = \alpha_{\sigma_\tau(i)}$ pour tout i.

Posons $D := \prod_{i<j}(\alpha_i - \alpha_j) \in K_f$. Les deux racines carrées de $\mathrm{disc}(f)$ dans K_f sont D et $-D$. Ainsi $\mathrm{disc}(f) \in k^2 \Leftrightarrow D \in k$. Puisque $k = K_f^{G_f}$, étudions l'action de G_f sur D. Pour tout $\tau \in G_f$ on a, en notant ε la signature $\mathfrak{S}_n \longrightarrow \{\pm 1\}$,

$$\tau(D) = \prod_{i<j}(\alpha_{\sigma_\tau(i)} - \alpha_{\sigma_\tau(j)}) = \varepsilon(\sigma_\tau)\prod_{i<j}(\alpha_i - \alpha_j) = \varepsilon(\sigma_\tau)D.$$

Si $\mathrm{car}(k) \neq 2$, il s'ensuit que $D \in K_f^{G_f} = k \Leftrightarrow G_f \subset \mathfrak{A}_n$. $\square$

Remarque. – Si $\mathrm{disc}(f) \notin k^2$, l'extension intermédiaire $k \subset k(\sqrt{\mathrm{disc}(f)}) \subset K_f$ est quadratique sur k et $\mathrm{Gal}(K_f/k(\sqrt{\mathrm{disc}(f)})) = G_f \cap \mathfrak{A}_n$.

Exemple. – Considérons $X^5 + 20X - 16$. On vérifie que f est irréductible dans $\mathbb{F}_3[X]$ et possède une factorisation de type $(1,1,3)$ dans $\mathbb{F}_7[X]$. Le groupe G_f contient donc un 5-cycle et un 3-cycle. Par ailleurs, f possède 4 racines non réelles, donc contient un produit de transpositions disjointes, d'ordre 2. Il s'ensuit que $30 | |G_f|$. Enfin, $\mathrm{disc}(f) = (2^8 5^3)^2$ est un carré, donc $G_f \subset \mathfrak{A}_5$. Or $\mathfrak{A}_5$ ne contient pas de sous-groupe d'indice 2 (qui serait distingué de quotient abélien), donc $G_f \simeq \mathfrak{A}_5$.

2.11.5 *Application : résolvantes.* Le discrimant Δ peut être vu comme le $\mathfrak{S}_n$-symétrisé du polynôme $\mathfrak{A}_n$-invariant $\psi = \prod_{i<j}(X_i - X_j)$ et le critère ci-dessus nous dit que $G_f \subset \mathfrak{A}_n$ si et seulement si le polynôme $(T - \psi(\alpha_1, \cdots, \alpha_n)(T + \psi(\alpha_1, \cdots, \alpha_n)) = T^2 - \Delta(f)$ a une racine simple dans k.

Plus généralement, si $\psi \in k[X_1, \cdots, X_n]$ est H-invariant pour un sous-groupe $H < \mathfrak{S}_n$, on pose

$$R_\psi(T) := \prod_{\sigma \in \mathfrak{S}_n/H}(T - \sigma.\psi) \in k[X_1, \cdots, X_n]^{\mathfrak{S}_n}[T] = k[\Sigma_1, \cdots, \Sigma_n][T],$$

que l'on peut spécialiser à un polynôme $f = X^n + a_1X^{n-1} + \cdots + a_n \in k[X]$ en

$$R_{\psi,f}(T) = R_\psi(-a_1, \cdots, (-1)^n a_n)(T) \in k[T].$$

Ce polynôme est de degré $|\mathfrak{S}_n/H|$, et on a le critère suivant :

Proposition. – *Si $R_{\psi,f}(T)$ possède une racine simple dans k, alors G_f est contenu dans un conjugué de H dans $\mathfrak{S}_n$.*

Démonstration. Comme plus haut, soient $\alpha_1, \cdots, \alpha_n$ les racines de f dans K_f. Notons $\tau \mapsto \sigma_\tau$ l'injection de G_f dans $\mathfrak{S}_n$ associée à cette numérotation des racines.

Posons $\overline{\psi} := \psi(\alpha_1, \cdots, \alpha_n) \in K_f$, et plus généralement $\overline{\sigma\psi} := \psi(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$ pour $\sigma \in \mathfrak{S}_n$. On a donc $\overline{\sigma\sigma'\psi} = \overline{\sigma\psi}$ si $\sigma' \in H$ et on a $\overline{\sigma_\tau\sigma\psi} = \tau(\overline{\sigma\psi})$ pour $\tau \in G_f$.

Les racines de $R_{\psi,f}$ sont les $\overline{\sigma\psi}$ pour σ décrivant $\mathfrak{S}_n/H$ (ou plutôt un ensemble de représentants de $\mathfrak{S}_n/H$). Supposons que $\overline{\sigma\psi}$ est racine de $R_{\psi,f}$ dans k. Alors $\overline{\sigma_\tau\sigma\psi} = \tau(\overline{\sigma\psi}) = \overline{\sigma\psi}$ pour tout $\tau \in G_f$. Si de plus, $\overline{\sigma\psi}$ est racine simple, alors $\sigma_\tau\sigma H = \sigma H$ et $\sigma_\tau \in \sigma H \sigma^{-1}$. L'action de G_f se fait donc à travers $\sigma H \sigma^{-1}$. □

Encore plus généralement, soient deux sous-groupes $H \subset G \subset \mathfrak{S}_n$ et supposons que G_f agisse à travers G sur les racines (pour un ordre préalablement choisi). On peut alors simplement G-symétriser un polynôme H-invariant ψ en posant

$$R^G_{\psi,f}(T) = \prod_{\sigma \in G/H} (T - \psi(\alpha_{\sigma(1)}, \cdots, \alpha_{\sigma(n)}) \in K_f[X].$$

Ce polynôme de degré $[G : H]$ est alors G_f-invariant, donc dans $k[X]$. Comme ci-dessus, s'il admet une racine simple dans k alors l'action de G_f se fait à travers un conjugué de H. Sinon, si K désigne le sous-corps de K_f engendré par une racine simple de $R^G_{\psi,f}$, alors $\mathrm{Gal}(K_f/K)$ agit à travers un conjugué de H.

Remarque. – Ce principe de "calcul de G_f" est un avatar du "principe de Lagrange" pour résoudre le polynôme f, *i.e.* contruire K_f. Supposons en effet H distingué dans G et $R^G_{\psi,f}$ séparable. Si on sait construire le corps de décomposition K_1 de $R^G_{\psi,f}$ (qui est de degré $\leqslant \deg(f)$), on sait que le corps K_f de décomposition de f sur K_1 sera de groupe contenu dans H. Le principe de Lagrange est donc de bien choisir ψ pour être capable de résoudre la "résolvante" $R^G_{\psi,f}$, puis inductivement construire ainsi K_f (en se ramenant à construire des extensions successives de groupes de Galois cycliques). Bien-sûr ce principe ne peut fonctionner que si G est résoluble.

