# ALGÈBRE II

Joseph Le Potier

UNIVERSITÉ DENIS DIDEROT - PARIS 7
1998-1999

TABLE DES MATIÈRES

1. Nullstellensatz ..... 5
1.1. Nilradical ..... 5
1.2. Radical de Jacobson ..... 6
1.3. Entiers algébriques ..... 7
1.4. Théorème des zéros ..... 9
1.5. Théorème de normalisation de Noether ..... 12
1.6. Démonstration du théorème des zéros ..... 14
2. Décomposition primaire ..... 15
2.1. Topologie de Zariski ..... 15
2.2. Composantes irréductibles ..... 17
2.3. Idéaux premiers associés ..... 20
2.4. Décomposition primaire ..... 25
2.5. Unicité ..... 26
2.6. Modules de longueur finie ..... 30
3. Dimension ..... 39
3.1. Chaînes de fermés irréductibles ..... 39
3.2. Extensions entières ..... 40
3.3. Degré de transcendance de $\mathrm{K(A)}$ ..... 44
3.4. Hauteur d'un idéal premier ..... 46
3.5. Modules filtrés ..... 50
3.6. Anneaux et modules gradués associés ..... 52
3.7. Séries de Poincaré ..... 53
3.8. Dimension des anneaux locaux noethériens ..... 58
3.9. Anneaux locaux réguliers ..... 62
4. Représentations des groupes finis ..... 66
4.1. Définitions ..... 66
4.2. Le théorème de Maschke ..... 69
4.3. Lemme de Schur ..... 71
4.4. Produit tensoriel ..... 73
4.5. Caractère d'une représentation ..... 78
4.6. Fonctions centrales ..... 83
4.7. Exemples ..... 86
4.8. L'anneau des représentations ..... 92
4.9. L'algèbre $k[\mathrm{G}]$ ..... 95
4.10. Représentations du groupe symétrique ..... 101
4.11. Représentations induites ..... 107

## 1. Nullstellensatz

Les anneaux considérés seront toujours des anneaux commutatifs et unitaires. Un tel anneau est non nul si et seulement si $1 \neq 0$.

### 1.1. Nilradical

Soit A un anneau non nul. On rappelle qu'un idéal $\mathfrak{p}$ de A est premier s'il est distinct de A et si l'anneau quotient $A/\mathfrak{p}$ est intègre, c'est-à-dire que si $a$ et $b$ sont deux éléments de A tels que $ab \in \mathfrak{p}$ alors soit $a \in \mathfrak{p}$, soit $b \in \mathfrak{p}$.

DÉFINITION 1.1. — *Un élément $x \in A$ est dit nilpotent s'il existe un entier $n \geq 0$ tel que $x^n = 0$. On appelle nilradical de A (ou radical nilpotent) l'idéal $\mathfrak{n} \subset A$ des éléments nilpotents.*

PROPOSITION 1.2. — *Le nilradical de A est l'intersection des idéaux premiers de A.*

*Démonstration.* Il est clair que le nilradical est contenu dans tout idéal premier. Montrons l'inclusion en sens inverse, ou ce qui revient au même, que si $x$ un élément qui n'est pas nilpotent, il existe un idéal premier $\mathfrak{p}$ de A qui ne contient pas $x$.

On considère pour ceci l'ensemble S des puissances $x^n$ de $x$, pour $n$ entier $\geq 0$. Cet ensemble est une partie multiplicative, ce qui signifie que les deux propriétés suivantes sont satisfaites :

— $1 \in A$ ;

— si $s'$ et $s'' \in S$, on a $s's'' \in S$.

On peut dans ces conditions considérer l'anneau des fractions $S^{-1}A$ des fractions à dénominateur dans S, noté aussi $A_x$. Pour ceci, on introduit le quotient de l'ensemble des couples $(x, s) \in A \times S$ par la relation d'équivalence définie par $(a, s) \sim (a', s')$ s'il existe $s'' \in S$ telles que $s''(sx' - s'x) = 0$. La classe d'équivalence de $(a, s)$ est notée $\frac{x}{s}$, et on met sur cet ensemble une structure d'anneau en recopiant les règles habituelles de calcul sur les fractions. Remarquons que l'homomorphisme canonique

$$i : A \longrightarrow S^{-1}A$$

n'est pas obligatoirement injectif, et qu'il a pour noyau l'ensemble des éléments $a \in A$ tels qu'il existe $n \in \mathbb{N}$ tel que $ax^n = 0$. L'hypothèse $x$ non nilpotent signifie que ce noyau est un idéal propre, et pas conséquent $A_x$ est bien un anneau non nul. Il a alors des idéaux maximaux, et donc des idéaux premiers : l'image réciproque $\mathfrak{q} = i^{-1}(\mathfrak{p})$ d'un idéal premier $\mathfrak{p}$ de $A_x$ est un idéal premier de A. Un tel idéal premier ne rencontre pas S. Par suite, $x \notin \mathfrak{q}$. □

DÉFINITION 1.3. — *Soit I un idéal propre d'un anneau A. On appelle radical de I l'ensemble des éléments de A dont une puissance appartient à I.*

COROLLAIRE 1.4. — *Pour tout idéal I de A, le radical de I (ou racine de I) est l'intersection des idéaux premiers qui le contiennent. On le note* Rad I.

*Démonstration.* Le radical de I est l'image inverse du nilradical de A/I par la projection $A \longrightarrow A/I$. Il suffit donc d'appliquer la proposition 1.2 à l'anneau quotient A/I. □

### 1.2. Radical de Jacobson

DÉFINITION 1.5. — *Soit* A *un anneau non nul. On appelle radical de Jacobson de* A *l'intersection des idéaux maximaux de* A.

PROPOSITION 1.6. — *Un élément* $a \in A$ *appartient au radical de Jacobson si et seulement si* $1 - ax$ *est inversible pour tout* $x \in A$.

*Démonstration.* Supposons que $a$ appartienne au radical de Jacobson. Pour tout élément $x \in A$, l'élément $1-ax$ n'appartient à aucun idéal maximal, et donc est inversible. Réciproquement, si $1 - ax$ est inversible pour tout $x \in A$, montrons que $a$ appartient à tout idéal maximal $\mathfrak{m}$ de A. Supposons qu'il existe un idéal maximal $\mathfrak{m}$ tel que $a \notin \mathfrak{m}$. Alors la classe de $a$ dans $A/\mathfrak{m}$ est inversible, donc il existe $x$ tel que $ax - 1 \in \mathfrak{m}$. Ceci contredit l'hypothèse. □

Il est évident que le radical d'un anneau est contenu dans le radical de Jacobson. En général, le radical de Jacobson diffère du radical. Rappelons d'abord la notion d'anneau local.

PROPOSITION 1.7. — *Soit* A *un anneau non nul. Les assertions suivantes sont équivalentes :*
(1) *L'anneau* A *a un seul idéal maximal.*
(2) *L'ensemble des éléments non inversibles est un idéal.*

*Démonstration.* (1) ⇒ (2) : Soit $\mathfrak{m}$ l'unique idéal maximal de A, et U le groupe des éléments inversibles. Si $a \in A$ est un élément qui n'est pas inversible, on sait qu'il appartient à un idéal maximal, donc à $\mathfrak{m}$. Ainsi, $\mathfrak{m} = A - U$, et donc le complémentaire de U est un idéal.
(2) ⇒ (1) Si le complémentaire de U est un idéal $\mathfrak{m}$, cet idéal est évidemment le plus grand des idéaux propres. Tout idéal maximal est alors contenu dans $\mathfrak{m}$, et donc égal à $\mathfrak{m}$. □

DÉFINITION 1.8. — *Un anneau qui n'a qu'un idéal maximal s'appelle un anneau local.*

Il est clair que dans un anneau local qui n'est pas un corps, le radical de Jacobson diffère du radical. Dans certains cas, on peut cependant affirmer que le radical de Jacobson et le radical coïncident.

### 1.3. Entiers algébriques

Soit B un anneau et A un sous-anneau de B. Alors B peut être considéré comme un module sur A.

DÉFINITION 1.9. — *On dit qu'un élément* $x \in B$ *est entier sur* A *s'il existe un polynôme unitaire à coefficients dans* A

$$P = X^n + a_1 X^{n-1} + \ldots + a_n$$

*tel que* $P(x) = 0$. *Si tout élément* $x \in B$ *est entier algébrique sur* A *on dit que* B *est entier sur* A, *ou que* B *est une extension entière de* A.

La proposition suivante est souvent utile pour vérifier qu'un élément est entier. Elle permet par exemple de vérifier que les éléments de B qui sont entiers sur A constituent un sous-anneau de B, qu'on appelle fermeture intégrale de A dans B.

PROPOSITION 1.10. — *Soit* B *un anneau, et* A *un sous-anneau de* B. *Soit* $x$ *un élément de* B. *Les assertions suivantes sont équivalentes :*
(i) *L'élément* $x$ *est entier algébrique sur* A;
(ii) *Le sous-anneau* $A[x]$ *engendré par* A *et* $x$ *est un* A*−module de type fini ;*
(iii) *Il existe un sous-anneau de* B *contenant* A *et* $x$ *qui soit un* A*−module de type fini.*

*Démonstration.* Seule l'implication (iii) $\Rightarrow$ (i) n'est pas évidente. Soit C un sous-anneau de B contenant $x$ et A qui soit un A−module de type fini. Soit $(e_i)_{i=1,\ldots,m}$ un système de générateurs de C. L'inclusion $x\mathrm{C} \subset \mathrm{C}$ permet d'écrire

$$xe_i = \sum_j a_{i,j} e_j$$

avec $a_{i,j} \in \mathrm{A}$ ce qui s'écrit aussi dans $\mathrm{C}^n$, en introduisant le symbole de Kronecker

$$\sum_j (x\delta_{i,j} - a_{i,j}) e_j = 0$$

Considérons la matrice à coefficient dans A définie par $a = (a_{i,j})$. Si on multiplie à gauche par la matrice des cofacteurs, on obtient $\det(x\mathrm{id} - a)e_j = 0$ pour tout $j$. Puisque l'unité appartient à C, on obtient $\det(x\mathrm{id} - a) = 0$ ce qui donne en développant un polynôme unitaire à coefficients dans A annulant $x$. □

Nous aurons besoin dans les applications du lemme suivant.

LEMME 1.11. — *Soit* A *un sous-anneau d'un anneau* B, *et* M *un* B−*module de type fini. On suppose que* B *est un* A−*module de type fini. Alors* M *est un* A−*module de type fini.*

*Démonstration.* Soit $e_1, \ldots, e_m$ des générateurs du B−module M, et $b_1, \ldots, b_k$ des générateurs du A−module B. Alors les éléments $b_j e_i$ engendrent le A−module M. □

COROLLAIRE 1.12. — *Si* $x_1, \ldots, x_n \in \mathrm{B}$ *sont entiers algébriques sur* A, *le sous-anneau* $\mathrm{A}[x_1, \ldots, x_n]$ *engendré par* A *et* $x_1, \ldots, x_n$ *est de type fini sur* A.

*Démonstration.* On raisonne par récurrence sur $n$. C'est vrai pour $n = 1$ d'après le lemme ci-dessus. Supposons vrai pour $n - 1$. Alors dans les extensions $\mathrm{A} \subset \mathrm{B} = \mathrm{A}[x_1, \ldots, x_{n-1}] \subset \mathrm{A}[x_1, \ldots, x_n]$ la première est une extension de type fini d'après l'hypothèse de récurrence, et la seconde est un $\mathrm{A}[x_1, \ldots, x_{n-1}]$−module de type fini d'après l'énoncé ci-dessus, parce $x_n$ est entier sur B . Alors $\mathrm{A}[x_1, \ldots, x_n]$ est un A−module de type fini d'après le lemme ci-dessus. □

COROLLAIRE 1.13. — *L'ensemble des éléments* $x \in \mathrm{B}$ *qui sont entiers algébriques sur* A *est un sous-anneau de* B.

*Démonstration.* Il suffit de voir que si $x$ et $y \in \mathrm{B}$ sur des entiers algébriques sur A il en est de même de $x + y$ et $xy$. Mais $\mathrm{A}[x, y]$ est un A−module de type fini d'après le corollaire ci-dessus, et donc tout élément de $\mathrm{A}[x, y]$ est entier algébrique sur A d'après la proposition 1.10. □

COROLLAIRE 1.14. — *Soit* C *un anneau, et* $\mathrm{A} \subset \mathrm{B} \subset \mathrm{C}$ *deux sous-anneaux. Si* B *est entier sur* A *et* C *entier sur* B, *l'anneau* C *est entier sur* A.

*Démonstration.* Un élément $c \in \mathrm{B}$ entier sur B satisfait à une équation de dépendance intégrale

$$c^n + b_1 c^{n-1} + \ldots + b_n = 0$$

avec $b_i \in \mathrm{B}$. Les éléments $b_i$ sont entiers sur A, et $\mathrm{B}' = \mathrm{A}[b_1, \ldots, b_n]$ est donc un module de type fini sur A. De plus, l'équation de dépendance intégrale montre que $\mathrm{B}'[c]$ est un $\mathrm{B}'$−module de type fini. Par conséquent, $\mathrm{B}'[c]$ est un A−module de type fini. Il résulte de la proposition 1.10 que $c$ est entier sur A.

### 1.4. Théorème des zéros

THÉORÈME 1.15. — *(Nullstellensatz) Soit $k$ un corps, et* A *une $k-$algèbre de type fini sur $k$. Alors pour tout idéal maximal* $\mathfrak{m}$ *de* A, *l'extension*

$$k \hookrightarrow \mathrm{A}/\mathfrak{m}$$

*est une extension algébrique (finie).*

La démonstration de ce théorème sera donnée dans la section 1.6 ; donnons dès à présent quelques corollaires.

COROLLAIRE 1.16. — *Soient $k$ un corps, et* A *une $k-$algèbre de type fini. Alors le radical de Jacobson de* A *coïncide avec le radical nilpotent de* A.

La démonstration s'appuie sur le lemme suivant :

LEMME 1.17. — *Soit* B *un anneau intègre, et* $\mathrm{A} \subset \mathrm{B}$ *un sous-anneau. On suppose que* B *est entier sur* A. *Alors* B *est un corps si et seulement si* A *est un corps.*

*Démonstration.* Montrons que si B est un corps, A est un sous-corps de B. Soit $x \in \mathrm{A}$, non nul. Alors l'inverse $y = \frac{1}{x}$ de $x$ dans B est entier sur A, ce qui signifie qu'il existe un entier $n \geq 1$ et des éléments $a_1, \ldots, a_n \in \mathrm{A}$ tels que

$$y^n + a_1 y^{n-1} + \ldots + a_n = 0$$

Alors $1 + x(a_1 + \ldots + a_n x^{n-1}) = 0$. Il en résulte immédiatement que $y \in \mathrm{A}$. Réciproquement, supposons que A soit un corps. Soit $x$ un élément non nul de B. Il satisfait à une équation de dépendance intégrale

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

avec $a_i \in \mathrm{A}$. Si on choisit cette équation de sorte que $n$ soit minimal, puisque B est intègre $a_n \neq \mathrm{O}$, sinon on pourrait trouver après simplification une équation analogue de degré $< n$. Cette équation s'écrit

$$x(x^{n-1} + a_1 x^{n-1} + \ldots + a_{n-1}) = -a_n$$

ce qui implique évidemment que $x$ est inversible. □

Démonstration du corollaire 1.16

On raisonne comme dans la proposition 1.2. Il s'agit de montrer que $x \in \mathrm{A}$ est un élément qui n'est pas nilpotent, il existe un idéal maximal $\mathfrak{m}$ de A tel que $x \notin \mathfrak{m}$. Soit S la partie multiplicative de A formée des puissances $x^n$ de $x$ et $\mathrm{S}^{-1}\mathrm{A}$ l'anneau des fractions à dénominateur dans S. La démonstration de la proposition 1.2 fournit un morphisme non nul $\mathrm{A} \longrightarrow \mathrm{S}^{-1}\mathrm{A}$. Soit $\mathfrak{m}$ un idéal maximal de $\mathrm{S}^{-1}\mathrm{A}$, et $\mathfrak{p}$ l'idéal premier image réciproque de $\mathfrak{m}$. On a alors des homomorphismes injectifs d'anneaux

$$k \hookrightarrow \mathrm{A}/\mathfrak{p} \hookrightarrow \mathrm{L} = \mathrm{S}^{-1}\mathrm{A}/\mathfrak{m}.$$

Il est clair que $\mathrm{S}^{-1}\mathrm{A}$ est encore une $k-$algèbre de type fini, puisqu'elle est en fait isomorphe au quotient de $\mathrm{A}[\mathrm{Y}]$ par l'idéal engendré par $x\mathrm{Y} - 1$. Le théorème 1.15 montre que l'extension $k \hookrightarrow \mathrm{L}$ est entière, et par suite tout élément de L est entier sur $\mathrm{A}/\mathfrak{p}$. D'après le lemme ci-dessus, l'anneau $\mathrm{A}/\mathfrak{p}$ est un corps. Donc $\mathfrak{p}$ est un idéal maximal, et cet idéal maximal ne contient pas $x$. □

COROLLAIRE 1.18. — *Soient $k$ un corps, et* A *une $k-$algèbre de type fini. Pour tout idéal* $\mathrm{I} \subset \mathrm{A}$, *le radical de* I *est l'intersection des idéaux maximaux qui contiennent* I.

*Démonstration.* L'ensemble $\mathsf{Max}(A/I)$ des idéaux maximaux de $A/I$ s'identifie par image réciproque par la projection $p : A \longrightarrow A/I$ à l'ensemble des idéaux maximaux de A qui contiennent I. Soit N le radical nilpotent de $A/I$. L'égalité

$$N = \bigcap_{\mathfrak{m}\in \mathsf{Max}(A/I)} \mathfrak{m}$$

devient par image réciproque par $p$

$$\mathsf{Rad}(I) = \bigcap_{\mathfrak{m}\in \mathsf{Max}(A),I\subset\mathfrak{m}} \mathfrak{m}$$

ce qui démontre le corollaire.