Exemple : polynômes cubiques sur $\mathbb{Q}$. Lagrange considérait la résolvante associée à $\psi = (X_1 + jX_2 + j^2X_3)^3$ qui est invariant par le groupe H engendré par le cycle $(1, 2, 3)$ (il faut donc adjoindre j à $\mathbb{Q}$, et on peut rapprocher cela du discriminant en degré 2, qui est associé à $(X_1 - X_2)^2$). Le polynôme

$$R_\psi(T) = (T - (X_1 + jX_2 + j^2X_3)^3)(T - (X_1 + j^2X_2 + jX_3)^3) \in \mathbb{Z}[X_1, X_2, X_3][T]$$

est de degré 2 en T et la preuve du théorème 2.11.3 suggère un procédé inductif de calcul de ses coefficients en tant qu'éléments de $\mathbb{Z}[\Sigma_1, \Sigma_2, \Sigma_3]$. Si l'on spécialise à un polynôme $f = X^3 + aX + b$ sans terme en X^2, les formules se simplifient un peu et on peut montrer que $R_{\psi,f} = T^2 + 27bT - 27a^3$. On sait résoudre un tel trinôme. Si $\overline{\psi}_1$, $\overline{\psi}_2$ en sont les racines, on a donc (pour une numérotation convenable des racines) $\overline{\psi}_1 = (\alpha_1 + j\alpha_2 + j^2\alpha_3)^3$ et

$\overline{\psi}_2 = (\alpha_1 + j^2\alpha_2 + j\alpha_3)^3$. Après extraction de racine cubique, et tenant compte de l'égalité $\alpha_1 + \alpha_2 + \alpha_3 = 0$, on trouve donc les α_i en résolvant un système linéaire 3×3.

Exemple : polynômes de degré 4 *sur* $\mathbb{Q}$. Lagrange utilisait la résolvante associée au polynôme $\psi = (X_1 + X_2)(X_3 + X_4)$ qui est invariant par un sous-groupe H d'indice 3 de $\mathfrak{S}_4$. On peut montrer par exemple que si $f = X^4 + aX^2 + bX + c$ alors $R_{\psi,f} = T^3 - 2aT^2 + (a^2 - 4c)T + b^2$. Par l'exemple précédent, on sait construire les trois racines $\overline{\psi}_1, \overline{\psi}_2, \overline{\psi}_3$ de $R_{\psi,f}$. Pour une bonne numérotation de ces racines, on a $\overline{\psi}_i = (\alpha_1 + \alpha_{1+i})(\alpha_? + \alpha_!)$ pour chaque $i = 1, 2, 3$ et où $\{1, 2, 3, 4\} = \{1, 1 + i, ?, !\}$. Mais alors, en utilisant $\sum \alpha_i = 0$, on obtient que $\alpha_1 + \alpha_{1+i}$ est une racine carrée de $-\overline{\psi}_i$ pour $i = 1, 2, 3$. Puis après extraction de ces racines, on n'a plus qu'à résoudre un système linéaire pour obtenir les α_i.

2.11.6 *Application : groupe de Galois du polynôme "général".* Commençons par un corollaire du théorème 2.11.3 concernant les fractions rationnelles symétriques. Remarquons au passage que l'action de $\mathfrak{S}_n$ sur $k[X_1, \cdots, X_n]$ se prolonge uniquement à $k(X_1, \cdots, X_n)$.

Corollaire. – *On a* $k(X_1, \cdots, X_n)^{\mathfrak{S}_n} = k(\Sigma_1, \cdots, \Sigma_n)$.

Démonstration. On a une inclusion claire, à savoir $\supset$. Pour l'autre inclusion, soit $\phi \in k(X_1, \cdots, X_n)^{\mathfrak{S}_n}$. Puisque $k[X_1, \cdots, X_n]$ est factoriel, on peut écrire ϕ de manière unique sous la forme $\phi = \frac{f}{g}$ avec $(f, g) = 1$ et f, g unitaires (choisir un ordre total sur $\mathbb{N}^n$ pour définir "unitaire"). On a alors, pour tout $\sigma \in \mathfrak{S}_n$, $\phi = \sigma(\phi) = \frac{\sigma(f)}{\sigma(g)}$ et aussi $(\sigma(f), \sigma(g)) = 1$ et $\sigma(f), \sigma(g)$ unitaires. Il s'ensuit que $f = \sigma(f)$ et $g = \sigma(g)$. Donc $f, g \in k[\Sigma_1, \cdots, \Sigma_n]$ et finalement $\phi \in k(\Sigma_1, \cdots, \Sigma_n)$. □

Changeons maintenant de point de vue. Soit k un corps, et $K := k(a_1, \cdots, a_n)$ le corps des fractions rationnelles en les n indéterminées $a_1, \cdots, a_n$. On s'intéresse au polynôme "général" $f = X^n + a_1X^{n-1} + \cdots + a_n \in K[X]$, dont on veut déterminer un corps de décomposition et le groupe de Galois G_f. Pour cela, considérons le corps $L := k(\alpha_1, \cdots, \alpha_n)$ des fractions rationnelles à n-indéterminées $\alpha_1, \cdots, \alpha_n$. Le théorème 2.11.3 nous dit que les éléments $\Sigma_i(\alpha_1, \cdots, \alpha_n) \in L$ sont algébriquement indépendants sur k. Il existe donc un unique plongement

$$K \hookrightarrow L,\ a_i \mapsto (-1)^i\Sigma_i(\alpha_1, \cdots, \alpha_n).$$

Théorème. – *Le polynôme f est séparable et irréductible dans $K[X]$. Le corps L est un corps de décomposition de f sur K dans lequel les α_i sont les racines de f. L'action du groupe de Galois G_f sur les α_i identifie G_f à $\mathfrak{S}_n$.*

Démonstration. Via le morphisme d'anneaux $\mathbb{Z}[X_1, \cdots, X_n][T] \longrightarrow L[X]$ qui envoie X_i sur α_i et T sur X, la factorisation du lemme 2.11.2 implique la factorisation $(X - \alpha_1) \cdots (X - \alpha_n) = X^n + a_1X^{n-1} + \cdots + a_n$ dans $L[X]$. Il s'ensuit que les α_i sont les racines de f dans L, donc f est séparable et L est un corps de décomposition de f. L'action de $\mathrm{Gal}(L/K)$ sur les α_i nous fournit un plongement $\mathrm{Gal}(L/K) \hookrightarrow \mathfrak{S}_n$. Mais le corollaire ci-dessus nous dit que $K = L^{\mathfrak{S}_n}$, et la proposition 2.7.7 implique que $\mathrm{Gal}(L/K) = \mathfrak{S}_n$. En particulier, $\mathrm{Gal}(L/K)$ agit transitivement sur les racines de f, donc f est irréductible, en vertu du lemme 2.8.1. □

Remarque. – On peut se demander quelle implication peut avoir un tel résultat sur les polynômes qui nous intéressent vraiment, à savoir ceux où les a_i sont des éléments de k. Il se trouve que la réponse dépend fortement de k. Par exemple si $k = \mathbb{C}$, tout polynôme f obtenu par spécialisation des a_i en des éléments de $\mathbb{C}$ est scindé, donc son groupe de Galois est trivial ! Si $k = \mathbb{R}$ et $n > 2$, une spécialisation de f n'est jamais irréductible et son groupe de Galois est trivial ou égal à $\mathbb{Z}/2\mathbb{Z}$. Si $k = \mathbb{F}_p$, une spécialisation de f peut être irréductible, mais son groupe de Galois est toujours abélien. Mais pour $k = \mathbb{Q}$, un résultat de Hilbert affirme que pour une infinité de spécialisations de f, le polynôme spécialisé est irréductible et son groupe de Galois est $\mathfrak{S}_n$!

2.12 Extensions entières

2.12.1 *Polynôme caractéristique.* Soit A un anneau (commutatif unitaire) et M un A-module libre de type fini. Si l'on choisit une base $e = (e_i)_{i=1,\cdots,n}$ de M, on a un isomorphisme de A-algèbres $\mathrm{End}_A(M) \simeq \mathcal{M}_n(A)$ qui à un endomorphisme u associe sa matrice $M_e(u)$. Si e' est une autre base, et $P \in \mathrm{GL}_n(A)$ la matrice de passage de e dans e', alors $M_{e'}(u) = P^{-1}M_e(u)P$. Ceci montre que le déterminant et la trace de la matrice $M_e(u)$ ne dépendent que de u et pas de e. On les note

$$\det(u) \text{ et } \mathrm{tr}(u) \in A.$$

Remarquons que $\det(u)$ s'interprète aussi comme le scalaire donnant l'action de $\wedge^n u$ sur $\wedge^n M \simeq A$; en particulier on a $\det(u) = \mathrm{tr}(\wedge^n u)$.

On définit maintenant le polynôme caractéristique de l'endomorphisme u

$$\chi_u(T) = \det(T\,\mathrm{id}_M - u) \in A[T]$$

comme le déterminant de l'endomorphisme $T \otimes \mathrm{id}_M - 1 \otimes u$ du $A[T]$-module libre $A[T] \otimes_A M$. On retrouve bien la définition classique lorsque A est un corps. Le théorème suivant est classique lorsque A est un corps algébriquement clos.

Théorème. (Cayley-Hamilton) – *Soit M un A-module libre de rang fini et $u \in \mathrm{End}_A(M)$ un endomorphisme de M, Alors on a l'égalité $\chi_u(u) = 0$ dans l'anneau $\mathrm{End}_A(M)$.*

Démonstration. Considérons le cas particulier où $A = A_n := \mathbb{Z}[X_{ij}]_{1 \leqslant i,j \leqslant n}$, $M = A^n$ et u_n est donné dans la base canonique par la matrice $(X_{ij})_{1 \leqslant i,j \leqslant n}$. Puisque A_n est intègre, considérons son corps des fractions K_n et une clôture algébrique $\overline{K}_n$ de celui-ci. Le polynôme χ_{u_n} est aussi le polynôme caractéristique de la matrice u_n vue dans $M_n(K_n)$ ou dans $M_n(\overline{K}_n)$. Ce polynôme est scindé dans $\overline{K}_n[T]$ et $\overline{K}_n^n$ est somme directe des sous-espaces caractéristiques de u_n. En calculant dans une base subordonnée à cette décomposition, on constate que $\chi_{u_n}(u_n) = 0$ dans $M_n(\overline{K}_n)$ et puisque $M_n(A_n) \longrightarrow M_n(\overline{K}_n)$ est injective, la même égalité vaut dans $M_n(A_n)$.

Revenons à l'énoncé général du théorème. Choisissons une base de M et identifions M à A^n. Notons $(a_{ij})_{i,j}$ la matrice de u dans cette base, et considérons le morphisme d'anneaux "de spécialisation"

$$\varepsilon : \ A_n = \mathbb{Z}[X_{ij}]_{1 \leqslant i,j \leqslant n} \longrightarrow A, \quad X_{ij} \mapsto a_{ij}.$$

Ce morphisme induit aussi des morphismes d'anneaux $A_n[T] \longrightarrow A[T]$ et $M_n(A_n) \longrightarrow M_n(A)$ encore notés ε. Il est clair que $\varepsilon(\chi_{u_n}(T)) = \chi_u(T)$ et par là que $\varepsilon(\chi_{u_n}(u_n)) = \chi_u(u)$. On en déduit $\chi_u(u) = 0$. $\square$

Remarque. – On a l'égalité $\chi_u(T) = \sum_{i=1}^n (-1)^i \operatorname{tr}(\wedge^i u) T^{n-i}$. Pour le vérifier, on peut utiliser le même argument que ci-dessus : on traite le cas "universel" en se ramenant à un corps algébriquement clos où la formule se vérifie facilement via les relations entre coefficients et racines d'un polynôme. Puis on spécialise le cas universel au cas souhaité : avec $\varepsilon : A_n \longrightarrow A$ comme ci-dessus, on a $u = \mathrm{id} \otimes u_n \in \mathrm{End}_A(A \otimes_{A_n,\varepsilon} A_n^n) = \mathrm{End}_A(A^n)$ et, par fonctorialité, on a aussi $\wedge^i u = \mathrm{id} \otimes \wedge^i u_n$ dans $\mathrm{End}_A(A \otimes_{A_n,\varepsilon} \wedge^i A_n^n) = \mathrm{End}_A(\wedge^i A^n)$, de sorte que $\operatorname{tr}(\wedge^i u) = \varepsilon(\operatorname{tr}(\wedge^i u_n))$.