COROLLAIRE 1.19. — *Soit $k$ un corps algébriquement clos. Tout idéal maximal de l'anneau $A = k[X_1, \ldots, X_n]$ est de la forme $\mathfrak{m}_a$, idéal des polynômes $P \in k[X_1, \ldots, X_n]$ qui s'annulent en un point $a = (a_1, \ldots, a_n) \in k^n$.*

*Démonstration.* On prend $A = k[X_1, \ldots, X_n]$. Puisque $k$ est algébriquement clos, l'extension $k \hookrightarrow A/\mathfrak{m}$ est un isomorphisme. On définit $a_i \in k$ par l'image réciproque de la classe de $X_i$ par cet isomorphisme. Alors $X_i - a_i \in \mathfrak{m}$ et par suite $\mathfrak{m}_a \subset \mathfrak{m}$. Donc, puisque $\mathfrak{m}_a$ est maximal, $\mathfrak{m}_a = \mathfrak{m}$. □

DÉFINITION 1.20. — *Un fermé algébrique de $k^n$ est une partie V définie par l'annulation simultanée d'une famille de polynômes.*

Les fermés algébriques de $k^n$ sont les fermés d'une topologie sur $k^n$ appelée topologie de Zariski. Soit V le fermé algébrique défini par l'annulation d'une famille $P_i$ de polynômes ; le fermé V est aussi le fermé des zéros de l'idéal I engendré par les $P_i$. Puisque l'anneau $k[X_1, \ldots, X_n]$ est noethérien, un tel fermé peut être défini par l'annulation d'une famille finie de polynômes. L'énoncé ci-dessus implique en particulier que si I est un idéal propre de $k[X_1, \ldots, X_n]$ le fermé V(I) n'est pas vide.

COROLLAIRE 1.21. — *Soit $k$ est un corps algébriquement clos. Soient I un idéal de $k[X_1, \ldots, X_n]$, et V(I) le fermé des zéros communs aux polynômes de I. L'idéal I(V(I)) des polynômes qui s'annulent sur V(I) est le radical de I.*

*Démonstration.* On sait que $\mathsf{Rad}(I)$ est l'intersection des idéaux maximaux de $k[X_1, \ldots, X_n]$ qui contiennenet I. Ces idéaux maximaux sont de la forme $\mathfrak{m}_a$ et le fait que $I \subset \mathfrak{m}_a$ signifie que $a \in V(I)$. Le radical $\mathsf{Rad}(I)$ est est donc l'ensemble des polynômes qui s'annulent en tout point de V(I). □

Exemple
Considérons dans $k[X, Y]$ l'idéal $I = (X^2, Y)$. Le fermé algébrique V(I) est réduit à l'origine de $k^2$. Le radical de I est l'idéal (X, Y) c'est-à-dire l'idéal maximal de $k[X, Y]$ associé à l'origine.

COROLLAIRE 1.22. — *Si $k$ est algébriquement clos, l'application $I \mapsto V(I)$ est un isomorphisme de l'ensemble des idéaux I de $k[X_1, \ldots, X_n]$ égaux à leur racine sur l'ensemble des fermés algébriques de $k^n$.*

### 1.5. Théorème de normalisation de Noether

Soient $k$ un corps, et A une $k-$algèbre. Des éléments $x_1, \ldots, x_n$ de A sont algébriquement indépendants si l'homomorphisme $k[X_1, \ldots, X_n] \mapsto A$ défini par $P \mapsto P(x_1, \ldots, x_n)$ est injectif.

THÉORÈME 1.23. — *Soit $k$ un corps, et A une $k-$algèbre de type fini, intègre. Il existe $x_1, \ldots, x_n$ tels que*
(i) *les éléments $x_1, \ldots, x_n$ sont algébriquement indépendants.*
(ii) *l'anneau A est entier sur $k[x_1, \ldots, x_n]$.*

La démonstration repose sur un lemme technique dû à Nagata.

LEMME 1.24. — *(Nagata) Soit $\mathrm{F} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n] = \mathrm{A}$ un polynôme non constant. Il existe des entiers $(m_i)_{i \geq 2}$ tels que si on pose*

$$\mathrm{Y}_i = \mathrm{X}_i - \mathrm{X}_1^{m_i}$$

*l'anneau A soit entier sur le sous-anneau $\mathrm{B} = k[\mathrm{F}, \mathrm{Y}_2, \ldots, \mathrm{Y}_n]$.*

*Démonstration.* Il suffit de choisir les entiers $m_i$ de sorte que $\mathrm{X}_1$ soit entier sur B. Considérons le polynôme à coefficient dans B défini par

$$\mathrm{H}(\mathrm{T}) = \mathrm{F}(\mathrm{T}, \mathrm{Y}_2 + \mathrm{T}^{m_2}, \ldots, \mathrm{Y}_n + \mathrm{T}^{m_n}) - \mathrm{F}$$

On a évidemment $\mathrm{H}(\mathrm{X}_1) = 0$. Il suffit donc de montrer que l'on peut choisir les $m_i$ de sorte que le coefficient du terme dominant soit dans $k$. Soit $d$ le degré de F. On écrit

$$\mathrm{F}(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \sum_{\sum \alpha_i \leq d} a_\alpha \mathrm{X}_1^{\alpha_1} \ldots \mathrm{X}_n^{\alpha_n}$$

où $\alpha = (\alpha_1, \ldots, \alpha_n)$ et un multi-indice, et où les coefficients $a_\alpha$ appartiennent à $k$. On a alors

$$\mathrm{H}(\mathrm{T}) = \sum_\alpha a_\alpha (\mathrm{T}^{\alpha_1 + \sum_{i>1} \alpha_i m_i} + \mathrm{H}_\alpha(\mathrm{T}))$$

où $\mathrm{H}_\alpha(\mathrm{T})$ est un polynôme en T à coefficients dans B de degré inférieur à $\alpha_1 + \sum_{i>1} \alpha_i m_i$. Si on choisit par exemple $m_i = (d+1)^{i-1}$ toutes les sommes $\alpha_1 + \sum_{i>1} \alpha_i m_i$ sont distinctes. Alors le coefficient du terme de plus degré de H ne dépend pas des $\mathrm{Y}_i$. □

Démonstration du théorème 1.23

Soit $m$ le nombre minimal d'éléments dans un système de générateurs de l'algèbre A, et $a_1, \ldots, a_m$ des générateurs de A. On fait une récurrence sur $m$. Le cas $m = 0$ est trivial. Considérons l'homomorphisme $k[\mathrm{X}_1, \ldots, \mathrm{X}_m] \longrightarrow \mathrm{A}$ défini par $\mathrm{P} \mapsto \mathrm{P}(a_1, \ldots, a_m)$. Si cet homomorphisme est injectif, on peut l'énoncé est trivial. Sinon, le noyau $\mathfrak{p}$ contient un polynôme F non constant, auquel on applique le lemme de Nagata. On obtient un sous-anneau B de $\mathrm{C} = k[\mathrm{X}_1, \ldots, \mathrm{X}_m]$ sur lequel A est entier. Par suite, l'extension

$$\mathrm{B}' := \mathrm{B}/\mathrm{B} \cap \mathfrak{p} \hookrightarrow \mathrm{C}/\mathfrak{p} \simeq \mathrm{A}$$

est une extension entière. On identifie B′ à un sous-anneau de A. L'algèbre $\mathrm{B}' = \mathrm{B}/\mathrm{B} \cap \mathfrak{p}$ est engendrée par $m-1$ éléments, et on peut donc lui appliquer l'hypothèse de récurrence : il existe des éléments $x_1, \ldots, x_n \in \mathrm{B}'$ satisfaisant aux conditions suivantes :
— $x_1, \ldots, x_n$ sont algébriquement indépendants sur $k$;
— B' est entier sur $k[x_1, \ldots, x_n]$.
D'après le corollaire 1.14, l'anneau A est entier sur $k[x_1, \ldots, x_n]$. D'où le théorème. □

### 1.6. Démonstration du théorème des zéros

Soit $k$ un corps, et $k \hookrightarrow \mathrm{L}$ une extension qui soit une algèbre de type fini sur $k$. Il s'agit de montrer que L est une extension algébrique de $k$. D'après le lemme de normalisation de Noether, il existe des éléments $x_1, \ldots, x_n \in \mathrm{L}$ algébriquement indépendants sur $k$ et tels que l'extension

$$k[x_1, \ldots, x_n] \hookrightarrow \mathrm{L}$$

soit entière. Mais, d'après le lemme 1.17, l'anneau $k[x_1, \ldots, x_n]$ est un corps, donc $n = 0$. Ainsi, $k \hookrightarrow \mathrm{L}$ est une extension algébrique. □

## 2. Décomposition primaire

Commençons par un lemme que nous utiliserons à plusieurs reprises.

LEMME 2.1. — *Soit* X *un ensemble ordonné. Les assertions suivantes sont équivalentes :*
(i) *Toute partie non vide de* E *a un élément maximal ;*
(ii) *Toute suite croissante d'éléments de* E *est stationnaire.*

*Démonstration.* (i) $\Rightarrow$ (ii) : Soit $x_n$ une suite croissante d'éléments de E. Alors l'ensemble $F = \{x_n, n \in \mathbb{N}\}$ un élément maximal, $x_m$. Alors pour $n \geq m$, on a $x_n = x_m$.

(ii) $\Rightarrow$ (i) : Soit $F \subset E$ une partie non vide de E. Supposons que F n'ait pas d'élément maximal. On construit par récurrence une suite de E qui n'est pas stationnaire. Le premier terme $x_0$ est choisi arbitrairement dans F qui est non vide par hypothèse. On suppose construit $x_0, \ldots, x_n$. Alors l'ensemble des $x \in F$ tels que $x_n < x$ n'est pas vide, ce qui permet de choisir $x_{n+1}$ dans cet ensemble. La suite ainsi construite n'est pas stationnaire. □

### 2.1. Topologie de Zariski

DÉFINITION 2.2. — *Un espace topologique est noethérien si toute suite décroissante de fermés est stationnaire.*

PROPOSITION 2.3. — *L'espace topologique $k^n$ muni de la topologie de Zariski, est noethérien.*

*Démonstration.* Soit $A = k[X_1, \ldots, X_n]$ l'algèbre des polynômes. L'énoncé résulte de la remarque suivante : si Y est un fermé de $k^n$ et I(Y) l'idéal de A des polynômes qui s'annulent sur Y, on a V(I(Y)) = Y. Soit $Y_m$ une suite décroissante de fermés. Alors la suite d'idéaux $I(Y_m)$ est croissante, et comme l'anneau A est noethérien d'après le théorème de Hilbert, cette suite est stationnaire. Il en résulte que la suite $Y_m$ est elle-même stationnaire. □

COROLLAIRE 2.4. — *Toute partie de $k^n$ est quasi-compacte pour la topologie de Zariski.*

Ceci signifie que de tout recouvrement ouvert, on peut extraire un recouvrement fini. Cet énoncé résulte en fait d'un énoncé plus général :

PROPOSITION 2.5. — *Soit* X *un espace topologique noethérien. Alors toute partie* $Y \subset X$ *est quasi-compacte.*

*Démonstration.* Soit $Y \subset X$. Il s'agit de montrer qu'étant donnée une famille $(F_i)_{i \in I}$ de fermés de X qui rencontrent Y et telle que pour toute partie finie $J \subset I$ l'intersection $F_J = \cap_{i \in J} F_i$ rencontre Y, l'intersection $F = \cap_i F_i$ rencontre Y. On peut évidemment supposer que cette famille est stable par intersection finie. Puisque X est noethérien, dans cette famille il existe un élément minimal $F_0$, et on a alors pour tout $i \in I$

$$F_i \cap F_0 = F_0$$

par suite $F_0 \subset F_i$. Mais alors $F \cap Y = F_0 \cap Y$ et cette intersection est non vide par hypothèse. □

Plus généralement, considérons un anneau quelconque A, non nul et l'ensemble Spec A des idéaux premiers de A. Etant donné un idéal $I \subset A$ on considère l'ensemble V(I) des idéaux premiers

$\mathfrak{p}$ contenant I. Les parties V(I) de Spec A ainsi définies sont les fermés d'une topologie appelée topologie de Zariski sur Spec A : en effet, on a les ppropriétés suivantes :

— $V(0) = \text{Spec A}; V(A) = \emptyset$;

— Si $(\mathfrak{a}_i)_{i\in I}$ est une famille d'idéaux de A,

$$V(\sum_i \mathfrak{a}_i) = \cap_i V(\mathfrak{a}_i)$$

— Si $(\mathfrak{a}_i)_{1\leq i\leq m}$ est une famille finie d'idéaux de A,

$$\cup_{1\leq i\leq m} V(\mathfrak{a}_i) = V(\cap_i \mathfrak{a}_i)$$

Si $f : A \longrightarrow B$ est un homomorphisme d'anneaux, l'application

$$f^* : \text{Spec B} \longrightarrow \text{Spec A}$$

qui associe à un idéal premier $\mathfrak{q}$ de B l'image réciproque $f^{-1}(\mathfrak{q})$ est continue.

Exercice 2.1
Soit $k$ un corps, et $A = k[X_1, \ldots, X_n]$ l'anneau des polynômes. L'application

$$k^n \longrightarrow \text{Spec A}$$

qui associe au point $a \in k^n$ l'idéal maximal $\mathfrak{m}_a$ des polynômes qui s'annulent en $a$ est un homéomorphisme sur son image.

Exercice 2.2
L'adhérence $\overline{\{\mathfrak{p}\}}$ d'un ensemble réduit à un point $\mathfrak{p} \in \text{Spec A}$ est l'ensemble des idéaux premiers $\mathfrak{q}$ qui contiennent $\mathfrak{p}$. En particulier, un point $\mathfrak{p}$ est fermé si et seulement si $\mathfrak{p}$ est un idéal maximal.

PROPOSITION 2.6. — *Si* A *est un anneau noethérien, l'espace topologique* Spec A *est noethérien.*

*Démonstration.* A tout fermé $F \subset \text{Spec A}$, on associe l'idéal I(F) de A défini par

$$I(F) = \cap_{\mathfrak{p}\in F} \mathfrak{p}$$

Ainsi, d'après la proposition 1.2, pour tout idéal I de A, I(V(I)) est le radical de I. De plus V(I(F)) = F. En effet, l'inclusion $F \subset V(I(F))$ est évidente. Dans l'autre sens, si $F = V(\mathfrak{a})$ on a $I(V(\mathfrak{a})) = \text{Rad}\,\mathfrak{a}$ et $V(\text{Rad}\,\mathfrak{a}) \subset V(\mathfrak{a}) = F$. Maintenant si $F_n$ est une suite décroissante de fermés de A, la suite des idéaux $I(F_n)$ est croissante, donc stationnaire puisque l'anneau A est noethérien. Il en résulte que la suite de fermés $F_n$ est elle-même stationnaire.

### 2.2. Composantes irréductibles

DÉFINITION 2.7. — *Un espace topologique* X *non vide est dit réductible s'il peut s'écrire comme réunion de deux fermés distincts de* X. *Dans le cas contraire, on dit que* X *est irréductible.*

PROPOSITION 2.8. — *Soit* X *un espace topologique. Les assertions suivantes sont équivalentes :*

(i) *l'espace* X *est irréductible ;*

(ii) *tout ouvert non vide de* X *est partout dense ;*

(iii) *deux ouverts non vides de* X *se rencontrent.*

PROPOSITION 2.9. — *Soit* A *un anneau de radical nilpotent* N, *et* X = Spec A. *Alors* X *est irréductible si et seulement si* A/N *est intègre, autrement dit si* N *est un idéal premier.*

*Démonstration.* Puisque $\mathrm{Spec}\,A/N$ est homéomorphe à $\mathrm{Spec}\,A$, on peut supposer que A est réduit, c'est-à-dire que A n'a pas d'élément nilpotent non nul.

Supposons que A soit intègre. Si X était réductible, il s'écrirait $X = X_1 \cup X_2$, où $X_1 = V(\mathfrak{a}_1)$ et $X_2 = V(\mathfrak{a}_2)$ sont deux fermés distincts de X. Ainsi, les idéaux $\mathfrak{a}_i$ ne sont pas réduit à $\{0\}$, et $\mathfrak{a}_1 \cap \mathfrak{a}_2 = 0$. Il existe donc $f_i \in \mathfrak{a}_i$ non nuls, et alors $f_1 f_2 = 0$. Donc A n'est pas intègre.

Réciproquement supposons que A ne soit pas intègre. On peut alors trouver deux éléments non nuls $f, g \in A$ non nuls et dont le produit est nul. Alors $X = V(f) \cup V(g)$ ; puisque A n'a pas d'élément nilpotent, les fermés $V(f)$ et $V(g)$ sont distincts de X; donc X est réductible. □

Exercice 2.3

Soit $k$ un corps algébriquement clos, $A = k[X_1, \ldots, X_n]$ l'algèbre des polynômes. Pour tout fermé algébrique $Y \subset k^n$, on désigne par I(Y) l'idéal de $k[X_1, \ldots, X_n]$ des polynômes s'annulant sur Y.

(i) Un fermé algébrique $Y \subset k^n$ est irréductible si et seulement si l'algèbre quotient A/I(Y) est intègre.

(ii) L'espace topologique $k^n$, muni de la topologie de Zariski, est irréductible.

Propriétés

1. L'adhérence d'une partie irréductible d'un espace topologique X est irréductible.
2. La réunion de deux ouverts irréductibles qui se rencontrent est irréductible.
3. L'image d'un espace topologique irréductible par une application continue est irréductible.
4. Soit A un anneau, et $\mathfrak{p}$ un idéal premier de A. Alors $V(\mathfrak{p})$ est un fermé irréductible de $\mathrm{Spec}\,A$, et l'application $\mathfrak{p} \mapsto V(\mathfrak{p})$ de l'ensemble des idéaux premiers de A dans l'ensemble des fermés irréductibles est bijective.