Corollaire. – *Soit M un A-module de type fini et $u \in \mathrm{End}_A(M)$ un endomorphisme. Alors il existe un polynôme monique $f \in A[T]$ tel que $f(u) = 0$ dans $\mathrm{End}_A(M)$.*

Démonstration. Choisissons un épimorphisme $\pi : A^n \twoheadrightarrow M$ pour n convenable. Soit $(e_1, \cdots, e_n)$ la base canonique de A^n. Pour chaque $i = 1, \cdots, n$, choisissons un élément $f_i \in A^n$ tel que $\pi(f_i) = u(\pi(e_i))$. Cela définit un endomorphisme $\widetilde{u}$ de A^n donné par $\widetilde{u}(e_i) = f_i$. On a donc par construction $\pi \circ \widetilde{u} = u \circ \pi$, et par itération $\pi \circ \widetilde{u}^k = u^k \circ \pi$, et finalement $\pi \circ \chi_{\widetilde{u}}(\widetilde{u}) = \chi_{\widetilde{u}}(u) \circ \pi$. D'après le théorème précédent on a donc $\chi_{\widetilde{u}}(u) \circ \pi = 0$. Or π est surjective, donc $\chi_{\widetilde{u}}(u) = 0$. $\square$

2.12.2 *Eléments entiers d'une A-algèbre.* On "rappelle" qu'un élément b d'une A-algèbre B est dit *entier* sur A s'il existe $f \in A[X]$ unitaire tel que $f(b) = 0$.

Proposition. – *Soit B une A-algèbre. Pour $b \in B$, les propriétés suivantes sont équivalentes :*

i) b est entier sur A

ii) l'anneau $A[b]$ engendré par b est un module de type fini sur A.

iii) Il existe un $A[b]$-module fidèle qui est de type fini sur A.

Rappelons qu'un A-module M est "fidèle" si l'application $A \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$ est injective.

Démonstration. i) $\Rightarrow$ ii). Soit $f = X^n + a_1 X^{n-1} + \cdots + a_n$ comme dans i). On a donc $b^n \in A + Ab + \cdots + Ab^{n-1}$ et par récurrence $b^m \in A + Ab + \cdots + Ab^{n-1}$ pour tout $m \geqslant n$. Donc $A[b]$ est engendré par $1, b, \cdots, b^{n-1}$ comme A-module.

ii) $\Rightarrow$ iii). Il suffit de prendre le $A[b]$-module $A[b]$!

iii) $\Rightarrow$ i) découle du corollaire précédent. $\square$

2.12.3 *Clôture intégrale, normalisation.*

Corollaire. – *Soit B une A-algèbre. L'ensemble $\{b \in B, b$ entier sur $A\}$ est une sous-A-algèbre de B. On l'appelle* clôture intégrale de A dans B.

Démonstration. Supposons b et b' entiers sur A. Alors b' est *a fortiori* entier sur $A[b]$ donc $A[b][b']$ est un $A[b]$-module de type fini, et donc aussi un A-module de type fini. C'est aussi un $A[b+b']$-module fidèle (puisqu'il contient $A[b+b']$) donc $b+b'$ est entier par la caractérisation iii) de la proposition précédente. De même, bb' est entier. □

Remarque. – Une A-algèbre B d'anneaux est dite *entière* si tout élément de B est entier sur A. La proposition montre que si B est entière sur A et si C est une B-algèbre entière, alors C est aussi une A-algèbre entière.

Exemple. – Soit K une extension finie de $\mathbb{Q}$ (on dit que K est un "corps de nombres"), on note $\mathcal{O}_K$ la clôture intégrale de $\mathbb{Z}$ dans K et on l'appelle "anneau des entiers de K".

Définition. – *Si A est* intègre*, la clôture intégrale de A dans* Frac(A) *est appelée* normalisation *de A. On dit alors que A est* normal *(ou encore* intégralement clos*) s'il est égal à sa propre normalisation.*

Exemples. – i) $\mathcal{O}_K$ est normal car $K = \text{Frac}(\mathcal{O}_K)$. En effet, si $x \in K$, soit $a_i \in \mathbb{Q}$ tels que $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Choisissons $b \in \mathbb{Z}$ tel que $ba_i \in \mathbb{Z}$ pour tout i. Alors $(xb)^n + (a_1b)(xb)^{n-1} + \cdots + (a_nb^n) = 0$, ce qui montre que $xb \in \mathcal{O}_K$ et donc que $x \in \text{Frac}(\mathcal{O}_K)$

ii) $\mathbb{Z}[\sqrt{-3}]$ n'est pas intégralement clos car il ne contient pas l'élément $j = \frac{1+\sqrt{-3}}{2}$ de $\mathbb{Q}(\sqrt{-3})$ qui est pourtant entier puisqu'il annule X^3-1. En d'autres termes, $\mathbb{Z}[\sqrt{-3}] \subsetneq \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$.

Exemple. – A factoriel ⇒ A normal. En effet, soit $x \in \text{Frac}A$ vérifiant l'équation entière $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Puisque A est factoriel on peut écrire $x = a/b$ avec a et b sans facteur commun. Alors $a^n + a_1a^{n-1}b + \cdots a_nb^n = 0$, donc $a^n \in (b)$, i.e. b divise a^n, ce qui implique que b est inversible dans A.

Exercice. – Montrer que $\mathbb{Z}[X_1, \cdots, X_n]$ est la clôture intégrale de $\mathbb{Z}[\Sigma_1, \cdots, \Sigma_n]$ dans $\mathbb{Q}(X_1, \cdots, X_n)$.

Proposition. – *Si A est normal et L est une extension finie de $K :=$* Frac(A)*, alors $x \in L$ est entier si et seulement si son polynôme minimal $f_x \in K[X]$ est dans $A[X]$.*

Démonstration. Seul le sens ⇒ demande preuve. Supposons donc x entier et soit $f \in A[X]$ tq $f(x) = 0$. Alors $f_x | f$ dans $K[X]$ donc toute racine α de f_x dans une clôture algébrique $\overline{K}$ de K est une racine de f donc est entière sur A. Les coefficients de f_x sont donc aussi entiers sur A, et puisqu'ils sont dans K et que A est normal, ils sont dans A. □

Exemple. – Soit K une extension quadratique de $\mathbb{Q}$ (ie de degré 2). Alors il existe un unique entier $d \in \mathbb{Z}$ sans facteur carré tel que $K = \mathbb{Q}(\sqrt{d})$ (exercice). D'après la proposition précédente, un élément $\alpha = a + b\sqrt{d}$ de K est entier si et seulement si son polynôme minimal f_α est dans $\mathbb{Z}[X]$. Si $b \neq 0$, l'unique conjugué de α est $a - b\sqrt{d}$ et on a donc $f_\alpha = X^2 - 2aX + (a^2 - db^2)$. Ceci montre que

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \left\{a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d}),\ 2a \in \mathbb{Z},\ \text{et } a^2 - db^2 \in \mathbb{Z}\right\}.$$

Exemple. – Considérons la courbe plane $\mathcal{C}$ d'équation $X^2 = Y^3$. Son anneau de fonctions est donc l'anneau intègre $A = \mathbb{C}[X,Y]/(X^2 - Y^3)$, dont le corps de fractions $K = \mathbb{C}(Y)[X]/(X^2 - Y^3)$ est une extension quadratique de $\mathbb{C}(Y)$. Le même principe que ci-dessus nous montre alors que la normalisation de A, qui n'est autre que la clôture intégrale de $\mathbb{C}[Y]$ dans K puisque $A = \mathbb{C}[Y] + X\mathbb{C}[Y]$ est entier sur $\mathbb{C}[Y]$, est $\tilde{A} := \mathbb{C}[Y] + \frac{X}{Y}\mathbb{C}[Y]$. On peut remarquer que l'unique morphisme de $\mathbb{C}$-algèbres $\mathbb{C}[T] \longrightarrow \tilde{A}$ qui envoie T sur $\frac{X}{Y}$ est un isomorphisme (noter qu'il envoie T^2 sur Y et T^3 sur X). Géométriquement, la courbe $\mathcal{C}$ présente une "singularité" en le point $(0,0)$, et la non normalité de A est le reflet algébrique de cette singularité. De plus, on observe que la normalisation $\tilde{A}$ de A est l'anneau des fonctions d'une courbe "lisse" $\tilde{\mathcal{C}}$ (isomorphe à la droite affine) et l'inclusion $A \subset \tilde{A}$ fournit une application polynomiale $\tilde{\mathcal{C}} \longrightarrow \mathcal{C}$ (penser que les points de $\mathcal{C}$ sont les idéaux maximaux de A) que l'on peut interpréter comme une "désingularisation" de la courbe $\mathcal{C}$. Il se trouve que toute courbe singulière irréductible peut être "désingularisée" par normalisation, mais en dimension supèrieure c'est bien plus compliqué...

2.12.4 *Une autre preuve du théorème 2.11.3.* Avec les notations de 2.11.2, on souhaite montrer que $\mathbb{Z}[\Sigma_1, \cdots, \Sigma_n] = \mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n}$ et que les Σ_i sont algébriquement indépendants sur $\mathbb{Z}$. La première étape est d'utiliser la théorie de Galois pour prouver que $\mathbb{Q}(\Sigma_1, \cdots, \Sigma_n) = \mathbb{Q}(X_1, \cdots, X_n)^{\mathfrak{S}_n}$. Posons $K = \mathbb{Q}(X_1, \cdots, X_n)$ et $k = \mathbb{Q}(\Sigma_1, \cdots, \Sigma_n)$. On a manifestement $k \subset K^{\mathfrak{S}_n}$. La proposition 2.7.7 nous dit que $[K : K^{\mathfrak{S}_n}] = n!$ et le fait que K soit un corps de décomposition du polynôme $f = T^n - \Sigma_1 T^{n-1} + \cdots + (-1)^n \Sigma_n$ montre que $[K : k] \leqslant n!$. L'égalité $k = K^G$ s'ensuit. La deuxième étape utilise la notion de degré de transcendance. Puisque K est algébrique sur k, ils ont même degré de transcendance sur $\mathbb{Q}$ d'après le théorème 2.1.7. Mais cela implique que les Σ_i sont algébriquements indépendants sur $\mathbb{Q}$, et a fortiori sur $\mathbb{Z}$. La dernière étape est d'utiliser la normalité pour prouver que l'inclusion $\mathbb{Z}[\Sigma_1, \cdots, \Sigma_n] \subset \mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n}$ est une égalité. Posons $A = \mathbb{Z}[\Sigma_1, \cdots, \Sigma_n]$ et $B = \mathbb{Z}[X_1, \cdots, X_n]$. Puisque le polynôme f ci-dessus est unitaire et dans $A[T]$, l'anneau B est entier sur A. A fortiori, l'anneau $B^{\mathfrak{S}_n}$ est entier sur A, et par ailleurs, il est contenu dans le corps des fractions $k = K^{\mathfrak{S}_n}$ de A. Or, A est factoriel, donc normal, et il s'ensuit que $A = B$.

2.13 Anneaux d'entiers algébriques

On s'intéresse ici à la structure de l'anneau des entiers $\mathcal{O}_K$ d'un corps de nombres K. Le théorème suivant montre que c'est un $\mathbb{Z}$-module libre de rang $[K : \mathbb{Q}]$.

2.13.1 THÉORÈME.– *Soit A normal et B la clôture intégrale de A dans une extension séparable finie L de $K = \mathrm{Frac}(A)$. Alors il existe deux sous-A-modules M, M' de L, libres de rang $[L : K]$ et tels que $M \subset B \subset M'$. En particulier :*
- *Si A est noethérien, alors B est un A-module de type fini.*
- *Si A est principal, alors B est libre de rang $[L : K]$.*

La preuve repose sur la caractérisation de la séparabilité par la non-dégénérescence d'une certaine forme K-bilinéaire sur L. Pour la définir, considérons plus généralement une extension $A \subset B$ d'anneaux commutatifs avec B libre de rang fini sur A. Pour $b \in B$, on pose $\mathrm{Tr}_{B/A}(b) := \mathrm{tr}(m(b))$ où $m(b)$ est l'endomorphisme A-linéaire de B donné par la multiplication par b. On définit alors la forme A-bilinéaire symétrique

$$\theta_{B/A} : (b, b') \mapsto \mathrm{Tr}_{B/A}(bb').$$

Comme d'habitude, on dit que cette forme A-bilinéaire est *non-dégénérée* si $\forall b \in B, \exists b' \in B$ t.q. $\theta_{B/A}(bb') \neq 0$. Dans ce cas elle induit "un isomorphisme de B sur son A-dual", i.e. l'application A-linéaire $B \longrightarrow \mathrm{Hom}_A(B, A)$, $b \mapsto (b' \mapsto \theta_{B/A}(b'b))$, est un isomorphisme.