DÉFINITION 2.10. — *Soit* X *un espace topologique noethérien. Une composante irréductible de* X *est un fermé irréductible maximal.*

THÉORÈME 2.11. — *Soit* X *une espace topologique noethérien.*

(i) *L'ensemble des composantes irréductibles de* X *est fini.*

(ii) *Soient* $X_1, \ldots, X_m$ *ces composantes irréductibles. Alors*

$$X = X_1 \cup \ldots \cup X_m$$

*et tout fermé irréductible de* X *est contenu dans une des composantes irréductibles.*

*Démonstration.* On va montrer d'abord que tout fermé $Y \subset X$ non vide s'écrit comme réunion finie de fermés irréductibles. Sinon, l'espace topologique X étant noethérien, l'ensemble $\mathcal{F}$ des fermés non vides qui ne satisfont pas à cette condition aurait un élément minimal Y ; alors Y ne serait pas irréductible : il pourrait donc s'écrire $Y = Y_1 \cup Y_2$, où $Y_1$ et $Y_2$ sont deux fermés irréductibles distincts de Y. Mais alors soit $Y_1 \in \mathcal{F}$, soit $Y_2 \in \mathcal{F}$, ce qui contredit la minimalité de F.

En particulier, $X = X_1 \cup \ldots \cup X_m$, avec $X_i$ irréductible, et on peut supposer de plus que $X_i$ n'est pas contenu dans $X_j$ pour $i \neq j$. Si Y est un fermé irréductible, on a alors

$$Y = \cup_{i=1}^{m} (Y \cap X_i)$$

et il résulte de la définition de l'irréductibilité qu'il existe un indice $i$ tel que $Y \subset X_i$. En particulier, si Y est une composante irréductible de X, $Y = X_i$. Ainsi, l'ensemble $\mathcal{C}$ des composantes irréductibles de X est contenu dans $\{X_1, \ldots, X_m\}$, ce qui prouve (1). Réciproquement, pour tout $i$, $X_i$ est une composante irréductible, car si Y est un fermé irréductible tel que $X_i \subset Y$, on peut trouver $j$ tel que $X_i \subset Y \subset X_j$ et alors $i = j$. Donc $\mathcal{C} = \{X_1, \ldots, X_m\}$ : les $X_i$ sont exactement les composantes irréductibles de X. □

La deuxième partie de la démonstration a montré en fait comment reconnaître les composantes irréductibles de X :

PROPOSITION 2.12. — *Soit* X *un espace topologique noethérien et* $X_1, \ldots, X_m$ *des fermés irréductibles de* X *satisfaisant aux conditions suivantes*
(i) $X = X_1 \cup \ldots \cup X_m$ ;
(ii) *pour* $i \neq j$, $X_i \not\subset X_j$.
*Alors les* $X_i$ *sont les composantes irréductibles de* X.

L'énoncé ci-dessus s'applique en particulier à l'espace topologique Spec A quand A est noethérien. Dans la correspondance entre idéaux premiers de A et composantes irréductibles, les composantes irréductibles correspondent aux idéaux premiers minimaux. Le théorème ci-dessus peut donc se lire :

COROLLAIRE 2.13. — *Soit* A *un anneau noethérien, de radical nilpotent* N.
(i) *L'anneau* A *n'a qu'un nombre fini d'idéaux premiers minimaux.*
(ii) *Soient* $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ *les idéaux premiers minimaux. On a*

$$N = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_m$$

Exercice 2.4
Retrouver l'énoncé ci-dessus en raisonnant directement sur les idéaux de A.

La proposition qui suit permet de reconnaître les idéaux premiers minimaux :

PROPOSITION 2.14. — *Soient* A *un anneau noethérien de radical nilpotent* N, *et* $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ *des idéaux premiers tels que*
(i) $N = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_m$
(ii) *pour* $i \neq j$, *on a* $\mathfrak{p}_i \not\subset \mathfrak{p}_j$. *Alors les idéaux* $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ *sont les idéaux premiers minimaux de* A.

*Démonstration.* Ceci résulte de la proposition 2.12. On peut aussi raisonner directement : il résulte de (i) que tout idéal premier $\mathfrak{p}$ contient l'un des $\mathfrak{p}_i$. Si $\mathfrak{p}$ est minimal, c'est donc l'un des idéaux $\mathfrak{p}_i$. Réciproquement, chaque $\mathfrak{p}_i$ est bien minimal, car si $\mathfrak{p} \subset \mathfrak{p}_i$, on trouverait un indice $j$ tel que $\mathfrak{p}_j \subset \mathfrak{p} \subset \mathfrak{p}_i$. Donc $i = j$ et $\mathfrak{p}_i = \mathfrak{p}$. □

### 2.3. Idéaux premiers associés

On se donne un anneau noethérien A et un A−module M.

DÉFINITION 2.15. — *Un idéal premier* $\mathfrak{p}$ *de* A *est dit associé à* M *s'il est l'annulateur d'un élément* $x$ *de* M :

$$\mathfrak{p} = \mathrm{Ann}\,(x) = \{a \in A, ax = 0\}.$$

On désigne par Ass(M) l'ensemble des idéaux premiers associés à M.

PROPOSITION 2.16. — *Soit* M *un* A−*module non nul,* $\mathfrak{p}$ *un idéal maximal parmi les annulateurs d'éléments non nuls de* M. *Alors* $\mathfrak{p}$ *est un idéal premier.*

*Démonstration.* Soient $a, b \in A$ tels que $ab \in \mathfrak{p}$ et $b \notin \mathfrak{p}$. L'idéal $\mathfrak{p}$ est par définition l'annulateur d'un élément $x \in M$. On a donc $abx = 0$, et $bx \neq 0$. Par suite, $a$ appartient à $\mathrm{Ann}\,(bx) \supset \mathrm{Ann}\,(x) = \mathfrak{p}$ : par maximalité, ces deux idéaux sont égaux. Donc $a \in \mathfrak{p}$. □

COROLLAIRE 2.17. — *Si* A *est un anneau noethérien, tout* A−*module non nul* M *a au moins un idéal premier associé.*

COROLLAIRE 2.18. — *Soit* A *un anneau noethérien. Soit* M *un* A−*module de type fini, non nul. Alors* M *a une filtration croissante*

$$\{0\} = \mathrm{M}_0 \subset \mathrm{M}_1 \subset \ldots \subset \mathrm{M}_k = \mathrm{M}$$

*telle que* $\mathrm{M}_i/\mathrm{M}_{i-1}$ *soit un module isomorphe à* $\mathrm{A}/\mathfrak{p}_i$ *où* $\mathfrak{p}_i$ *est un idéal premier.*

*Démonstration.* En effet, puisque M est un module noethérien, il a un sous-module N, maximal parmi les sous-modules qui satisfont à la propriété de la proposition. Si $\mathrm{N} \neq \mathrm{M}$, le module quotient M/N aurait un idéal premier associé $\mathfrak{p}$, c'est l'annulateur d'un élément $x \in \mathrm{M}/\mathrm{N}$ : l'image réciproque du sous-module de M/N engendré par $x$ est un sous-module N′ qui contient strictement N, et qui satisfait encore à la propriété de l'énoncé. Ceci contredit la définition de N. Donc $\mathrm{M} = \mathrm{N}$.

PROPOSITION 2.19. — *Soit* $0 \to \mathrm{M}' \to \mathrm{M} \to \mathrm{M}'' \to 0$ *une suite exacte de* A−*modules. On a*

$$\mathsf{Ass}(\mathrm{M}') \subset \mathsf{Ass}(\mathrm{M}) \subset \mathsf{Ass}(\mathrm{M}') \cup \mathsf{Ass}(\mathrm{M}'').$$

*Démonstration.* La première inclusion est évidente. Montrons la seconde : soit $\mathfrak{p}$ un idéal premier associé à M : c'est l'annulateur d'un élément $x \in \mathrm{M}$. Si $\mathrm{A}x \cap f(\mathrm{M}') = \{0\}$, la projection $g : \mathrm{A}x \to \mathrm{M}''$ est injective, et par conséquent $\mathfrak{p}$ est l'annulateur de $g(x)$. Si $\mathrm{A}x \cap f(\mathrm{M}') \neq \{0\}$, il existe $a \in \mathrm{A}$ tel que $ax = f(x')$ soit non nul. L'annulateur de $x'$ est l'idéal des éléments $b \in \mathrm{A}$ tels que $bax = 0$, donc tels que $ab \in \mathfrak{p}$. Puisque $ax \neq 0$, $a \notin \mathfrak{p}$, cet idéal est exactement $\mathfrak{p}$. Donc $\mathfrak{p} \in \mathsf{Ass}(\mathrm{M}')$. □

COROLLAIRE 2.20. — *Soit* A *un anneau noethérien. Si* M *est un* A−*module de type fini, l'ensemble* $\mathsf{Ass}(\mathrm{M})$ *est fini.*

*Démonstration.* En vertu du corollaire 2.18 et de la proposition qu'on vient de voir, il suffit de montrer que $\mathsf{Ass}(\mathrm{A}/\mathfrak{p})$ est réduit à $\{\mathfrak{p}\}$. Mais ceci résulte de la définition d'un idéal premier. □

THÉORÈME 2.21. — *Soit* A *un anneau noethérien,* M *un* A−*module de type fini. On désigne, pour* $a \in \mathrm{A}$, *par* $\lambda_a : \mathrm{M} \to \mathrm{M}$ *l'homothétie de rapport* $a$.

(1) *L'application linéaire* $\lambda_a$ *est injective si et seulement si* $a$ *n'appartient à aucun idéal premier associé à* M.
(2) *L'application linéaire* $\lambda_a$ *est nilpotente si et seulement si* $a$ *appartient à tous les idéaux premiers associés à* M.

*Démonstration.* Par définition, si $a$ appartient à l'un des idéaux premiers associés à M, $a$ appartient à l'annulateur d'un élément $x \in \mathrm{M}$. Réciproquement, si $\lambda_a$ n'est pas injective, le noyau de $\lambda_a$ est un sous-module non nul de M, qui a donc un idéal premier associé $\mathfrak{p}$. Alors $a$ appartient à $\mathfrak{p}$, et cet idéal premier fait partie des idéaux premiers associés de M. Ceci démontre l'assertion (1).

(2) Supposons que $\lambda_a$ soit nilpotente ; considérons un entier $n \geq 1$ tel que $\lambda_{a^n}=0$. Alors pour tout idéal premier associé $\mathfrak{p}$ de M, on a $a^n \in \mathfrak{p}$. Par suite $a \in \mathfrak{p}$. Réciproquement, soit $a \in \mathrm{M}$ un élément de M appartenant à tous les idéaux premiers associés à M. Considérons la partie multiplicative S de A constituée des puissances de $a$, et le module des fractions $\mathrm{M}_a = \mathrm{S}^{-1}\mathrm{M}$. Si $\lambda_a$ n'est pas nilpotente, le fait que M est de type fini implique que le module $\mathrm{M}_a$ est non nul, et a donc des idéaux premiers associés. Un tel idéal premier $\mathfrak{p}$ ne rencontre pas S, et c'est l'annulateur d'une fraction $\frac{x}{1}$, avec $x \in \mathrm{M}$. Or, on a évidemment

$$\cup_{n\in\mathbb{N}} \mathrm{Ann}\,(a^n x) = \mathfrak{p}$$

La suite d'idéaux $\mathrm{Ann}\,(a^n x)$ est une suite croissante, qui est donc stationnaire. Ainsi, $\mathfrak{p}$ est l'annulateur d'un élément de la forme $a^n x$. Par suite, $\mathfrak{p} \in \mathsf{Ass}(\mathrm{M})$ et d'aaprès l'hypothèse, $a$ devrait appartenir à $\mathfrak{p}$, ce qui fournit une contradiction. □

*Exemple.*
Soit A un anneau factoriel, et un élément $a \in A$. Considérons la décomposition de $a$ en produit de facteurs irréductibles

$$a = up_1^{r_1} \dots p_n^{r_n}$$

avec $u$ inversible. Alors les idéaux premiers associés de $M = A/(a)$ sont les idéaux $\mathfrak{a}_i = (p_i)$. L'idéal des éléments nilpotents est l'idéal engendré par $(p_1 \dots p_n)$.

*Relations avec le support*

DÉFINITION 2.22. — *Etant donné un* A*−module* M*, on appelle support de* M *l'ensemble des idéaux premiers* $\mathfrak{p}$ *de* A *tels que* $M_\mathfrak{p} \neq 0$.

PROPOSITION 2.23. — *L'idéal premier* $\mathfrak{p}$ *appartient au support de* M *si et seulement si il existe* $x \in M$ *tel que* $\mathrm{Ann}\,(x) \subset \mathfrak{p}$.

*Démonstration.* Dire que $M_\mathfrak{p}$ est non nul signifie qu'il existe une fraction $\frac{x}{1}$ non nulle. Ceci équivaut à $sx \neq 0$ pour tout $s \notin \mathfrak{p}$, *i.e.* $\mathrm{Ann}\,(x) \subset \mathfrak{p}$. □

En particulier, les idéaux premiers associés font partie du support de M. Soit Supp (M) le support de M. Si M est un A−module de type fini, de générateurs $e_1, \dots, e_n$, le support de M est la réunion des fermés $V(\mathrm{Ann}\, e_i)$; c'est donc un fermé de Spec A.

Rappelons qu'étant donné un fermé F de Spec A, I(F) désigne l'intersection des idéaux premiers $\mathfrak{p} \in F$. Cet idéal est égal à son radical, et la correspondance $F \mapsto I(F)$ qui associe à un fermé F l'idéal I(F) est une bijection de l'ensmble des fermés de Spec A sur l'ensemble des idéaux de A égaux à leur radical. L'inverse est obtenu en associant à tout idéal $\mathfrak{a}$ de A égal à son radical le fermé $V(\mathfrak{a}) = \{\mathfrak{p} \in \mathrm{Spec}\, A, \mathfrak{a} \subset \mathfrak{p}\}$. L'annulateur d'un A−module M est le noyau de l'homomorphisme d'anneaux $A \longrightarrow \mathrm{Hom}_A(M, M)$ défini par $a \mapsto \lambda_a$.

COROLLAIRE 2.24. — *Soit* M *est un* A*−module de type fini.*

$$\mathrm{Rad}(\mathrm{Ann}\, M) = I(\mathrm{Supp}\, M) = \cap_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$$

*Démonstration.* Le radical de Ann (M) est l'idéal des $a \in A$ tels que l'homothétie $\lambda_a$ de rapport $a$ soit nilpotente. Si $\lambda_a$ est nilpotente, pour $n$ entier convenable, $a^n$ appartient à l'annulateur d'un élément $x \in M$. Par suite, il appartient à tout idéal premier $\mathfrak{p}$ faisant partie du support de M. L'inclusion $I(\mathrm{Supp}\, M) = \cap_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$ est évidente puisque Ass(M) ⊂ Supp M. Réciproquement, si $a$ appartient à la dernière intersection, il appartient à tout idéal premier associé. Donc, d'après le théorème 2.21, $\lambda_a$ est nilpotente. □

Puisque les idéaux figurant dans les égalités ci-dessus sont égaux à leur radical, on obtient un énoncé équivalent en termes de fermés de Spec A :

COROLLAIRE 2.25. — *Soit* M *un* A*−module de type fini. On a dans* Spec A

$$V(\mathrm{Ann}\, M) = \mathrm{Supp}\, M = \cup_{\mathfrak{p} \in \mathrm{Ass}(M)} V(\mathfrak{p})$$

*Démonstration.* L'énoncé est une conséquence immédiate des propriétés du fermé $V(\mathfrak{a})$ vues au §2.1, et du corollaire ci-dessus. □

Considérons dans Ass(M) l'ensemble $\mathrm{Ass}_0(M)$ des idéaux premiers associés minimaux. On a encore

$$\mathrm{Supp}\, M = \cup_{\mathfrak{p} \in \mathrm{Ass}_0(M)} V(\mathfrak{p})$$

Il résulte de la proposition 2.12 que les fermés irréductibles $V(\mathfrak{p})$ ainsi obtenus sont les composantes irréductibles du support. Les autres fermés irréductibles $V(\mathfrak{p})$ s'appellent les *composantes immergées* ou *plongées*. On dit aussi que les idéaux premiers associés qui ne sont pas minimaux dans Ass(M) sont les idéaux premiers immergés de M.

COROLLAIRE 2.26. — *Soit un* A*−module* M *de type fini, non nul, sur un anneau* A*−noethérien. Alors les assertions suivantes sont équivalentes*
(1) *L'ensemble* $\mathsf{Ass}(\mathrm{M})$ *est réduit à un point* $\mathfrak{p}$.
(2) *Pour tout* $a \in \mathrm{A}$ *l'homothétie* $\lambda_a$ *est ou injective, ou nilpotente.*

DÉFINITION 2.27. — *Soient* M *un* A*−module de type fini sur un anneau noethérien* A *et* N *un sous-module de* M. *Si* $\mathsf{Ass}(\mathrm{M/N})$ *est réduit au point* $\mathfrak{p}$, *on dit que* N *est* $\mathfrak{p}$*−primaire dans* M.

En particulier, un idéal $\mathfrak{q}$ de A est primaire si les seuls diviseurs de zéro de l'anneau quotient $\mathrm{A}/\mathfrak{q}$ sont les éléments nilpotents. Autrement dit, si $xy \in \mathfrak{q}$ et $x \notin \mathfrak{q}$, il existe un entier $n$ tel que $y^n \in \mathfrak{q}$. Le seul idéal premier associé à $\mathrm{A}/\mathfrak{q}$ est alors le radical de $\mathfrak{q}$.

*Exemples*
1. Soit A un anneau factoriel. Soit $p$ un élément irréductible de A ; l'idéal $\mathfrak{q} = (p^n)$ est primaire de radical $\mathfrak{p} = (p)$.
2. Soit $\mathfrak{m}$ un idéal maximal de A. Alors les idéaux $\mathfrak{m}$−primaires sont les idéaux $\mathfrak{q}$ pour lesquels il existe un entier $n$ tel que

$$\mathfrak{m}^n \subset \mathfrak{q} \subset \mathfrak{m}$$

En effet, puisque A est noethérien, le fait que $\mathsf{Rad}\,\mathfrak{q} = \mathfrak{m}$ entraîne bien l'existence d'un tel entier. Dans l'autre sens, les idéaux premiers associés de $\mathrm{A}/\mathfrak{q}$ sont des idéaux premiers contenant $\mathfrak{q}$ : mais un tel idéal premier contient $\mathfrak{m}^n$, et donc il contient forcément $\mathfrak{m}$. Par suite $\mathsf{Ass}(\mathrm{A}/\mathfrak{q}) = \{\mathfrak{m}\}$.
3. Soit $\mathfrak{p}$ un idéal premier de A. L'idéal $\mathfrak{p}^n$ dont le radical est $\mathfrak{p}$, n'est pas obligatoirement un idéal $\mathfrak{p}$−primaire. Considérons par exemple l'anneau quotient

$$\mathrm{A} = k[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]/(\mathrm{XY} - \mathrm{Z}^2)$$

et notons x,y,z les classes de X,Y,Z respectivement. Alors l'idéal $\mathfrak{p} = (x, z)$ est premier puisque le quotient $\mathrm{A}/\mathfrak{p}$ est isomorphe à $k[\mathrm{Y}]$ qui est intègre. Dans le quotient $\mathrm{A}/\mathfrak{p}^2$ l'image de $y$ est un diviseur de 0, mais ce n'est pas un élément nilpotent.

Exercice 2.5
Déterminer, dans l'exemple ci-dessus, les idéaux premiers associés de $\mathrm{A}/\mathfrak{p}^2$.

PROPOSITION 2.28. — *Soit* M *un* A*−module de type fini sur un anneau noethérien* A. *Soit* $(\mathrm{M}_i)_{i\in\mathrm{I}}$ *une famille finie non vide de sous-modules* $\mathfrak{p}$*−primaires dans* M. *Alors l'intersection* $\mathrm{N} = \cap_{i\in\mathrm{I}}\mathrm{M}_i$ *est* $\mathfrak{p}$*−primaire dans* M.

*Démonstration.* On a un plongement

$$\mathrm{M/N} \hookrightarrow \oplus_{i\in\mathrm{I}}\mathrm{M/M}_i$$

et $\mathrm{M} \neq \mathrm{N}$. Donc $\mathsf{Ass}(\mathrm{M/N}) = \{\mathfrak{p}\}$. □

### 2.4. Décomposition primaire

THÉORÈME 2.29. — *(Existence) Soient* M *un* A*−module de type fini sur un anneau noethérien* A, *et* $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ *les idéaux premiers associés à* M. *Il existe pour chaque* $i$ *un sous-module* $\mathrm{M}_i$ *de* M *tels que* $\mathrm{M}_i$ *soit* $\mathfrak{p}_i$*−primaire dans* M, *et tel que*

$$\{0\} = \cap_{i=1}^{m}\mathrm{M}_i.$$

Autrement dit, l'application linéaire canonique

$$\varphi : \mathrm{M} \longrightarrow \oplus_{i=1}^{m}\,\mathrm{M/M}_i$$

est injective.

*Démonstration.* Montrons l'existence d'un sous-module $M_i$ de M tel que $\mathsf{Ass}(M_i) = \mathsf{Ass}(M) - \{\mathfrak{p}_i\}$ et tel que $\mathsf{Ass}(M/M_i) = \{\mathfrak{p}_i\}$. Ceci implique le résultat : en effet si le noyau de $\varphi$ était non nul, il aurait un idéal premier associé, et on aurait $\mathsf{Ass}(\ker\varphi) \subset \cap_{i=1}^m \mathsf{Ass}(M_i)$, ce qui fournit une contradiction. Soit $\mathfrak{p}$ un des idéaux premiers associés de M. Considérons l'ensemble $\mathfrak{E}$ des sous-modules N de M tels que $\mathfrak{p} \notin \mathsf{Ass}(N)$. Cet ensemble est non vide et a donc, puisque M est noethérien, il a un élément maximal N. Montrons qu'alors $\mathsf{Ass}(M/N) = \{\mathfrak{p}\}$, ce qui entraînera le résultat en vertu de la proposition 2.19 . Soit $\mathfrak{q} \in \mathsf{Ass}(M/N)$. Alors $\mathfrak{q}$ est l'annulateur d'un élément $x \neq 0$ de M/N ; l'image réciproque N′ du sous-module engendré par $x$ contient strictement N et on a $\mathsf{Ass}(N') \subset \mathsf{Ass}\,N \cup \{\mathfrak{q}\}$. Donc puisque N est maximal dans $\mathfrak{E}$, le sous-module N′ n'appartient pas à $\mathfrak{E}$ et on a obligatoirement $\mathfrak{q} = \mathfrak{p}$. □

La décomposition ci-dessus s'appelle une décomposition primaire de $\{0\}$ dans M. Quand on prend pour M le quotient $A/\mathfrak{a}$ de A par un idéal $\mathfrak{a}$ on obtient en particulier le résultat suivant :

COROLLAIRE 2.30. — *Soit* A *un anneau noethérien,* $\mathfrak{a}$ *un idéal de* A, *et* $(\mathfrak{p}_i)_{i=1,\ldots,m}$ *les idéaux premiers associés à* $A/\mathfrak{a}$. *Il existe pour chaque* $i$ *un idéal* $\mathfrak{p}_i$*−primaire* $\mathfrak{q}_i$ *tels que*

$$\mathfrak{a} = \cap_{i=1}^m \mathfrak{q}_i$$

DÉFINITION 2.31. — *La décomposition ci-dessus s'appelle une décomposition primaire de* $\mathfrak{a}$.

Cet énoncé implique à nouveau $\mathsf{Rad}\,\mathfrak{a} = \cap_{i=1}^m \mathfrak{p}_i$ ce qu'on a déjà vu (*cf.* corollaire 2.24) puisque $\mathfrak{a}$ est l'annulateur du A−module $A/\mathfrak{a}$. On voit que dans cette décomposition, on peut supprimer les termes superflus, et ne garder que les idéaux premiers minimaux parmi les $\mathfrak{p}_i$. Les idéaux premiers qui restent sont les idéaux premiers minimaux contenant $\mathfrak{a}$. Ces idéaux premiers correspondent aux composantes irréductibles de $V(\mathfrak{a})$ ; les autres fermés irréductibles $V(\mathfrak{p}_i) \subset \mathsf{Spec}(A/\mathfrak{a})$ sont les composantes immergées, ou plongées de $A/\mathfrak{a}$.

### 2.5. Unicité

Le problème se pose de reconnaître une décomposition primaire.

THÉORÈME 2.32. — *(Premier théorème d'unicité) Soient* M *un* A*-module de type fini, et* $(M_i)_{i\in I}$ *une famille finie de sous-modules* $\mathfrak{p}_i$*− primaires dans* M *satisfaisant aux conditions suivantes*

(i) $\{0\} = \cap_{i\in I} M_i$

(ii) *les idéaux premiers* $\mathfrak{p}_i$ *sont deux à deux distincts ;*

(iii) *Pour tout* $j \in I$,

$$\bigcap_{i\in I, i\neq j} M_i \neq \{0\}.$$

*Alors les idéaux* $\mathfrak{p}_i$ *sont les idéaux premiers associés à* M.

Un telle décomposition s'appelle une *décomposition primaire minimale* ou *réduite* de $\{0\}$ dans M. La condition (iii) signifie que la famille $M_i$ ne contient pas de termes superflus. C'est évidemment le cas pour la famille obtenue dans le théorème d'existence : car si on supprime un terme dans la décomposition, on supprime aussi un des idéaux premiers associés.

*Démonstration.* La condition (i) signifie que le morphisme canonique

$$M \longrightarrow \oplus_{i\in I} M/M_i$$

est injectif, et par suite $\mathsf{Ass}(M) \subset \{\mathfrak{p}_i, i \in I\}$. Montrons que l'on a égalité : soit $j \in I$; le morphisme canonique

$$M \longrightarrow \oplus_{i\neq j} M/M_j$$

n'est plus injectif d'après la condition (iii). Ce noyau se plonge dans $M/M_j$ et par conséquent $\mathfrak{p}_j$ est un idéal premier associé à ce noyau donc à M. Ainsi, $\mathsf{Ass}(M) = \{\mathfrak{p}_i, i \in I\}$. □

En appliquant ce résultat au quotient $A/\mathfrak{a}$ d'un anneau noethérien par un idéal $\mathfrak{a}$ on obtient

COROLLAIRE 2.33. — *Soit* $\mathfrak{a}$ *un idéal propre d'un anneau noethérien* A, *et* $\mathfrak{q}_i$ *une famille finie d'idéaux* $\mathfrak{p}_i-$*primaires telle que*

(i) $\mathfrak{a} = \cap_{i\in I}\mathfrak{q}_i$

(ii) *Les idéaux premiers* $\mathfrak{p}_i$ *sont deux à deux distincts ;*

(iii) *pour tout* $j \in I$,

$$\mathfrak{a} \neq \bigcap_{i\in I, j\neq i} \mathfrak{q}_i$$

*Alors les idéaux premiers* $\mathfrak{p}_i$ *sont les idéaux premiers associés de* $A/\mathfrak{a}$.

Exemple

Soit $k$ un corps. Dans $A = k[X, Y]$, on a

$$(X^2, XY) = (X, Y)^2 \cap (X) = (X^2, Y) \cap (X)$$

Les idéaux $(X, Y)^2$ et $(X^2, Y)$ sont des idéaux primaires de $k[X, Y]$ de radical $(X, Y)$; l'idéal $(X)$ est un idéal premier. Ces idéaux premiers sont les idéaux premiers associés de $A/(X^2, XY)$.

Exercice 2.6

Soit A un anneau noethérien réduit. Montrer qu'il n'y a pas de composante immergée, autrement dit que les seuls idéaux premiers associés à A sont les idéaux premiers minimaux.

Exercice 2.7

Soit A un anneau noethérien, et M un $A-$module de type fini. Soit $\mathfrak{a} = \mathrm{Ann}(M)$ l'annulateur de M. Montrer que $\mathsf{Ass}(A/\mathfrak{a}) \subset \mathsf{Ass}(M)$.

Exercice 2.8

Démontrer le lemme de Nakayama : soient A un anneau local d'idéal maximal $\mathfrak{m}$, et M un $A-$module de type fini tel que $M = \mathfrak{m}M$. Alors $M = 0$.

Exercice 2.9

Soit A un anneau noethérien, et M un $A-$module de type fini non nul. Soit $\mathsf{End}(M)$ le module des endomorphismes de M.

1. Démontrer que $\mathsf{End}(M)$ se plonge dans $M^n$, pour $n$ convenable. En déduire que $\mathsf{Ass}(\mathsf{End}(M)) \subset \mathsf{Ass}(M)$.

2. Montrer que si $\mathfrak{q}$ est un idéal premier de A appartenant au support de M, il existe un homomorphisme non nul $M \longrightarrow A/\mathfrak{q}$ (On pourra commencer par le cas où A est un anneau local et où $\mathfrak{q}$ est l'idéal maximal $\mathfrak{m}$ de A ; remarquer que dans ce cas $M/\mathfrak{m}M$ est un $A/\mathfrak{m}-$espace vectoriel non nul en appliquant le lemme de Nakayama. Dans le cas où $\mathfrak{q}$ est quelconque, on se ramène au cas précédent par localisation.)

3. Soit $\mathfrak{p} \in \mathsf{Ass}(M)$. Montrer qu'il existe un homomorphisme $M \longrightarrow M$ dont l'image est isomorphe à un sous-module de $A/\mathfrak{p}$. En déduire que $\mathsf{Ass}(M) = \mathsf{Ass}(\mathsf{End}(M))$.

THÉORÈME 2.34. — *(Deuxième théorème d'unicité) Soit* M *un module de type fini sur un anneau noethérien* A, *et soit* $\{0\} = \cap_{i\in I} M_i$ *une décomposition primaire minimale de* $\{0\}$ *dans* M, *et* $\mathfrak{p}_i$ *l'idéal premier associé à* $M/M_i$. *Si* $\mathfrak{p}_i$ *est minimal dans* $\mathsf{Ass}(M)$, *le sous-module* $M_i$ *est le noyau du morphisme canonique*

$$M \xrightarrow{u} M_{\mathfrak{p}_i}$$

Ainsi, la composante primaire correspondant à un élément minimal de $\mathsf{Ass}(M)$ est parfaitement déterminée. Comme on l'a vu dans l'exemple ci-dessus, il n'en va pas de même des composantes primaires correspondant aux idéaux premiers immergés. La démonstration dépend de l'étude du comportement des idéaux associés par localisation. Cet énoncé dit simplement que dans la localisation disparaissent les idéaux premiers associés qui rencontrent la partie multiplicative :

LEMME 2.35. — *Soient* S *une partie multiplicative d'un anneau noethérien et* M *un* A−*module de type fini. Alors un idéal premier* $\mathfrak{p} \in \operatorname{Spec} A$ *est associé au* A−*module* $S^{-1}M$ *si et seulement si* $\mathfrak{p}$ *est associé à* M *et ne rencontre pas* S.

*Démonstration.* Remarquons tout d'abord que si $x \in M$, l'annulateur dans A de la fraction $\frac{x}{1}$ est la réunion des annulateurs des éléments $sx$, quand $s$ parcourt S. Si $\mathfrak{p}$ est associé à M, c'est l'annulateur d'un élément $x \in M$. Si en outre $\mathfrak{p}$ ne rencontre pas S l'annulateur de $sx$ est exactemmment $\mathfrak{p}$ et par suite, $\mathfrak{p}$ est aussi l'annulateur de la fraction $\frac{x}{1}$. Donc $\mathfrak{p} \in \operatorname{Ass}(S^{-1}M)$. Inversement, supposons que $\mathfrak{p} \in \operatorname{Spec} A$ soit l'annulateur de la fraction $\frac{x}{1}$. Alors $\mathfrak{p}$ ne rencontre pas S, sinon cette fraction serait nulle. Soient $a_1, \ldots, a_n$ des générateurs de $\mathfrak{p}$. Pour tout $i = 1, \ldots, n$ il existe un élément $s_i \in S$ tel que $s_i a_i x = 0$. Soit $s = s_1 \ldots s_n$. Il en résulte

$$\mathfrak{p} \subset \cup_{i=1}^{n} \operatorname{Ann}(s_i x) \subset \operatorname{Ann} sx$$

et le dernier terme est contenu dans $\mathfrak{p}$. Donc $\mathfrak{p} = \operatorname{Ann} sx$, et par suite $\mathfrak{p} \in \operatorname{Ass}(M)$. □

*Démonstration du théorème 2.34*

Contemplons le diagramme commutatif obtenu par localisation en $\mathfrak{p}_i$ de la projection canonique $M \xrightarrow{f} M/M_i$ :

$$\begin{array}{ccccc} M & \xrightarrow{f} & M/M_i & & \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} & & \\ (M_i)_{\mathfrak{p}_i} & \longrightarrow & M_{\mathfrak{p}_i} & \xrightarrow{g} & (M/M_i)_{\mathfrak{p}_i} \end{array}$$

et rappelons que localiser en un point $\mathfrak{p}_i \in \operatorname{Spec} A$ transforme suite exactes de modules en suites exactes. En particulier la seconde ligne est exacte. On va montrer que les applications linéaires $g$ et $v$ sont injectives, ce qui prouvera que $f$ et $u$ ont même noyau. Le sous-module $M_i$ se plonge dans $\oplus_{j \neq i} M/M_j$. Il en résulte que les idéaux associés de $M_i$ sont les idéaux associés de M autres que $\mathfrak{p}_i$. Les idéaux premiers associés de $(M_i)_{\mathfrak{p}_i}$ correspondent aux idéaux premiers associés $\mathfrak{p}_j$ distinct de $\mathfrak{p}_i$ qui sont contenus dans $\mathfrak{p}_i$. Ainsi, si $\mathfrak{p}_i$ est minimal, cet ensemble est vide et par conséquent $(M_i)_{\mathfrak{p}_i} = 0$. Il en résulte que la flèche horizontale $g$ est injective.

Considérons d'autre part le noyau K de la flèche de localisation $v$, s'il n'est pas nul, a pour seul idéal premier associé $\mathfrak{p}_i$. Alors $\mathfrak{p}_i$ serait l'annulateur d'un élément $x \in K$. Mais puisque $x$ est dans le noyau de $v$, il existe $s \notin \mathfrak{p}_i$ tel que $sx = 0$ et par suite $\operatorname{Ann} x \not\subset \mathfrak{p}_i$. Ainsi $\operatorname{Ass}(K) = \emptyset$; on en déduit $K = 0$ et donc $v$ est injective. Par conséquent, l'application $f : M \longrightarrow M_{\mathfrak{p}_i}$ a exactement $M_i$ pour noyau. □

### 2.6. Modules de longueur finie

Soit A un anneau noethérien.

DÉFINITION 2.36. — *Un* A−*module* M *est dit artinien si toute suite décroissante de sous-modules de* M *est sationnaire.*

En particulier, un anneau A est artinien si toute suite décroissante d'idéaux est stationnaire.

*Exemples*
(1) Les groupes finis sont des $\mathbb{Z}$-modules artiniens.
(2) Les corps sont artiniens.
(3) L'anneau des entiers $\mathbb{Z}$ n'est pas artinien.
(4) Si A est un anneau principal, les modules de type fini de torsion sont artiniens.

PROPOSITION 2.37. — *Soit* $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *une suite exacte de* A*−modules. Alors le module* M *est artinien si et seulement si* M′ *et* M″ *sont artiniens.*

*Démonstration.* Supposons M artinien. Alors une suite décroissante $M'_i$ de modules de M′ a pour image par $f$ une suite décroissante de sous-modules de M, donc stationnaire. Il en résulte qu'elle est stationnaire. Si $M''_i$ est une suite décroissante de sous-modules de M″, les images réciproques $M_i = g^{-1}(M_i)$ dans M forment une suite décroissante de sous-modules de M. Cette suite est donc stationnaire, et donc la suite $M''_i = g(M_i)$ est stationnaire.