LEMME. – *Une extension finie $K \subset L$ est séparable si et seulement si la forme K-bilinéaire $\theta_{L/K}$ est non-dégénérée.*

Démonstration. Soit $K \hookrightarrow \overline{K}$ une clôture algébrique de K. Regardons $\overline{K} \otimes_K L$ comme une $\overline{K}$-algèbre de dimension $[L : K]$. Pour tout $b \in L$, on a manifestement

$$\mathrm{Tr}_{\overline{K} \otimes_K L/\overline{K}}(1 \otimes bb') = \mathrm{Tr}_{L/K}(bb').$$

En particulier, si $b_1, \cdots, b_n$ est une K-base de L, alors le discriminant $\det(\mathrm{Tr}_{L/K}(b_i b_j)_{i,j})$ de $\theta_{L/K}$ dans cette base coïncide avec celui de $\theta_{\overline{K} \otimes_K L/\overline{K}}$ dans la $\overline{K}$-base $(1 \otimes b_1, \cdots, 1 \otimes b_n)$. Il s'ensuit que $\theta_{L/K}$ est non-dégénérée si et seulement si $\theta_{\overline{K} \otimes_K L/\overline{K}}$ est non dégénérée. D'un autre côté, on a vu que L/K est séparable si et seulement si $\overline{K} \otimes_K L$ est réduite, auquel cas elle est isomorphe à l'algèbre produit $\overline{K}^{[L:K]}$. Ainsi, si L/K est séparable, il existe une $\overline{K}$ base $e_1, \cdots, e_n$ de $\overline{K} \otimes_K L$ dans laquelle la multiplication est donnée par $e_i e_j = \delta_{ij} e_i$. On a alors $\mathrm{Tr}_{\overline{K} \otimes_K L/\overline{K}}(e_i) = 1$ et le discriminant dans cette base est donné par $\det(\theta_{\overline{K} \otimes_K L/\overline{K}}(e_i, e_j)) = \det(I_n) = 1$, donc $\theta_{L/K}$ est non dégénérée. Réciproquement, si L/K n'est pas séparable, soit $x \in \overline{K} \otimes_K L$ nilpotent non nul. Alors pour tout $y \in \overline{K} \otimes_K L$, l'élément xy est nilpotent, donc de trace nulle, et x est donc dans le noyau de $\theta_{\overline{K} \otimes_K L/\overline{K}}$. □

Démonstration du théorème 2.13.1. Notons $n = [L : K]$. Soit $b_1, \cdots, b_n$ une base de L sur K contenue dans B (existe car $L = \mathrm{Frac}(B)$). On a donc $M := \bigoplus_i A b_i \subset B$. Soit $b_1^*, \cdots, b_n^*$ la base duale pour la forme non dégénérée $\theta_{L/K}$ (séparabilité). Pour tout $b \in B$, on a

$$b = \sum_{i=1}^{n} \mathrm{Tr}_{L/K}(bb_i) b_i^*$$

et $\mathrm{Tr}_{L/K}(bb_i) \in A$ d'après le lemme ci-dessous. Donc $B \subset M' := \bigoplus_i A b_i^*$. □

LEMME. – *Dans la situation du théorème 2.13.1, on a $\mathrm{Tr}_{L/K}(b) \in A$ pour tout $b \in B$.*

Démonstration. Comme dans la preuve du lemme précédent, on a $\mathrm{Tr}_{L/K}(b) = \mathrm{Tr}_{\overline{K} \otimes_K L/\overline{K}}(1 \otimes b)$. Puisque L est séparable sur K, le morphisme de $\overline{K}$-algèbres $\overline{K} \otimes_K L \longrightarrow \prod_{\iota : L \hookrightarrow \overline{K}} \overline{K}$ (où le produit est indexé par les K-plongements de L dans $\overline{K}$) est un isomorphisme. Cet isomorphisme envoie $1 \otimes b$ sur $(\iota(b))_{\iota : L \hookrightarrow \overline{K}}$. Numérotons les plongements $\iota_1, \cdots, \iota_n$, et notons e_i l'idempotent de $\overline{K} \otimes_K L$ associé à ι_i, de sorte que $e_i e_j = \delta_{ij} e_i$. Alors la matrice de la multiplication par $1 \otimes b$ dans cette base est la matrice diagonale $(\iota_1(b), \cdots, \iota_n(b))$. On en déduit sa trace :

$$\mathrm{Tr}_{L/K}(b) = \sum_{\iota : L \hookrightarrow \overline{K}} \iota(b).$$

Or chaque élément $\iota(b) \in \overline{K}$ a le même polynôme minimal que b, donc est entier sur A. Il s'ensuit que $\mathrm{Tr}_{L/K}(b)$ est entier sur A. Comme c'est un élément de K et comme A est normal, on a $\mathrm{Tr}_{L/K}(b) \in A$. □

2.13.2 *Le problème de l'élément primitif.* On a vu que toute extension finie K de $\mathbb{Q}$ est monogène, i.e. de la forme $\mathbb{Q}(\alpha)$ pour un $\alpha \in K$. Il est naturel de se demander si $\mathcal{O}_K$ est aussi monogène sur $\mathbb{Z}$. C'est vrai (exercice) dans le cas $[K : \mathbb{Q}] = 2$, mais il y a déjà plein de contre-exemples en degré 3, par exemple $K = \mathbb{Q}(\sqrt[3]{175})$. Voici tout de même un critère qui parfois suffit à trouver un générateur.

Proposition. – *Soit $K = \mathbb{Q}[\alpha]$ un corps de nombres de degré n, avec $f_\alpha \in \mathbb{Z}[X]$ (donc α entier). Si $\mathrm{disc}(f_\alpha) \in \mathbb{Z}$ est sans facteur carré, alors $\{1, \alpha, \cdots, \alpha^{n-1}\}$ est une base de $\mathcal{O}_K$ sur $\mathbb{Z}$ (et donc $\mathcal{O}_K = \mathbb{Z}[\alpha]$).*

Démonstration. Nous allons encore utiliser la forme bilinéaire $\theta_{K/\mathbb{Q}}$. Si $b_1, \cdots, b_n$ sont des éléments de $\mathcal{O}_K$, on note $D_{K/\mathbb{Q}}(b_1, \cdots, b_n) := \det\left(\mathrm{Tr}_{K/\mathbb{Q}}(b_i b_j)\right)_{i,j}$. D'après le lemme précédent, c'est un élément de $\mathbb{Z}$. Choisissons $b_1, \cdots, b_n$ de sorte à former une $\mathbb{Z}$-base de $\mathcal{O}_K$. Si $b'_1, \cdots, b'_n$ est une autre famille d'éléments de $\mathcal{O}_K$, et P est la matrice de passage $(b'_i)_i = P.(b_i)_i$, alors on a

$$D_{K/\mathbb{Q}}(b'_1, \cdots, b'_n) = \det(P)^2 \cdot D_{K/\mathbb{Q}}(b_1, \cdots, b_n).$$

Si $b'_1, \cdots, b'_n$ est aussi une $\mathbb{Z}$-base de $\mathcal{O}_K$, alors $P \in \mathrm{GL}_n(\mathbb{Z})$ a pour déterminant ± 1, et on voit que l'entier

$$\mathrm{disc}(K/\mathbb{Q}) := D_{K/\mathbb{Q}}(b_1, \cdots, b_n)$$

ne dépend pas de la $\mathbb{Z}$-base de $\mathcal{O}_K$ choisie. On l'appelle *discriminant* de K.