Réciproquement, supposons les modules M′ et M″ artiniens. Soit $M_i$ une suite décroissante de sous-modules de M. Alors la suite des images $M''_i$ est décroissante, et donc stationnaire. De même la suite $M'_i = M' \cap M_i$ est une suite décroissante de sous-modules de M′, donc stationnaire. La suite exacte

$$0 \to M'_i \to M_i \to M''_i \to 0$$

montre que la suite décroissante $M_i$ est stationnaire. □

*Exemples*

(1) Une somme directe finie de modules artiniens est un module artinien.

(2) Soit A un anneau principal, et $p$ un élément irréductible de A. Alors $A/(p^n)$ est un anneau artinien. En effet, soit $\mathfrak{a}_i$ l'idéal engendré par la classe de $p^i$. Cette suite est décroissante, stationnaire, et le module quotient $\mathfrak{a}_i/\mathfrak{a}_{i+1}$ est isomorphe au corps $A/(p)$. On voit donc par récurrence descendante que $\mathfrak{a}_i$ est artinien.

DÉFINITION 2.38. — *Un* A*-module* M *est dit simple s'il n'est pas nul et s'il n'a pas de sous-module autre que* $\{0\}$ *et lui-même.*

Ceci signifie donc que M est isomorphe à un corps $A/\mathfrak{m}$, avec $\mathfrak{m}$ idéal maximal de A.

DÉFINITION 2.39. — *Soit* M *un* A*−module. Une filtration de Jordan-Hölder de* M *est une suite croissante finie de sous-modules* $M_i$ *de* M

$$0 = M_0 \subset M_1 \subset \ldots \subset M_k = M$$

*tels que* $M_i/M_{i-1}$ *soit un module simple. Le module*

$$\mathrm{gr}(M) = \oplus_{i=1}^{k} M_i/M_{i-1}$$

*s'appelle le gradué de Jordan-Hölder de la filtration, et l'entier* $k$ *la longueur de la filtration.*

THÉORÈME 2.40. —

(1) *Un module* M *a une filtration de Jordan-Hölder si et seulement si il est artinien et noethérien. On dit alors que* M *est de longueur finie.*

(2) *Si* M *est de longueur finie, la classe d'isomorphisme du gradué*

$$\mathrm{gr}(M) = \oplus_i M_i/M_{i-1}$$

*associé à une filtration de Jordan-Hölder ne dépend pas de cette filtration.*

*Démonstration.* Supposons que M ait une filtration de Jordan-Hölder $M_i$. Alors par récurrence sur $i$, on voit en appliquant la proposition 2.37 que $M_i$ est artinien et noethérien.

Réciproquement, si M est noethérien, parmi les sous-modules qui ont une filtration de Jordan-Hölder, il en existe un, disons N, qui est maximal. Si $N \neq M$, le quotient M/N est lui aussi un module artinien non nul ; il a alors un sous-module simple S, car sinon on pourrait construire une suite décroissante de sous-modules qui ne serait pas stationnaire. L'image réciproque $N_1$ de S est

alors évidemment un sous-module de M qui contient strictement N et qui a une filtration de Jordan-Hölder. Ceci contredit la définition de N. Ceci démontre (1). Démontrons (2). Soit $\ell$ la longueur minimum des filtrations de Jordan-Hölder de M. Le raisonnement se fait par récurrence sur $\ell$. Pour $\ell = 1$, le résultat est évident car M est alors un module simple. Supposons maintenant $\ell \geq 2$, et considérons deux filtrations de Jordan-Hölder $M_i$ et $M'_i$ de longueur $\ell$ et $\ell'$ , de gradué gr(M) et gr'(M) respectivement. Considérons l'indice $j$ défini par les conditions $M_1 \subset M'_j$ et $M_1 \not\subset M'_{j-1}$ Considérons l'application linéaire induite

$$M_1 \to M'_j/M'_{j-1}$$

Les deux membres étant des modules simples, ce morphisme non nul est obligatoirement un isomorphisme. Il en découle que l'on a une somme directe $M'_{j-1} \oplus M_1 = M'_j$. Considérons le quotient $\overline{M} = M/M_1$. Les filtrations induites sur ce quotient par les deux filtrations initiales sont encore des filtrations de Jordan-Hölder, dont les gradués respectifs sont isomorphes à

$$\mathrm{gr}(\overline{M}) = \oplus_{i\geq 2}\mathrm{gr}_i(M) \quad ; \quad \mathrm{gr}'(\overline{M}) = \oplus_{i\neq j}\mathrm{gr}'_i(M).$$

Puisque la première filtration de Jordan-Hölder est de longueur $\ell - 1$, on peut appliquer à $M/M_1$ l'hypothèse de récurrence : on obtient que $\ell' - 1 = \ell - 1$, et que les deux gradués ci-dessus sont isomorphes. Par suite, $\ell = \ell'$, et les gradués initiaux, qui s'obtiennent (à l'ordre des facteurs près) en faisant la somme directe avec $M_1 \simeq \mathrm{gr}'_j(M)$, sont eux aussi isomorphes. D'où l'assertion (2). □

COROLLAIRE 2.41. — *Soit* M *un* A*−module de longueur finie. Toutes les filtrations de Jordan-Hölder de* M *sont de même longueur* $\ell$*. Ce nombre* $\ell = \ell(M)$ *s'appelle la longueur de* M.

PROPOSITION 2.42. — *Soit une suite exacte courte de* A*−modules de longueur finie*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

*On a* $\ell(M) = \ell(M') + \ell(M'')$.

*Démonstration.* Soient $\ell' = \ell(M'), \ell'' = \ell(M'')$ et $\ell = \ell' + \ell''$. Soient $(M'_i)_{i=0,\ldots,\ell'}$ une filtration de Jordan-Hölder pour M', et $(M''_i)_{i=\ell'+1,\ldots,\ell}$ une filtration de Jordan-Hölder de M''. On obtient une filtration de Jordan-Hölder de M en posant $M_i = f(M'_i)$ pour $i = 0, \ldots, \ell'$ et $M_i = g^{-1}(M''_i)$ pour $i = \ell' + 1, \ldots, \ell$. Ainsi, $\ell(M) = \ell$. □

*Exemples*

(1) Soit M un espace vectoriel sur un corps $k$. Alors M est de dimension finie si et seulement si M est de longueur finie. On a alors $\ell(M) = \mathsf{dim}_k(M)$.

(2) Soit A un anneau principal, et $p$ un élément irréductible de A. Alors $\ell(A/(p^n)) = n$.

PROPOSITION 2.43. — *Soit* M *un* A*−module de type fini sur un anneau noethérien. Les propriétés suivantes sont équivalentes :*

(i) *Le module* M *est de longueur finie.*

(ii) *Tout idéal premier* $\mathfrak{p} \in \mathsf{Ass}(M)$ *est maximal.*

(iii) *Tout idéal premier* $\mathfrak{p} \in \mathrm{Supp}\,(M)$ *est maximal.*

*Démonstration.* (i)⇒(ii) : Si M est de longueur finie, il a une filtration de Jordan-Hölder, et l'on a $\mathsf{Ass}(M) \subset \cup_i \mathsf{Ass}(\mathrm{gr}_i M)$. Puisque $\mathrm{gr}_i(M)$ est isomorphe à $A/\mathfrak{m}_i$, où $\mathfrak{m}_i$ est un idéal maximal, le seul idéal premier associé à $A/\mathfrak{m}_i$ est $\mathfrak{m}_i$ et on a donc $\mathsf{Ass}(M) \subset \{\mathfrak{m}_i\}$. L'implication (ii)⇒(iii) résulte du fait que le support de M est la réunion des fermés $V(\mathfrak{p})$, où $\mathfrak{p}$ est un idéal premier associé à M. Montrons que (iii)⇒(i). On sait qu'il existe une suite finie croissante $(M_i)_{0\leq i\leq n}$ de sous-modules de M telle que $M_i/M_{i-1}$ soit isomorphe à $A/\mathfrak{p}_i$ où $\mathfrak{p}_i$ est un idéal premier de A. On a alors

$$\mathfrak{p}_i \in \mathrm{Supp}\, M_i \subset \mathrm{Supp}\, M.$$

De l'hypothèse (iii), il résulte que les idéaux $\mathfrak{p}_i$ sont maximaux. Par suite, M est de longueur finie.

COROLLAIRE 2.44. — *Pout tout* A−*module* M *de longueur finie sur un anneau noethérien* A *on a* $\mathsf{Ass}(M) = \mathrm{Supp}\,(M)$.

En effet, pour $\mathfrak{p} \in \mathsf{Ass}(M)$, le fermé $V(\mathfrak{p})$ est alors réduit au point $\mathfrak{p}$.

COROLLAIRE 2.45. — *Soit* A *un anneau noethérien. Les assertions suivantes sont équivalentes :*
(i) *L'anneau* A *est artinien.*
(ii) *Les seuls idéaux premiers de* A *sont les idéaux maximaux.*
(iii) *L'espace topologique* $\mathsf{Spec}\,A$ *est discret.*
*Si ces conditions sont satisfaites,* $\mathsf{Spec}\,A$ *est fini.*

Le fait que (i) est équivalent à (ii) est une conséquence directe de la proposition, compte-tenu du fait que $\mathsf{Spec}\,A = \mathrm{Supp}\,A$. L'assertion (iii) signifie que tous les points de $\mathsf{Spec}\,A$ sont fermés, autrement dit tous les idéaux premiers sont maximaux. La finitude de $\mathsf{Spec}\,A$ quand A est artinien résulte de l'égalité $\mathsf{Ass}(A) = \mathsf{Spec}\,A$. et du fait que A est noethérien.

Exercice 2.10
Trouver des anneaux non artiniens A tels que $\mathsf{Spec}\,A$ soit fini. (Considérer par exemple, $k$ étant un corps algébriquement clos, le localisé de $k[X]_{\mathfrak{m}}$ en un idéal maximal $\mathfrak{m}$ de $k[X]$).

COROLLAIRE 2.46. — *Soient* M *un* A−*module de type fini sur un anneau noethérien* A, *et* $\mathfrak{p}$ *un idéal premier de* A. *Pour que le localisé* $M_{\mathfrak{p}}$ *soit un* $A_{\mathfrak{p}}$−*module de longueur finie* $\neq 0$, *il faut et il suffit que* $\mathfrak{p}$ *soit un élément minimal de* $\mathsf{Ass}(M)$.

*Démonstration.* Supposons que $\mathfrak{p}$ soit un élément minimal de $\mathsf{Ass}(M)$. Alors $M_{\mathfrak{p}}$ est un $A_{\mathfrak{p}}$−module de longueur finie, et $\mathsf{Ass}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}})$ est réduit à l'idéal $\mathfrak{p}A_{\mathfrak{p}}$ d'après le lemme 2.12. Cet idéal est maximal, donc $M_{\mathfrak{p}}$ est de longueur finie $\neq 0$ sur $A_{\mathfrak{p}}$. Réciproquement, si $M_{\mathfrak{p}}$ est de longueur finie $\neq 0$, le support de M contient $\mathfrak{p}$ ; de plus, $\mathsf{Ass}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}})$ est réduit au point $\mathfrak{p}A_{\mathfrak{p}}$. Il résulte du lemme 2.35 que M n'a pas d'idéal premier associé contenu dans $\mathfrak{p}$ autre que $\mathfrak{p}$. Donc $\mathfrak{p}$ est minimal dans $\mathsf{Ass}(M)$. □

PROPOSITION 2.47. — *Soient* M *un* A−*module de longueur finie sur un anneau noethérien* A.

(i) *Il existe pour tout* $\mathfrak{p} \in \mathsf{Ass}(M)$ *un sous-module primaire* $M(\mathfrak{p})$ *de* M *et un seul tel que l'on ait la décomposition primaire de* $\{0\}$ *dans* M

$$\{0\} = \cap_{\mathfrak{p}\in\mathsf{Ass}(M)} M(\mathfrak{p})$$

(ii) *Si* $n$ *est un entier assez grand, on a* $M(\mathfrak{p}\,) = \mathfrak{p}^n M$ *pour tout* $\mathfrak{p} \in \mathsf{Ass}(M)$.

(iii) *Pour tout* $\mathfrak{p} \in \mathsf{Ass}(M)$, *le morphisme canonique* $M \longrightarrow M_{\mathfrak{p}}$ *est surjectif.*

(iv) *Le morphisme canonique*

$$M \longrightarrow \oplus_{p\in\mathsf{Ass}(M)}\, M/M(\mathfrak{p})$$

*est un isomorphisme.*

Nous aurons besoin du lemme suivant :

LEMME 2.48. — *Soit* M *un* A−*module de longueur finie sur un anneau noethérien* A. *Tout endomorphisme injectif* $f : M \longrightarrow M$ *est bijectif.*

En effet, la suite exacte $0 \longrightarrow M \xrightarrow{f} M \longrightarrow \operatorname{coker} f \longrightarrow 0$ montre que le conoyau coker $f$ est de longueur nulle. Donc il est nul.

*Démonstration de la proposition 2.47.*

La décomposition (i) est évidemment minimale. Puisque chaque $\mathfrak{p} \in \mathsf{Ass}(M)$ est minimal dans Ass(M), il résulte du théorème 2.34 que la composante $\mathfrak{p}-$primaire est déterminée par $\mathfrak{p}$ : c'est le noyau du morphisme $M \longrightarrow M_{\mathfrak{p}}$. Ceci prouve (i). Montrons (ii).Soit $\mathfrak{p} \in \mathsf{Ass}(M)$. Pour tout élément $a \in \mathfrak{p}$ l'homothétie $\lambda_a$ est nilpotente dans $M/M(\mathfrak{p})$. Donc, puisque $\mathfrak{p}$ est de type fini il exsite un entier $n_{\mathfrak{p}}$ tel que pour $n \geq n_{\mathfrak{p}}$, $\mathfrak{p}^n M \subset M(\mathfrak{p})$. Soient $N = \max n_{\mathfrak{p}}$, et $n \geq n_{\mathfrak{p}}$. Les idéaux premiers associés du module $M/\mathfrak{p}^n M$ sont des idéaux premiers contenant $\mathfrak{p}^n$ donc contenant $\mathfrak{p}$. Puisque $\mathfrak{p}$ est un idéal maximal

$$\mathsf{Ass}(M/\mathfrak{p}^n M) = \{\mathfrak{p}\}.$$

Autrement dit $\mathfrak{p}^n M$ est $\mathfrak{p}-$primaire. On a

$$\{0\} = \cap_{p \in \mathsf{Ass}(M)} \mathfrak{p}^n M$$

et de l'unicité de la décomposition primaire, il résulte que $\mathfrak{p}^n M = M(\mathfrak{p})$.

Montrons (iv). Soient $\mathsf{Ass}(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell\}$, et $n$ étant choisi comme ci-dessus, posons $\mathfrak{q}_i = \mathfrak{p}_i^n$. Puisqu'il n'y a pas d'idéal premier contenant $\mathfrak{q}_i$ et $\mathfrak{q}_j$ pour $i \neq j$ on a $\mathfrak{q}_i + \mathfrak{q}_j = A$ et par le même argument, on obtient même pour tout $i$

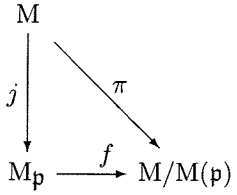
$$\mathfrak{q}_i + \cap_{j \neq i} \mathfrak{q}_j = A.$$

Pour peut alors trouver un élément $e_i \in \cap_{j \neq i} \mathfrak{q}_j$ tel que $1 - e_i \in \mathfrak{q}_i$. Montrons que l'application canonique $M \longrightarrow \oplus_i M/\mathfrak{q}_i M$ est surjective. Soit $x_i \in M$ pour $i = 1, \ldots, \ell$. Posons $x = \sum_i e_i x_i$. On a alors

$$x - x_i = (1 - e_i)x_i + \sum_{j \neq i} e_j x_j$$

et par conséquent $x \equiv x_i \bmod \mathfrak{q}_i M$. D'où la surjectivité.

Il reste à montrer (iii). Si $a \notin \mathfrak{p}$, l'homothétie $\lambda_a$ de $M/M(\mathfrak{p})$ est injective, donc inversible d'après le lemme ci-dessus. Il en résulte que le morphisme de passage au quotient se factorise suivant le diagramme




L'application $f$ est définie pour $x \in M$ et $s \notin \mathfrak{p}$ par

$$f(\frac{x}{s}) = \frac{1}{s}.[x]$$

où $[x]$ désigne la classe de $x$ dans $M/M(\mathfrak{p})$. Puisque $\ker \pi \subset \ker j$, on voit que l'application linéaire $f$ est injective, et par suite inversible. Mais alors $j$ est surjective. □

COROLLAIRE 2.49. — *Un anneau artinien est isomorphe à un produit fini d'anneaux locaux artiniens.*

En effet, soit A un anneau artinien. Si $\mathsf{Ass}(A) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, le morphisme canonique

$$A \longrightarrow \oplus_{i=1}^n A_{\mathfrak{p}_i}$$

est un isomorphisme d'anneaux, et chacun des anneaux $A_{\mathfrak{p}_i}$ est un anneau local artinien.

PROPOSITION 2.50. — *Soient $k$ un corps algébriquement clos et $\mathrm{A} = k[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathfrak{a}$ une $k-$algèbre de type fini. Les assertions suivantes sont équivalentes :*

(i) *L'anneau* A *est un anneau artinien.*

(ii) *Le fermé de $k^n$ défini par* $\mathrm{V}(\mathfrak{a})$ *est fini.*

(iii) *L'algèbre* A *est un $k-$espace vectoriel de dimension finie.*

*Si ces conditions sont satisfaites, on a $\ell(\mathrm{A}) = \dim_k \mathrm{A}$.*

*Démonstration.* (i)⇒ (ii) : On sait que $\mathrm{V}(\mathfrak{a})$ est en bijection avec l'ensemble des idéaux maximaux de A. Puisque Spec A est fini, l'ensemble des idéaux maximaux est fini, et par suite $\mathrm{V}(\mathfrak{a})$ est lui même fini. Réciproquement, si $\mathrm{V}(\mathfrak{a})$ est fini, les composantes irréductibles de $\mathrm{V}(\mathfrak{a})$ sont des points, et correspondent donc aux idéaux maximaux : ainsi tout idéal premier est maximal ce qui implique (i).