Prenons maintenant la famille $(b'_1, \cdots, b'_n) = (1, \alpha, \cdots, \alpha^{n-1})$. On a donc

$$D_{K/\mathbb{Q}}(1, \alpha, \cdots, \alpha^{n-1}) = \mathrm{disc}(K/\mathbb{Q}) \cdot \det(P)^2.$$

Nous allons montrer que $D_{K/\mathbb{Q}}(1, \alpha, \cdots, \alpha^{n-1}) = \mathrm{disc}(f_\alpha)$. Par l'hypothèse de la proposition, il s'en suivra que le terme de gauche ci-dessus est sans facteur carré, donc que $\det(P) = \pm 1$, donc $P \in \mathrm{GL}_n(\mathbb{Z})$ et finalement $(1, \alpha, \cdots, \alpha^{n-1})$ est bien une $\mathbb{Z}$-base de $\mathcal{O}_K$.

Pour calculer $D_{K/\mathbb{Q}}(1, \alpha, \cdots, \alpha^{n-1})$, on utilise la formule prouvée dans le lemme précédent $\mathrm{Tr}_{K/\mathbb{Q}}(b) = \sum_{\iota : K \hookrightarrow \overline{\mathbb{Q}}} \iota(b)$. En numérotant les plongements $\iota_1, \cdots, \iota_n$ on constate que

$$\mathrm{Tr}_{K/\mathbb{Q}}(b'_i b'_j) = \sum_{k=1}^{n} \iota_k(b'_i) \iota_k(b'_j)$$

donc la matrice $(\mathrm{Tr}_{K/\mathbb{Q}}(b'_i b'_j))_{i,j}$ est le produit ${}^tU.U$ avec U la matrice $(\iota_i(b'_j))_{i,j}$. Faisons maintenant $b'_j = \alpha^{j-1}$. La matrice U est donc une matrice de Vandermonde $(\iota_i(\alpha)^{j-1})_{i,j}$ et on a donc

$$D_{K/\mathbb{Q}}(1, \alpha, \cdots, \alpha^{n-1}) = \det(U)^2 = \prod_{i<j}(\iota_i(\alpha) - \iota_j(\alpha))^2 = \mathrm{disc}(f_\alpha),$$

la dernière égalité venant du fait que les $\iota_i(\alpha)$ sont les racines de f_α dans $\overline{\mathbb{Q}}$. $\square$

Exemples. – Mêmes notations que la proposition.

i) Si $f_\alpha(X) = X^3 - X - 1$, on calcule $\mathrm{disc}(f_\alpha) = -23$, donc $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

ii) Si $f_\alpha(X) = X^3 + X^2 - 2X + 8$, alors $\mathrm{disc}(f_\alpha) = -2012 = -4 \times 503$. Dans ce cas, on peut montrer que $\mathbb{Z}[\alpha] \neq \mathcal{O}_K$.

2.13.3 *Pour aller plus loin.* Avec les notations de la preuve ci-dessus, le théorème d'échelonnage des matrices entières nous dit que $|\det(P)|$ est l'indice $(\mathcal{O}_K : \mathbb{Z}[\alpha])$ du sous-groupe $\mathbb{Z}[\alpha]$ dans $\mathcal{O}_K$. La preuve nous borne cet indice, au sens où pour tout premier p, on a $\nu_p(\mathcal{O}_K : \mathbb{Z}[\alpha]) \leqslant \frac{1}{2}\nu_p(\mathrm{disc}(f_\alpha))$. Pour pouvoir dire plus, il faut des informations sur $\mathrm{disc}(K/\mathbb{Q})$

PROPOSITION. – *Soit K un corps de nombres. On a*

i) $\mathrm{sgn}(\mathrm{disc}(K/\mathbb{Q})) = (-1)^{r_2}$ *où r_2 est la moitié du nombre de plongements imaginaires* $K \hookrightarrow \mathbb{C}$.

ii) $\mathrm{disc}(K/\mathbb{Q}) \equiv 0$ *ou* 1 *modulo* 4 *(Stickelberger).*

Démonstration. i) Soit $\omega_1, \cdots, \omega_n$ une base de $K/\mathbb{Q}$ et $\sigma_1, \cdots, \sigma_n$ les plongements $K \hookrightarrow \mathbb{C}$. Soit $M = (\sigma_i(\omega_j))_{i,j} \in M_n(\mathbb{C})$. On sait que $D_{K/\mathbb{Q}}(\omega_1, \cdots, \omega_n) = (\det(M))^2$ et le signe que l'on cherche est donc celui de $(\det(M))^2$. Or la matrice conjuguée $\overline{M} = (\overline{\sigma}_i(\omega_j))_{i,j}$ s'obtient à partir de M par r_2 échanges de lignes, de sorte que $\det(\overline{M}) = (-1)^{r_2}\det(M)$. On en déduit que $(\det(M)) = (-1)^{r_2}|\det(M)|^2$, d'où le signe annoncé.

ii) Soit $\alpha_1, \cdots, \alpha_n$ une base de $\mathcal{O}_K$ sur $\mathbb{Z}$ et $\sigma_1, \cdots, \sigma_n$ les plongements $K \hookrightarrow \mathbb{C}$. Alors

$$\begin{aligned}\mathrm{disc}(K/\mathbb{Q}) = \left(\det\left(\sigma_i(\alpha_j)\right)_{i,j}\right)^2 &= \left(\sum_{\tau\in\mathfrak{S}_n, \varepsilon(\tau)=1}\prod_{i=1}^n \sigma_i(\alpha_{\tau(i)}) - \sum_{\tau\in\mathfrak{S}_n, \varepsilon(\tau)=-1}\prod_{i=1}^n \sigma_i(\alpha_{\tau(i)})\right)^2 \\ &= (P - I)^2 \\ &= (P + I)^2 - 4PI\end{aligned}$$

Nous allons montrer que $P + I$ et PI sont des entiers (dans $\mathbb{Z}$), ce qui impliquera que $\mathrm{disc}(K/\mathbb{Q}) \equiv (P + I)^2[4] \equiv 0, 1[4]$ puisque le carré d'un entier est toujours congru à 0 ou 1 modulo 4.