Supposons que A soit artinien, et montrons (iii). Si on considère une filtration de Jordan-Hölder de A, le gradué $\mathrm{gr}_i$ est un A−module isomorphe à $\mathrm{A}/\mathfrak{m}$ où $\mathfrak{m}$ est un idéal maximal de A. Cet idéal maximal correspond à un point de $\mathrm{V}(\mathfrak{a})$ et l'algèbre quotient $\mathrm{A}/\mathfrak{m}$ est isomorphe à $k$ d'après le théorème des zéros de Hilbert. Par suite $\dim_k \mathrm{A} < \infty$. De plus, $\ell(\mathrm{A}) = \dim_k \mathrm{A}$.

(iii)⇒ (i) : Soit $\mathfrak{p}$ un idéal premier associé à A. Alors $\mathrm{A}/\mathfrak{p}$ est un $k-$espace vectoriel de dimension finie ; par suite l'anneau intègre $\mathrm{A}/\mathfrak{p}$ est entier sur $k$. Il résulte du lemme 1.17 que $\mathrm{A}/\mathfrak{p}$ est un corps. Donc $\mathfrak{p}$ est un idéal maximal. Ainsi, A est un anneau artinien. □

*Remarque*

Si $k$ n'est plus algébriquement clos, les assertions (i) et (iii) sont encore équivalentes, et impliquent (ii). Par contre, il n'est plus vrai que (ii) implique (i). Par exemple, si $\mathrm{A} = \mathbb{R}[\mathrm{X}, \mathrm{Y}]/(\mathrm{X}^2 + \mathrm{Y}^2)$ on a $\mathrm{V}(\mathrm{X}^2 + \mathrm{Y}^2) = \{0\}$ dans $\mathbb{R}^2$. Pourtant, cet anneau est intègre, et $\{0\}$ est un idéal premier qui n'est pas maximal. Si de plus A est de longueur finie et locale d'idéal maximal $\mathfrak{m}$ on a

$$\dim_k \mathrm{A} = \lg(\mathrm{A})[\mathrm{A}/\mathfrak{m} : k]$$

où $[\mathrm{A}/\mathfrak{m} : k]$ désigne le degré de l'extension finie $k \hookrightarrow \mathrm{A}/\mathfrak{m}$.

## 3. Dimension

### 3.1. Chaînes de fermés irréductibles

Soit X un espace topologique. Une chaîne de fermés irréductibles de longueur $\ell$ de X est une suite strictement croissante

$$X_0 \subsetneqq X_2 \subsetneqq \ldots \subsetneqq X_\ell$$

de fermés irréductibles de X.

DÉFINITION 3.1. — *Soit* X *un espace topologique noethérien. Si les chaînes de fermés irréductibles sont de longueur bornée, on dit que* X *est de dimension de Krull finie. La longueur maximale des chaînes de fermés irréductibles de* X *s'appelle la dimension de Krull de* X.

DÉFINITION 3.2. — *Un anneau* A *est de dimension de Krull finie si l'espace topologique* $X = \mathsf{Spec}\, A$ *est de dimension finie. La dimension de* A *est alors la dimension de* $\mathsf{Spec}\, A$.

En vertu de la correspondance entre fermés irréductibles de $\mathsf{Spec}\, A$ et idéaux premiers, l'anneau A est de dimension de Krull finie si la longueur $\ell$ des chaînes d'idéaux premiers

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_\ell$$

est bornée. La longueur maximale des chaînes d'idéaux premiers est la dimension de Krull de A.

Il n'est pas vrai que les anneaux noethériens sont de dimension de Krull finie. Un des objets de cette section est de prouver que c'est pourtant vrai pour un anneau local noethérien.

*Exemples*

1. Soit A un anneau noethérien. Alors A est de dimension de Krull 0 si et seulement si A est de longueur finie.

2. L'anneau des entiers $\mathbb{Z}$ est de dimension de Krull 1. Si $k$ est un corps, $k[X]$ est de dimension de Krull 1.

3. Si $k$ est un corps, $k[X_1, \ldots, X_n]$ est évidemment de dimension de Krull $\geq n$. On démontrera que cette dimension de Krull est $n$.

4. Si $k$ est un corps algébriquement clos, la dimension de Krull de $k[X_1, \ldots, X_n]$ est aussi la dimension de Krull de $k^n$, muni de la topologie de Zariski. Plus généralement, si $Y \subset k^n$ est un fermé algébrique, I(F) l'idéal des polynômes qui s'annulent sur F, la dimension de Krull de F est la dimension de Krull de l'algèbre $A = k[X_1, \ldots, X_n]/I(F)$, isomorphe à l'algèbre des fonctions $f : F \longrightarrow k$ qui sont restrictions de polynômes. De telles fonctions sont aussi appelées fonctions régulières sur F.

### 3.2. Extensions entières

L'objet de cette section est de démontrer qu'une algèbre de type fini est de dimension de Krull finie. La démonstration repose sur la comparaison des dimension de Krull de deux anneaux dont l'un est entier sur l'autre.

PROPOSITION 3.3. — *Soit* B *un anneau entier sur un sous-anneau* A. *Alors* A *est de dimension finie si et seulement si* B *est de dimension finie, et* $\dim A = \dim B$.

LEMME 3.4. — *Soient* B *un anneau entier sur un sous-anneau* A, *et* $i : A \hookrightarrow B$ *l'inclusion canonique.*

*Considérons l'application continue* $i^* : \mathrm{Spec}\, B \longrightarrow \mathrm{Spec}\, A$.

(i) *L'application* $i^*$ *est surjective.*

(ii) *Les fibres de* $i^*$ *sont de dimension* 0.

(iii) *Le morphisme* $i^*$ *est fermé.*

*Démonstration.* (i) Soit $\mathfrak{p}$ un idéal premier de A. Il s'agit de prouver qu'il existe un idéal premier $\mathfrak{q}$ de B tel que $\mathfrak{q} \cap A = \mathfrak{p}$.

Commençons par le cas où A est un anneau local d'idéal maximal $\mathfrak{p}$. Si $\mathfrak{q}$ est un idéal maximal de B alors le morphisme

$$A/\mathfrak{q} \cap A \hookrightarrow B/\mathfrak{q}$$

est encore entier, et d'après le lemme 1.17 l'anneau quotient $A/\mathfrak{q} \cap A$ est un corps, donc $\mathfrak{q} \cap A$ est un idéal maximal : c'est donc $\mathfrak{p}$. En fait, le même lemme montre que les seuls points de la fibre de $i^*$ au-dessus de l'idéal maximal de A sont les idéaux maximaux de B.

Dans le cas général, on considère le diagramme obtenu en considérant les localisés par rapport la partie multiplicative $A - \mathfrak{p}$ :

$$\begin{array}{ccc} A & \xrightarrow{\ i\ } & B \\ \downarrow & & \downarrow j \\ A_{\mathfrak{p}} & \xrightarrow{\ i_{\mathfrak{p}}\ } & B_{\mathfrak{p}} \end{array}$$

qui induit un diagramme commutatif

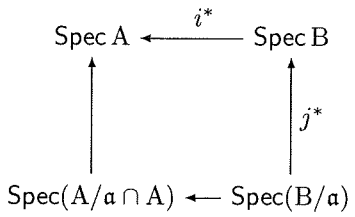
$$\begin{array}{ccc} \mathrm{Spec}\, A & \xleftarrow{\ i^*\ } & \mathrm{Spec}\, B \\ \uparrow & & \uparrow j^* \\ \mathrm{Spec}\, A_{\mathfrak{p}} & \xleftarrow{\ i_{\mathfrak{p}}^*\ } & \mathrm{Spec}\, B_{\mathfrak{p}} \end{array}$$

Le morphisme d'anneaux $A_{\mathfrak{p}} \longrightarrow B_{\mathfrak{p}}$ est encore entier. Considérons le point $\mathfrak{p}A_{\mathfrak{p}} \in \mathrm{Spec}\, A_{\mathfrak{p}}$ . Ce point provient d'un idéal maximal $\mathfrak{m}$ de $B_{\mathfrak{p}}$. D'après le diagramme commutatif ci-dessus, l'idéal premier de B défini par $\mathfrak{q} = j^*(\mathfrak{m})$ convient. Ceci démontre (i).

(ii) Les points de la fibre de $i^*$ au-dessus du point $\mathfrak{p}$ sont les idéaux premiers $\mathfrak{q}$ de B tels que $\mathfrak{q} \cap A = \mathfrak{p}$. Cette fibre est homéomorphe à la fibre de l'application continue $i_{\mathfrak{p}}^*$ : $\mathrm{Spec}\, B_{\mathfrak{p}} \longrightarrow \mathrm{Spec}\, A_p$ au-dessus de l'idéal maximal : on raisonne donc dans le cas où A est un anneau local et $\mathfrak{p}$ l'idéal maximal. Les fermés irréductibles $V(\mathfrak{q})$ contenus dans cette fibre sont forcément donnés par un idéal $\mathfrak{q}$ maximal : par suite la dimension de la fibre est bien nulle.

(iii) Considérons le fermé $V(\mathfrak{a})$, où $\mathfrak{a}$ est un idéal propre de B. On va montrer que $i^*(V(\mathfrak{a})) = V(\mathfrak{a} \cap A)$. Il est clair que $i^*(V(\mathfrak{a})) \subset V(\mathfrak{a} \cap A)$. Montrons l'inclusion dans l'autre sens. Considérons le morphisme injectif $A/\mathfrak{a} \cap A \longrightarrow B/\mathfrak{a}$. Ce morphisme est encore entier. Un point $\mathfrak{p}$ de $V(\mathfrak{a} \cap A)$ définit un idéal premier dans $A/\mathfrak{a} \cap A$. D'après (i), cet idéal premier provient d'un idéal premier

de $B/\mathfrak{a}$. Le diagramme commutatif




montre que l'image de ce point dans Spec B, qui appartient à $V(\mathfrak{a})$ se projette sur le point $\mathfrak{p}$. □

*Remarque*

Dire que la fibre au-dessus de $\mathfrak{p}$ est de dimension 0 revient signifie qu'il n'existe pas de chaîne d'idéaux premiers $\mathfrak{q}$ de longueur 1 satisfaisant à la condition $\mathfrak{q} \cap A = \mathfrak{p}$. En effet, une telle chaîne correspond à une chaîne d'idéaux premiers dans la fibre de $i^*_{\mathfrak{p}}$ au- dessus du point défini par l'idéal maximal.

*Démonstration de la proposition 3.3*

Considérons l'application continue

$$i^* : \mathrm{Spec}\, B \longrightarrow \mathrm{Spec}\, A.$$

Si $\mathfrak{q}$ est un idéal premier de B, on vient de voir que l'image de $V(\mathfrak{p})$ est le fermé irréductible $V(\mathfrak{p} \cap A)$; l'assertion (i) dit que tout fermé irréductible de Spec A est l'image d'un fermé irréductible de Spec B.

L'image d'une chaîne de fermés irréductibles de longueur $\ell$ dans Spec B fournit aussi une chaîne de fermés irréductibles de longueur $\ell$ dans Spec A en vertu de l'assertion (ii). Par suite, si A est de dimension finie, il en est de même de B, et alors $\dim B \leq \dim A$.

Dans l'autre sens, on applique le résultat suivant, qui montre que si B est de dimension finie, il en est de même de A et que l'on a $\dim B \leq \dim A$ :

LEMME 3.5. — *Soit* $Y_0 \subsetneqq Y_2 \subsetneqq \ldots \subsetneqq Y_\ell$ *est une chaîne de fermés irréductibles de* Spec A. *Il existe une chaîne de fermés irréductibles*

$$X_0 \subsetneqq X_1 \subsetneqq \ldots \subsetneqq X_\ell$$

*de* X *telle que* $i^*(X_j) = Y_j$.

On construit les $X_j$ par récurrence descendante sur $j$. En effet, on construit $X_\ell$ de manière arbitraire en appliquant la remarque ci-dessus. Supposons construits les fermés $X_j, \ldots, X_\ell$. Pour construire $X_{j-1} \subset X_j$ on remarque que si $X_j = V(\mathfrak{q}_j)$ et $\mathfrak{p}_j = \mathfrak{q}_j \cap A$ le morphisme induit $X_j \longrightarrow Y_j$ par $i^*$ est celui qui est associé au morphisme d'anneaux

$$A/\mathfrak{p}_j \longrightarrow B/\mathfrak{q}_j$$

Ce morphisme est encore une extension entière : on peut donc trouver un fermé irréductible $X_{j-1} \subset X_j$ tel que $i^*(X_{j-1}) = Y_{j-1}$.

Le principe de construction utilisé ci-dessus, qui consiste à construire la chaîne $X_i$ en commençant par le plus grand des fermés $X_i$ s'appelle dans la littérature "going-up". La terminologie s'explique parce qu'elle est souvent formulée en termes d'idéaux premiers.

PROPOSITION 3.6. — *Soit* A *une algèbre de type fini sur un corps* $k$*, engendrée par* $n$ *éléments. Alors* A *est de dimension de Krull* $\leq n$.

*Démonstration.* On raisonne par récurrence sur le nombre minimal de générateurs de A. Soit $n$ le nombre minimal d'éléments dans un système de générateurs de A, et $x_1, \ldots, x_n$ des générateurs de A définissant un morphisme surjectif

$$\varphi : \mathrm{B} = k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \longrightarrow \mathrm{A}.$$

Si $n = 0$, le résultat est trivial. Considérons une chaîne d'idéaux premiers de A :

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r.$$

Soient $\mathfrak{q}_i$ l'image réciproque de $\mathfrak{p}_i$ par $\varphi$, et $\mathrm{F} \in \mathrm{B}$ un polynôme non nul appartenant à $\mathfrak{q}_1$. D'après le lemme de Nagata, il existe $\mathrm{Y}_2, \ldots, \mathrm{Y}_n$ tels que $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ soit entière sur $\mathrm{B} = k[\mathrm{F}, \mathrm{Y}_2, \ldots, \mathrm{Y}_n]$. L'algèbre $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathfrak{q}_1 = \mathrm{A}/\mathfrak{p}_1$ est entière sur $\mathrm{B}' = \mathrm{B}/\mathrm{B} \cap \mathfrak{q}_1$ et B′ est une algèbre engendrée par $n-1$ éléments. Alors par hypothèse de récurrence, B′ est de dimension de Krull finie, et d'après la proposition 3.3, $\mathrm{A}/\mathfrak{p}_1$ est de dimension finie $\leq n-1$. Par suite, $r - 1 \leq n - 1$, donc $r \leq n$. □

COROLLAIRE 3.7. — *L'algèbre* $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *est de dimension de Krull* $n$.

### 3.3. Degré de transcendance de K(A)

On remarque d'abord que la dimension d'un anneau A est la même que celle du quotient de A par son idéal nilpotent. On est ainsi ramené au cas d'un anneau réduit. De plus, si $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ sont les idéaux premiers minimaux de A, puisque tout idéal premier contient un idéal premier minimal on a

$$\dim \mathrm{A} = \max \dim \mathrm{A}/\mathfrak{p}_i$$

ce qui nous ramène au cas d'un anneau intègre de type fini sur $k$. On se propose de relier la dimension de Krull d'une algèbre de type fini intègre au degré de transcendance du corps des fractions de A. La principale application concerne le calcul de la dimension de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]/(\mathrm{F})$, où F est un polynôme non constant.

*Bases de transcendance*

DÉFINITION 3.8. — *Soit* L *un corps, et* $\mathrm{K} \subset \mathrm{L}$ *un sous-corps de* L*. On dit qu'une partie* $\mathrm{B} \subset \mathrm{L}$ *est une base de transcendance de* L *sur* K *si*

(i) *les éléments de* L *sont algébriquement indépendants sur* K *;*

(ii) *le corps* L *est une extension algébrique du sous-corps engendré par* K *et* B.

LEMME 3.9. — *Soit* $\mathrm{L} = \mathrm{K}(x_1, \ldots, x_r)$ *une extension de* K *engendrée par un nombre fini d'éléments.*

(i) *Le corps* L *a une base de transcendance finie.*

(ii) *Deux bases de transcendance ont le même nombre d'éléments.*

Le nombre d'éléments d'une base de transcendance de L sur K s'appelle degré de transcendance. On le note deg $\mathrm{tr}_{\mathrm{K}}\mathrm{L}$.

*Démonstration.* (i) Un système maximal $\mathrm{B} \subset \{x_1, \ldots, x_r\}$ d'éléments algébriquement indépendants sur K est une base de transcendance de L sur K.

(ii) Soient B et B′ deux bases de transcendance de L sur K, dont l'une au moins est supposée finie. Montrons par récurrence descendante sur le nombre d'éléments $k = \#\mathrm{B} \cap \mathrm{B}'$ que B et B′ ont le même nombre d'éléments. Supposons par exemple B′ finie. Si $\#\mathrm{B} \cap \mathrm{B}' = \#\mathrm{B}'$, on a $\mathrm{B}' \subset \mathrm{B}$ et par définition des bases de transcendance $\mathrm{B} = \mathrm{B}'$. Supposons $\mathrm{B} \neq \mathrm{B}'$. Alors B n'est pas contenu

dans B′ ; soit $b \in \mathrm{B} - \mathrm{B}'$. Alors $\mathrm{B}' \cup \{b\}$ n'est plus une base de transcendance. Donc il existe un système maximal B″ d'éléments algébriquement indépendants tel que

$$(\mathrm{B} \cap \mathrm{B}') \cup \{b\} \subset \mathrm{B}'' \subsetneqq \{b\} \cup \mathrm{B}'.$$

Par définition B″ est une base de transcendance. On a $\#\mathrm{B} \cap \mathrm{B}'' > k$ et donc d'après l'hypothèse de récurrence, B est finie et a même nombre d'éléments que B″; ainsi $\#\mathrm{B} \leq \#\mathrm{B}'$. Si on échange les rôles de B et B′, on obtient que ces bases ont le même nombre d'éléments. □

PROPOSITION 3.10. — *Soit $k$ un corps, et* A *une $k$-algèbre de type fini, intègre. Soit* K(A) *le corps des fractions de* A. *La dimension de Krull de* A *est donnée par*

$$\dim \mathrm{A} = \deg \mathrm{tr}_k \mathrm{K}(\mathrm{A})$$

*Démonstration.* On sait d'après le théorème de normalisation de Noether qu'il existe $x_1, \ldots, x_r$ in A, algébriquement indépendants sur $k$, et tels que l'extension $k[x_1, \ldots, x_r] \subset \mathrm{A}$ soit entière. Alors d'après la proposition 3.3, A est même dimension de Krull que $k[x_1, \ldots, x_r]$ c'est-à-dire $r$ d'après le corollaire ci-dessus. Alors l'extension $k(x_1, \ldots, x_r) \subset \mathrm{K}(\mathrm{A})$ est une extension algébrique. En effet, tout élément $x \in \mathrm{A}$ est évidemment algébrique sur $k(x_1, \ldots, x_r)$; les éléments de K(A) algébriques sur $k$ forment un sous-corps de K(A) : il suffit évidemment de vérifier que si $x \in \mathrm{K}(\mathrm{A})$ est non nul, et algébrique sur $k(x_1, \ldots, x_r)$, l'inverse $\frac{1}{x}$ est algébrique sur $k(x_1, \ldots, x_r)$. Mais $x$ est entier sur $k(x_1, \ldots, x_r)$ il satisfait à une équation

$$x^n + a_i x^{n-1} + \ldots + a_n = 0$$

de degré minimal avec $a_i \in k[x_1, \ldots, x_n]$. Puisque $a_n \neq 0$, cette équation montre que $\frac{1}{x}$ est algébrique sur $k(x_1, \ldots, x_r)$. Ainsi tout élément de K(A) est algébrique sur $k(x_1, \ldots, x_r)$. Alors $\{x_1, \ldots, x_r\}$ est une base de transcendance de K(A) sur $k$ et donc $\deg \mathrm{tr}\, \mathrm{K}(\mathrm{A}) = r$. □

COROLLAIRE 3.11. — *Soit $k$ un corps et* $\mathrm{F} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *un polynôme non constant. Alors l'algèbre* $\mathrm{A} = k[\mathrm{X}_1, \ldots, \mathrm{X}_n]/(\mathrm{F})$ *est de dimension de Krull* $n - 1$.

*Démonstration.* D'après le corollaire 3.7, on a évidemment

$$\dim \mathrm{A} \leq n - 1$$

et c'est l'inégalité dans l'autre sens qu'il faut vérifier. Tout idéal premier contenant F contient un facteur irréductible de F. On est ramené à montrer le même résultat quand F est irréductible ; on peut de plus, quitte à changer l'ordre des indéterminées, supposer que $\mathrm{F} \notin k[\mathrm{X}_1, \ldots, \mathrm{X}_{n-1}]$. Considérons alors le morphisme naturel

$$k[\mathrm{X}_1, \ldots, \mathrm{X}_{n-1}] \longrightarrow \mathrm{A}$$

qui induit une inclusion $k(\mathrm{X}_1, \ldots, \mathrm{X}_n) \hookrightarrow \mathrm{K}(\mathrm{A})$. Le degré de transcendance de A est donc $\geq n - 1$, et par suite $\dim \mathrm{A} = n - 1$. □

### 3.4. Hauteur d'un idéal premier

DÉFINITION 3.12. — *Soit* $\mathfrak{p} \subset \mathrm{A}$ *un idéal premier de* A. *On dit que* $\mathfrak{p}$ *est de hauteur finie si le localisé* $\mathrm{A}_\mathfrak{p}$ *est de dimension de Krull finie ; la hauteur de* $\mathfrak{p}$ *est alors*

$$\mathrm{ht}\,(\mathfrak{p}) = \dim \mathrm{A}_\mathfrak{p}$$

C'est donc la longueur maximum $r$ des chaînes d'idéaux premiers

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r = \mathfrak{p}$$

LEMME 3.13. — *Soit* A *un anneau factoriel. Les idéaux premiers de* A *de hauteur 1 sont les idéaux engendrés par les éléments irréductibles.*

*Démonstration.* Soit $\mathfrak{p}$ un idéal premier de hauteur 1. Il contient évidement un élément irréductible $p$ ; puisque A est factoriel, cet élément engendre un idéal premier ; puisque $\mathfrak{p}$ est de hauteur 1, on a $\mathfrak{p} = (p)$. Réciproquement, considérons un élément irréductible $p$ ; l'idéal $\mathfrak{p}$ engendré par $p$ est alors premier ; de plus, considérons un idéal premier non nul $\mathfrak{q} \subset (p)$. Un tel idéal premier doit contenir un élément irréductible $q$ et l'inclusion $(q) \subset (p)$ montre que $p = uq$, où $u$ est une unité et par suite $\mathfrak{q} = \mathfrak{p}$. Donc $\mathfrak{p}$ est de hauteur 1. □

Si A est de dimension finie, tout idéal premier $\mathfrak{p}$ de A est évidemment de hauteur finie, et

$$\mathrm{ht}\,(\mathfrak{p}) + \dim \mathrm{A}/\mathfrak{p} \leq \dim \mathrm{A}.$$

Il n'est pas toujours vrai qu'on a l'égalité. Cependant c'est vrai dans la plupart des anneaux A rencontrés dans la pratique, pourvu que A soit intègre. Par exemple en géométrie algébrique, c'est vrai pour les anneaux intègres que l'on construit à partir de l'anneau des polynômes par passage au quotient ou localisation.

*Exemple.*
Soit F le fermé algébrique de $k^2$ défini par l'union d'une droite $\ell$ et d'un point $p \notin \ell$. L'algèbre $\mathrm{A} = k[\mathrm{X}, \mathrm{Y}]/\mathrm{I}(\mathrm{F})$ est de dimension 1, et l'idéal maximal $\mathfrak{m}_p$ de A est aussi minimal, donc de hauteur 0. Donc l'inégalité est stricte.

THÉORÈME 3.14. — *Soit* A *une* $k$*-algèbre de type fini intègre. Alors pour tout idéal premier* $\mathfrak{p}$ *de* A *on a*

$$\mathrm{ht}\,(\mathfrak{p}) + \dim \mathrm{A}/\mathfrak{p} = \dim \mathrm{A}.$$

Commençons par une propriété qui généralise le théorème de Gauss dans le cadre des anneaux factoriels.

LEMME 3.15. — *Soit* A *un anneau factoriel, et* $\mathrm{A} \hookrightarrow \mathrm{B}$ *une extension entière. On suppose que* B *est intègre. Soient* $a$ *et* $b \in \mathrm{A}$ *premiers entre eux. Soit* $c \in \mathrm{B}$ *tel que* $a$ *divise* $bc$*. Alors* $a$ *divise une puissance convenable de* $c$ *dans* B.

*Anneaux intégralement clos.*
En fait la démonstration de ce lemme fait intervenir une propriété plus faible que celle d'anneau factoriel : c'est la notion d'anneau intégralement clos. Rappelons que la fermeture intégrale d'un anneau intègre A est le sous-anneau du corps des fractions de A des éléments qui sont entiers sur A.

DÉFINITION 3.16. — *Un anneau intègre* A *est intégralement clos si la fermeture intégrale de* A *dans son corps des fractions* K(A) *est* A *lui-même.*

Par exemple, on sait que $\mathbb{Z}$ est intégralement clos. La même démonstration prouve en fait qu'un anneau factoriel est intégralement clos. C'est cette propriété que nous allons utiliser pour vérifier le lemme 3.15 ci-dessus.

*Démonstration du lemme 3.15*
Désignons par K et L les corps de fractions respectifs pour A et B. Le polynôme minimal $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ de $c$, choisi unitaire, est à coefficients dans A ; en effet, dans une extension de L qui contient toutes les racines de P, les autres racines sont encore entières, puisque conjuguées sous le groupe de Galois ; d'après les relations entre coefficients et racines, les coefficients de P sont entiers sur A. Mais l'anneau A étant intégralement clos, ces coefficients sont alors dans l'anneau A. On écrit donc

$$\mathrm{P} = \mathrm{X}^n + \sum_{i \geq 1} u_i \mathrm{X}^{n-i}$$

avec $u_i \in \mathrm{A}$. L'élément $c' = \dfrac{bc}{a}$ de B a pour polynôme minimal

$$\mathrm{Q} = \mathrm{X}^n + \sum_{i=1}^{k} u_i (\frac{b}{a})^i \mathrm{X}^{n-i}$$

et puisque cet élément est entier sur A, les coefficients appartiennent à A : ceci entraîne que $a$ divise $u_1 b, \ldots, u_k b^k$. Puisque A est un anneau factoriel, le théorème de Gauss entraîne que $a$ divise $u_i$. Mais la relation $c^n + u_1 c^{k-1} + \ldots + u_n = 0$ entraîne que $a$ divise $c^n$. Ceci achève la démonstration du lemme 3.15. □

*Démonstration du théorème 3.14*

On fait une récurrence sur $\mathrm{ht}\,(\mathfrak{p})$. Si $\mathfrak{p}$ est de hauteur 0, c'est l'idéal premier $\{0\}$, et l'énoncé est alors évident.

Supposons $\mathrm{ht}\,(\mathfrak{p}) = r$; considérons une chaîne d'idéaux premiers

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_r = \mathfrak{p}$$

et l'anneau quotient $\mathrm{A}/\mathfrak{p}_1$. L'hypothèse de récurrence, appliquée à $\mathfrak{p}/\mathfrak{p}_1$ montre que

$$r - 1 + \dim \mathrm{A}/\mathfrak{p} = \dim \mathrm{A}/\mathfrak{p}_1$$

On est donc ramené à prouver que $\dim \mathrm{A} = \dim \mathrm{A}/\mathfrak{p}_1 + 1$, c'est-à-dire l'énoncé dans le cas particulier où $\mathfrak{p}$ est de hauteur 1.

Soient $x_1, \ldots, x_n \in \mathrm{A}$ des éléments algébriquement indépendants tels que $\mathrm{B} = k[x_1, \ldots, x_n] \subset \mathrm{A}$ soit une extension entière. De tels éléments existent d'après le théorème de normalisation de Noether. Alors $\dim \mathrm{A} = n$ et $\mathrm{B} \cap \mathfrak{p} \neq 0$, car $1 + \dim \mathrm{A}/\mathfrak{p} \leq n$. On va montrer que si $\mathfrak{p}$ est de hauteur 1, $\mathrm{B} \cap \mathfrak{p}$ est encore un idéal premier de B de hauteur 1. Un tel idéal premier dans l'anneau factoriel B est engendré par un élément irréductible F. L'extension $\mathrm{B}/\mathrm{B} \cap \mathfrak{p} \longrightarrow \mathrm{A}/\mathfrak{p}$ est entière, par suite, d'après le corollaire 3.3, $\dim \mathrm{A}/\mathfrak{p} = \dim \mathrm{B}/\mathrm{FB} = n - 1$ : c'est le résultat attendu.

Soit $\mathfrak{q}$ un idéal premier de B de hauteur 1 contenu dans $\mathfrak{p}$. On va montrer que $\mathfrak{p} \cap \mathrm{B} = \mathfrak{q}$. Soit $\mathfrak{a} = \mathfrak{q}\mathrm{A}$ l'idéal de A engendré par $\mathfrak{q}$. Puisque $\mathfrak{p}$ est supposé de hauteur 1, $\mathfrak{p}/\mathfrak{a}$ est obligatoirement l'un des idéaux premiers minimaux de $\mathrm{A}/\mathfrak{a}$. L'idéal $\mathfrak{p}$ est donc un idéal premier associé minimal du A−module $\mathrm{A}/\mathfrak{a}$. Soit $\mathfrak{r}$ la composante primaire de radical $\mathfrak{p}$ dans la décomposition primaire de l'idéal $\mathfrak{a}$; on sait qu'elle est déterminée de façon unique : l'idéal $\mathfrak{r}/\mathfrak{a}$ est le noyau du morphisme canonique

$$\mathrm{A}/\mathfrak{a} \longrightarrow (\mathrm{A}/\mathfrak{a})_{\mathfrak{p}}.$$

Puisque $\mathrm{Ass}(\mathrm{A}/\mathfrak{r}) = \mathfrak{p}$, pour tout $x \in \mathfrak{p}$, il existe un entier $k$ tel que $x^k \in \mathfrak{r}$. On est ramené à vérifier le lemme suivant :

LEMME 3.17. — *L'idéal* $\mathfrak{r} \cap \mathrm{B}$ *est contenu dans* $\mathfrak{q}$.

*Démonstration.* Soit $b \in \mathfrak{r} \cap \mathrm{B}$, non nul. Vu la caractérisation de l'idéal $\mathfrak{r}$, il existe un élément $s \notin \mathfrak{p}$ tel que $sb \in \mathfrak{a}$. L'idéal $\mathfrak{q}$ de B est engendré par un élément irréductible F ; ainsi F divise $sb$ dans A. Les éléments F et $b$ sont des éléments de l'anneau factoriel B. Le lemme 3.15 montre que si F ne divise pas $b$ dans B, il existerait un entier $k$ tel que F divise $s^k$ dans A. Mais alors $s^k$ et donc $s$ appartiendrait à $\mathfrak{p}$ ce qui contredit la définition de $s$. Donc F divise $b$ et donc $b$ appartient à $\mathfrak{q}$. □

Exercice 3.1

Soient A une $k$−algèbre de type fini intègre, et $\mathfrak{a}$ un idéal de A. On pose

$$\mathrm{ht}\,(\mathfrak{a}) = \min_{\substack{\mathfrak{p} \in \mathrm{Spec\,A} \\ \mathfrak{p} \supset \mathfrak{a}}} \mathrm{ht}\,\{\mathfrak{p}\}$$

Démontrer que

$$\mathrm{ht}\,(\mathfrak{a}) + \dim \mathrm{A}/\mathfrak{a} = \dim \mathrm{A}.$$

### 3.5. Modules filtrés

Soit A un anneau, et M un module sur A. Une suite décroissante de sous-modules

$$M = M_0 \supset M_1 \supset M_2 \supset \dots$$

sera appelée une filtration de M.

*Exemple*
Soit $\mathfrak{a}$ un idéal de A. Alors $M_n = \mathfrak{a}^n M$ est une filtration de M.

Une filtration sur M définit une topologie invariante par translation et multiplication par un scalaire. En effet, $M_n$ constitue une base de voisinages de 0 d'une telle topologie.

LEMME 3.18. — (i) *Pour la topologie associée à une filtration* $M_n$, *l'adhérence de* 0 *est l'intersection des* $M_n$.
(ii) *Cette topologie de* M *est séparée si et seulement si*

$$\bigcap_n M_n = \{0\}$$

*Démonstration.* (i) On a $\overline{\{0\}} = \cap_n M_n$. En effet, $x$ appartient à $\overline{\{0\}}$ si et seulement si pour tout $n$, le voisinage de $x$ défini par $x + M_n$ contient 0, ce qui équivaut à $x \in \cap_n M_n$.
(ii) Si M est séparé, les points sont fermés, et donc $\cap_n M_n = 0$. Réciproquement, si cette intersection est réduite à 0, les points sont fermés. Si $x$ et $y$ sont deux points distincts de M, il existe $n$ tel que $x - y \notin M_n$. Alors les voisinages ouverts $x + M_n$ et $y + M_n$ ne se rencontrent pas et donc séparent les points $x$ et $y$. □

DÉFINITION 3.19. — *Soit* $\mathfrak{a}$ *un idéal de* A. *On dit qu'une filtration* $(M_n)_{n\in\mathbb{N}}$*de* M *est une* $\mathfrak{a}$*−filtration si pour tout* $n$ *on a* $\mathfrak{a}M_n \subset M_{n+1}$. *On dit qu'une filtration est* $\mathfrak{a}$*-stable si c'est une* $\mathfrak{a}$*−filtration et si pour* $n$ *assez grand* $M_{n+1} = \mathfrak{a}M_n$.

Ainsi, si une telle filtration de M est $\mathfrak{a}$−stable, il existe un entier $m$ tel que pour $n \geq 0$ on ait $M_{n+m} = \mathfrak{a}^n M_m$.

LEMME 3.20. — *Deux filtrations* $\mathfrak{a}$*−stables définissent la même topologie sur* M.

*Démonstration.* Soient M une filtration $\mathfrak{a}$−stable. Alors il existe un entier $m$ tel que pour tout $n$ on ait

$$M_{n+m} \subset \mathfrak{a}^n M \subset M_n$$

ce qui prouve que la topologie définie par les filtrations $M_n$ et $\mathfrak{a}^n M$ sont les mêmes. □

DÉFINITION 3.21. — *La topologie définie par une filtration* $\mathfrak{a}$*−stable sur* M *s'appelle la topologie* $\mathfrak{a}$*−adique.*

L'objet principal de cette section est de prouver le théorème suivant, connu sous le nom de lemme d'Artin-Rees.

THÉORÈME 3.22. — (lemme d'Artin-Rees) *Soient* A *un anneau noethérien, et* $\mathfrak{a}$ *un idéal de* A. *Soit* M *un module de type fini sur* A, *et* M′ *un sous-module de* M. *La filtration sur* M′ *définie par* $\mathfrak{a}^n M \cap M'$ *est* $\mathfrak{a}$*−stable.*

La démonstration fait intervenir la notion d'anneau gradué, donnée dans la section suivante. Donnons d'abord quelques conséquences.

COROLLAIRE 3.23. — *Sous les mêmes hypothèses, la topologie induite sur* M′ *par la topologie* $\mathfrak{a}-$*adique coïncide avec la topologie* $\mathfrak{a}-$*adique sur* M′.