Puisque les $\sigma_i(\alpha_j)$ sont des entiers algébriques, $P + I$ et PI ont aussi des entiers algébriques, et il nous suffira donc de prouver qu'ils sont rationnels (dans $\mathbb{Q}$), *i.e.* invariants par $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Soit donc $\gamma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Il induit une permutation $\tau_\gamma : \sigma \mapsto \gamma \circ \sigma$ des plongements $\sigma_1, \cdots, \sigma_n$. Si τ_γ est paire, on a $\gamma(P) = P$ et $\gamma(I) = I$. Si τ_γ est impaire, on a $\gamma(P) = I$ et $\gamma(I) = P$. Il s'ensuit que $\gamma(P+I) = P+I$ et $\gamma(PI) = PI$, comme voulu. $\square$

2.13.4 *Corps quadratiques.* Supposons $K = \mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z}$ sans facteur carré. On a alors

$$\mathrm{disc}(X^2 - d) = 4d = \mathrm{disc}(K/\mathbb{Q})(\mathcal{O}_K : \mathbb{Z}[\sqrt{d}])^2,$$

ce qui laisse a priori deux possibilités pour $\mathrm{disc}(K/\mathbb{Q})$: soit il vaut $4d$, soit il vaut d. Dans ce dernier cas on doit avoir $d \equiv 1[4]$ d'après le théorème de Stickelberger. On en déduit la dichotomie suivante :

i) Si $d \equiv 2$ ou 3 modulo 4, alors $\mathrm{disc}(K/\mathbb{Q}) = 4d$ et $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.

ii) Si $d \equiv 1$ modulo 4, alors $\frac{1+\sqrt{d}}{2}$ est entier donc $\mathbb{Z}[\sqrt{d}] \neq \mathcal{O}_K$ et $\mathrm{disc}(K/\mathbb{Q}) = d$. Dans ce cas on a $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

2.13.5 *Corps p-cyclotomiques.* Fixons un entier $r \geqslant 1$ et posons $\zeta_r := \exp(\frac{2i\pi}{p^r}) \in \mathbb{C}$. Nous allons montrer que $\mathcal{O}_{\mathbb{Q}(\zeta_r)} = \mathbb{Z}[\zeta_r]$.

Le polynôme minimal de ζ_r est $\Phi_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1}$. Calculons son discriminant par la formule

$$\mathrm{disc}(\Phi_{p^r}) = (-1)^{\frac{\varphi(p^r)(\varphi(p^r)-1)}{2}} N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\Phi'_{p^r}(\zeta_r)).$$

On a $\Phi'_{p^r}(\zeta_r) = p^r \frac{\zeta_r^{p^r-1}}{\zeta_r^{p^{r-1}}-1} = p^r \frac{\zeta_r^{-1}}{\zeta_1 - 1}$. Remarquons que $N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\zeta_r)$ est une racine p^r-ème de l'unité dans $\mathbb{Q}$, donc vaut 1 si $p \neq 2$. Si $p = 2$, alors la formule $N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\zeta_r) = \prod_{a \in (\mathbb{Z}/p^r\mathbb{Z})^\times} \zeta_r^a$ montre que $N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\zeta_r) = 1$ sauf dans le cas $r = 1$ où $N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\zeta_r) = -1$. Par ailleurs, on a

$$N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\zeta_1 - 1) = N_{\mathbb{Q}(\zeta_1)/\mathbb{Q}}(\zeta_1 - 1)^{[\mathbb{Q}(\zeta_r):\mathbb{Q}(\zeta_1)]} = \left(\prod_{i=1}^{p-1}(\zeta_1^i - 1)\right)^{p^{r-1}}.$$

Le produit $\prod_{i=1}^{p-1}(\zeta_1^i - 1)$ est le produit des racines du polynôme $\Phi_p(1+T) = (1+T)^{p-1} + \cdots + (1+T) + 1$, donc est égal à $(-1)^{p-1}p$. Finalement on obtient

$$\mathrm{disc}(\Phi_{p^r}) = \pm p^{r\varphi(p^r)} \frac{1}{p^{p^{r-1}}} = \pm p^{rp^r - (r+1)p^{r-1}}.$$

La formule $\mathrm{disc}(\Phi_{p^r}) = (\mathcal{O}_{\mathbb{Q}(\zeta_r)} : \mathbb{Z}[\zeta_r])^2 \mathrm{disc}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$ nous dit que p est le seul premier susceptible de diviser l'indice $(\mathcal{O}_{\mathbb{Q}(\zeta_r)} : \mathbb{Z}[\zeta_r])$. Pour conclure, on utilise le résultat suivant joint à l'observation que $\Phi_{p^r}(1+X)$ est Eisenstein en p avec $\Phi_{p^r}(1) = p$.

PROPOSITION. – *Soit $f \in \mathbb{Z}[X]$ un polynôme Eisenstein pour le premier p et α une racine de f dans $\overline{\mathbb{Q}}$. Alors p ne divise pas l'indice de $\mathbb{Z}[\alpha]$ dans $\mathcal{O}_{\mathbb{Q}(\alpha)}$.*

Démonstration. Nous allons supposer pour simplifier que $f(0) = \pm p$ car cette hypothèse est satisfaite dans le cas cyclotomique qui nous intéresse (exercice : adapter au cas général).

Nous voulons montrer que si $x \in \mathcal{O}_K$ et $p^k x \in \mathbb{Z}[\alpha]$ alors $x \in \mathbb{Z}[\alpha]$. En notant $n = \deg(f)$, l'hypothèse Eisenstein implique $\alpha^n \in p\mathbb{Z}[\alpha]$. Il suffit donc de montrer que si $x \in \mathcal{O}_K$ et $\alpha^{k'} x \in \mathbb{Z}[\alpha]$ alors $x \in \mathbb{Z}[\alpha]$. Par récurrence, on peut supposer $k' = 1$. Soit donc $x \in \mathcal{O}_K$ tel que $\alpha x \in \mathbb{Z}[\alpha]$. Soit $x^m + b_1 x^{m-1} + \cdots + b_m = 0$ une équation entière satisfaite par x. En multipliant par α^m, on constate que $(\alpha x)^m \in \alpha\mathbb{Z}[\alpha]$ D'après notre hypothèse supplémentaire, on a $\mathbb{Z}[\alpha]/\alpha\mathbb{Z}[\alpha] = \mathbb{Z}[X]/(f, X) = \mathbb{Z}/f(0)\mathbb{Z} = \mathbb{Z}/p\mathbb{Z}$, donc $\alpha\mathbb{Z}[\alpha]$ est un idéal premier et α est un élément irréductible de $\mathbb{Z}[\alpha]$ dont la valuation associée v_α est multiplicative. La relation $(\alpha x)^m \in \alpha\mathbb{Z}[\alpha]$ implique alors que $v_\alpha(\alpha x) > 0$ donc il existe $y \in \mathbb{Z}[\alpha]$ tel que $\alpha x = \alpha y$ et finalement $x = y \in \mathbb{Z}[\alpha]$. $\square$

Remarque. – En adaptant la preuve, on peut montrer par récurrence sur le nombre de facteurs premiers de n que $\mathcal{O}_{\mathbb{Q}(\exp(2i\pi/n))} = \mathbb{Z}[\exp(2i\pi/n)]$.