COROLLAIRE 3.24. — (Krull) *Si* M *est un module de type fini sur un anneau local noethérien d'idéal maximal* $\mathfrak{m}$, *la topologie* $\mathfrak{m}-$*adique est séparée. Autrement dit,*

$$\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n \mathrm{M} = \{0\}$$

*Démonstration.* On considère $\mathrm{M}' = \bigcap_{n\in\mathbb{N}} \mathfrak{m}^n\mathrm{M}$. Puisque A est un anneau noethérien, M′ est encore un module de type fini. La fitration induite sur M′ par la filtration $\mathfrak{m}^n\mathrm{M}$ est $\mathfrak{m}-$stable : ainsi $\mathrm{M}' = \mathfrak{m}\mathrm{M}'$. Le lemme de Nakayama (*cf.* exercice 2.8) implique que $\mathrm{M}' = 0$. □

### 3.6. Anneaux et modules gradués associés

DÉFINITION 3.25. — *Un anneau* A *est gradué s'il est somme directe*

$$\mathrm{A} = \bigoplus_{n=0}^{\infty} \mathrm{A}_n$$

*de sous-groupes* $\mathrm{A}_n$ *tels que si* $x \in \mathrm{A}_n$ *et* $y \in \mathrm{A}_m$ *on ait* $xy \in \mathrm{A}_{n+m}$.

Si $\mathrm{A} = \oplus \mathrm{A}_n$ est un anneau gradué, $\mathrm{A}_0$ est un sous-anneau de A, et chaque composante $\mathrm{A}_n$ est un $\mathrm{A}_0-$module. Le sous-groupe $\mathrm{A}_n$ s'appelle composante homogène de degré $n$.

*Exemple*

L'anneau des polynômes $\mathrm{A} = k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est muni d'une structure naturelle d'anneau gradué : la composante homogène de degré $n$ est constituée de l'espace vectoriel des polynômes homogènes de degré $n$.

DÉFINITION 3.26. — *Soit* A *un anneau gradué. Un module gradué est la donnée d'un* $\mathrm{A}-$*module* M *et d'une décomposition en somme directe de sous-groupes* $\mathrm{M}_n$

$$\mathrm{M} = \bigoplus_{n=0}^{\infty} \mathrm{M}_n$$

*telle que pour tout* $a \in \mathrm{A}_n$ *et* $x \in \mathrm{M}_m$ *on ait* $ax \in \mathrm{M}_{n+m}$.

Si M est un A−module gradué, chaque composante $\mathrm{M}_n$ est un $\mathrm{A}_0-$module.

PROPOSITION 3.27. — *Un anneau gradué* $\mathrm{A} = \oplus_n \mathrm{A}_n$ *est noethérien si et seulement si* $\mathrm{A}_0$ *est noethérien, et* A *est une* $\mathrm{A}_0-$*algèbre de type fini.*

*Démonstration.* Il est clair que si ces conditions sont satisfaites, A est noethérien comme quotient de l'anneau de polynômes $\mathrm{A}_0[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ d'après le théorème de transfert de Hilbert. Réciproquement si A est noethérien, le quotient de A par l'idéal $\mathrm{A}_+ = \oplus_{n>0} \mathrm{A}_n$ est noethérien. Mais ce quotient est isomorphe à l'anneau $\mathrm{A}_0$ : ainsi $\mathrm{A}_0$ est un anneau noethérien. De plus, l'idéal $\mathrm{A}_+$ a un nombre fini de générateurs $x_1, \ldots, x_\ell$ et on peut supposer $x_i$ homogène de degré $d_i > 0$. On a alors $\mathrm{A} = \mathrm{A}_0[x_1, \ldots, x_\ell]$. En effet, si $x \in \mathrm{A}_n$ on peut écrire

$$x = \sum_i a_i x_i$$

avec $a_i \in \mathrm{A}_{n-d_i}$. On voit donc en raisonnant par récurrence sur le degré que $x \in \mathrm{A}_0[x_1, \ldots, x_\ell]$. □

DÉFINITION 3.28. — *Considérons un anneau* A, *et un idéal* $\mathfrak{a}$ *de* A. *On appelle éclaté de* $\mathfrak{a}$ *dans* A *l'anneau gradué*

$$\mathrm{A}^* = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n$$

Il est clair que si A est un anneau noethérien, l'anneau ci-dessus est une A−algèbre de type fini. Donc $A^*$ est un anneau noethérien. Considérons maintenant un A−module M muni d'une $\mathfrak{a}$−filtration $M_n$. La somme directe $M^* = \oplus M_n$ est alors munie d'une structure naturelle de $A^*$−module gradué, obtenue en considérant la multiplication $\mathfrak{a}^n \times M_n \longrightarrow M_{n+m}$.

PROPOSITION 3.29. — *Soit* A *un anneau noethérien, et* M *un* A−*module de type fini. Alors le* $A^*$−*module* $M^*$ *est de type fini si et seulement si la filtration* $M_n$ *est* $\mathfrak{a}$−*stable.*

*Démonstration.* Supposons que la filtration soit $\mathfrak{a}$−stable. Il existe un entier $m$ tel que pour $n \geq m$ on ait $M_n = \mathfrak{a}^{n-m}M_m$. Alors $M^*$ est engendré comme $A^*$−module par $M_0 \oplus \ldots \oplus M_m$. Puisque $M_i$ est un A−module de type fini, il en résulte que $M^*$ est lui-même un $A^*$−module de type fini. Dans l'autre sens, supposons que $M^*$ soit un $A^*$−module de type fini. Considérons le sous-module $S_n$ sur $A^*$ engendré par $\oplus_{i=0}^n M_i$. Ces sous-modules forment une suite croissante, donc stationnaire. Ainsi, il existe un entier $m$ tel que pour $n \geq m$ on ait $S_n = S_{n+1}$. Il en résulte en particulier que $S_{n+1} \subset S_n$ ; en regardant la partie homogène de degré $n+1$ on obtient $M_{n+1} \subset \mathfrak{a}M_n$ pour $n \geq m$. □

*Démonstration du théorème 3.22*

On considère la filtration $M_n = \mathfrak{a}^n M$ et le $A^*$−module associé $M^*$. D'après la proposition 3.29 ce module est un $A^*$−module de type fini. A la $\mathfrak{a}$−filtration de M′ définie par $M'_n = M' \cap \mathfrak{a}^n M$ est associé un sous-module $M'^*$ de $M^*$ ; puisque $A^*$ est un anneau noethérien, ce sous-module est de type fini. Donc, d'après la proposition 3.29 ci-dessus, la filtration $M'_n$ est $\mathfrak{a}$−stable. □

### 3.7. Séries de Poincaré

Considérons un anneau gradué $A = \oplus_{i \geq 0} A_i$. On suppose que

(i) le sous-anneau $A_0$ est un anneau de longueur finie ;

(ii) l'anneau A est une $A_0$-algèbre de type fini, engendrée par des éléments $x_1, \ldots, x_d$ où $x_i$ est un élément homogène de degré 1.

Considérons un A−module de type fini gradué $M = \oplus_{n \geq 0} M_n$. Alors chaque $M_n$ est un $A_0$−module de type fini et par conséquent artinien. On considère la série formelle

$$\chi(M) = \sum_{n \geq 0} \ell(M_n) t^n$$

C'est la série de Poincaré du module gradué M.

DÉFINITION 3.30. — *Etant donnés deux* A−*modules gradués* $M = \oplus_{n \geq 0} M_n$ *et* $N = \oplus_{n \geq 0} N_n$, *un morphisme de* A−*modules gradués* $f : M \longrightarrow N$ *est une application* A*-linéaire telle que* $f(M_n) \subset N_n$.

LEMME 3.31. — *Etant donnée une suite exacte de* A−*modules de type fini gradués*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

*on a*

$$\chi(M) = \chi(M') + \chi(M'').$$

*Démonstration.* Une telle suite exacte induit pour tout entier $n$ une suite exacte de $A_0$−modules

$$0 \longrightarrow M'_n \longrightarrow M_n \longrightarrow M''_n \longrightarrow 0$$

et on a en vertu de la propriété d'additivité de la longueur $\ell(M_n) = \ell(M'_n) + \ell(M''_n)$. □

THÉORÈME 3.32. — (Hilbert-Serre) *Avec les hypothèses ci-dessus, la série de Poincaré du module gradué de type fini* M *s'écrit*

$$\chi(\mathrm{M}) = \frac{\mathrm{P}(t)}{(1-t)^d}$$

*où* $\mathrm{P}(t) \in \mathbb{Z}[t]$ *est un polynôme à coefficients entiers.*

*Démonstration.* On raisonne par récurrence sur $d$. Pour $d = 0$, le module $\mathrm{M}_n$ est nul pour $n$ suffisamment grand, et donc le résultat est trivial. Supposons le résultat établi quand A est une $\mathrm{A}_0-$algèbre engendrée par $d-1$ éléments. On considère le module gradué $\mathrm{M}[-1]$ défini par $\mathrm{M}[-1]_n = \mathrm{M}_{n-1}$ obtenu par décalage à partir de M. C'est encore un A-module gradué de type fini, et on a $\chi(\mathrm{M}[-1]) = t\chi(\mathrm{M})$. La multiplication par $x_1$ définit un morphisme de $\mathrm{A}-$modules gradués $\mathrm{M}[-1] \xrightarrow{x_1} \mathrm{M}$ dont on désigne par K le noyau et par Q le conoyau. On a donc la suite exacte

$$0 \longrightarrow \mathrm{K} \longrightarrow \mathrm{M}[-1] \longrightarrow \mathrm{M} \longrightarrow \mathrm{Q} \longrightarrow 0$$

et par conséquent $\chi(\mathrm{Q}) - \chi(\mathrm{K}) = \chi(\mathrm{M}) - \chi(\mathrm{M}[-1]) = (1-t)\chi(\mathrm{M})$. Considérons l'anneau gradué $\overline{\mathrm{A}} = \mathrm{A}/x_1\mathrm{A}$. Le sous-anneau $\overline{\mathrm{A}}_0$ des éléments homogènes de degré 0 coïncide avec $\mathrm{A}_0$ et comme $\mathrm{A}_0-$ algèbre, $\overline{\mathrm{A}}$ est engendrée par $d-1-$éléments. Les modules gradués K et L peuvent être considérés comme des $\overline{\mathrm{A}}-$modules gradués, et par hypothèse de récurrence $\chi(\mathrm{K})$ et $\chi(\mathrm{Q})$ sont des fractions rationnelles

$$\chi(\mathrm{K}) = \frac{\mathrm{P}_\mathrm{K}(t)}{(1-t)^{d-1}} \; ; \; \chi(\mathrm{Q}) = \frac{\mathrm{P}_\mathrm{Q}(t)}{(1-t)^{d-1}}$$

En vertu du lemme 3.31 ceci entraîne évidemment le résultat. □

COROLLAIRE 3.33. — *Il existe un entier* $n_0$ *tel que pour* $n \geq n_0$ *la suite* $n \mapsto \ell(\mathrm{M}_n)$ *soit un polynôme en* $n$ *à coefficients rationnels de degré* $\leq d-1$.

*Démonstration.* On peut écrire après simplification éventuelle

$$\chi(\mathrm{M}) = \frac{\mathrm{Q}(t)}{(1-t)^k}$$

où $\mathrm{Q}(t) = \sum_{0 \leq j \leq m} a_j t^j$ est un polynôme à coefficients entiers tel que $\mathrm{Q}(1) \neq 0$. Si $k = 0$, on a $\ell(\mathrm{M}_n) = 0$ pour $n$ assez grand, donc l'énoncé est vrai. On suppose maintenant $k \geq 1$. On a $(1-t)^{-k} = \sum_{i \geq 0} \binom{k+i-1}{k-1} t^i$ et par conséquent

$$\chi(\mathrm{M}) = \sum_{n \geq 0} \Big( \sum_{\substack{i+j=n \\ 0 \leq j \leq m}} a_j \binom{k+i-1}{k-1} \Big) t^n$$

Par suite

$$\ell(\mathrm{M}_n) = \sum_{0 \leq j \leq m} a_j \binom{n+k-j-1}{k-1}.$$

Evidemment, pour $n \geq j-k+1$, la suite $n \mapsto \binom{n+k-j-1}{k-1}$ est un polynôme en $n$ de degré $k-1$ à coefficients rationnels. Ainsi, pour $n \geq m-k+1$, la longueur $\ell(\mathrm{M}_n)$ est un polynôme en $n$ de degré $k-1$, dont le terme dominant est $\frac{\mathrm{Q}(1)}{(k-1)!}$ ce qui achève la démonstration. □

*Exemple*

Soit $A_0$ un module de longueur finie. On considère l'anneau des polynômes $A = A_0[X_1, \ldots, X_d]$ à coefficients dans $A_0$. Pour tout $n \geq 0$ on a

$$\ell(A_n) = \ell(A_0)\binom{n+d-1}{d-1}$$

Exercice 3.2

On suppose que $A_0$ est de longueur finie, et que A est une $A_0-$algèbre engendrée par des éléments $x_1, \ldots, x_d$ où $x_i$ est homogène de degré $r_i$. Vérifier que pour tout A−module gradué M de type fini la série de Poincaré de M est une fonction rationnelle de la forme

$$\chi(M) = \frac{P(t)}{\prod_{i=1}^{d}(1-t^{r_i})}$$

où $P(t) \in \mathbb{Z}[t]$.

COROLLAIRE 3.34. — *Soient* A *un anneau local noethérien d'idéal maximal* $\mathfrak{m}$, *de corps résiduel* $k = A/\mathfrak{m}$ *et* $\mathfrak{q}$ *un idéal* $\mathfrak{m}-$*primaire. Soit* $d$ *le nombre minimal de générateurs de* $\mathfrak{q}$. *Soit* M *un* A−*module de type fini.*

(i) *Pour* $n$ *assez grand, la longueur de* $M/\mathfrak{q}^n M$ *est un polynôme en* $n$ *de degré* $\leq d$.

(ii) *Le degré de ce polynôme ne dépend pas de* $\mathfrak{q}$.

*Démonstration.* On associe à l'idéal $\mathfrak{q}$ l'anneau gradué

$$\mathrm{gr}_{\mathfrak{q}}(A) = \bigoplus_n \mathfrak{q}^n/\mathfrak{q}^{n+1}$$

appellé le cône de $\mathfrak{q}$. Ce module gradué est une $A/\mathfrak{q}$-algèbre engendré par $\mathfrak{q}/\mathfrak{q}^2$, et par suite elle est engendrée par $d-$éléments. Au module M on associe le $\mathrm{gr}_{\mathfrak{q}}(A)$-module gradué de type fini

$$\mathrm{gr}_{\mathfrak{q}}(M) = \bigoplus_n \mathfrak{q}^n M/\mathfrak{q}^{n+1}M.$$

Puisque $A/\mathfrak{q}$ est un anneau de longueur finie, on peut appliquer ce qui précède : la longueur de $\mathfrak{q}^n M/\mathfrak{q}^{n+1}M$ est pour $n$ assez grand un polynôme en $n$ de degré $\leq d-1$. Le A−module $M/\mathfrak{q}^n M$ est de longueur finie et la suite exacte

$$0 \longrightarrow \mathfrak{q}^i M/\mathfrak{q}^{i+1}M \longrightarrow M/\mathfrak{q}^{i+1}M \longrightarrow M/\mathfrak{q}^i M \longrightarrow 0$$

montre que

$$\ell(M/\mathfrak{q}^n M) = \sum_{0 \leq i \leq n-1} \ell(\mathfrak{q}^i M/\mathfrak{q}^{i+1}M)$$

d'où découle immédiatement l'assertion (i).

Vérifions (ii). On a pour $r$ assez grand $\mathfrak{m}^r \subset \mathfrak{q} \subset \mathfrak{m}$. Donc

$$\mathfrak{m}^{rn}M \subset \mathfrak{q}^n M \subset \mathfrak{m}^n M.$$

Il en résulte que pour $n$ assez grand

$$\ell(M/\mathfrak{m}^{rn}M \geq \ell(M/\mathfrak{q}^n M) \geq \ell(M/\mathfrak{m}^n M)$$

Les deux polynômes extrêmes sont pour $n$ assez grand des polynômes en $n$ de même degré ; il en résulte que le polynôme du milieu est aussi de même degré.

DÉFINITION 3.35. — *Le polynôme* $P_{\mathfrak{q}}(M)$ *défini par* $P_{\mathfrak{q}}(M)(n) = \ell(M/\mathfrak{q}^n M)$ *pour* $n$ *assez grand s'appelle le polynôme de Hilbert de* M *relatif à l'idéal primaire* $\mathfrak{q}$. *Dans le cas où* $M = A$, *on l'appelle le polynôme caractéristique de l'idéal* $\mathfrak{q}$, *et on le note* $P_{\mathfrak{q}}(A)$.

COROLLAIRE 3.36. — *Soit* $\delta(A)$ *le nombre minimal de générateurs d'un idéal* $\mathfrak{m}-$*primaire de l'anneau local noethérien* A. *Pour tout idéal* $\mathfrak{m}-$*primaire* $\mathfrak{q}$ *on a*

$$\deg P_{\mathfrak{q}}(A) = \deg P_{\mathfrak{m}}(A) \leq \delta(A).$$

### 3.8. Dimension des anneaux locaux noethériens

Nagata a construit des exemples d'anneaux noethériens qui ne sont pas de dimension de Krull finie (*cf.* exercice 3.5). Par contre, les anneaux locaux noethériens sont de dimension finie :

THÉORÈME 3.37. — *Soit* A *un anneau local noethérien, d'idéal maximal* $\mathfrak{m}$. *Alors* A *est de dimension de Krull finie. De plus les trois nombres suivants sont égaux*
(i) $\dim \mathrm{A}$;
(ii) *le nombre minimal de générateurs* $\delta(\mathrm{A})$ *d'un idéal* $\mathfrak{m}-$*primaire ;*
(iii) *le degré* $d(\mathrm{A})$ *du polynôme de Hilbert* $\mathrm{P}_{\mathfrak{m}}(\mathrm{A})$.

D'après le corollaire 3.36, on a déjà vu que $d(\mathrm{A}) \leq \delta(\mathrm{A})$.

LEMME 3.38. — *Soit* $x \in \mathfrak{m}$ *un élément qui n'est pas diviseur de* 0. *Alors* $d(\mathrm{A}/x\mathrm{A}) \leq d(\mathrm{A})-1$

*Démonstration.* On a une suite exacte

$$0 \longrightarrow \mathrm{A} \xrightarrow{x} \mathrm{A} \longrightarrow \mathrm{A}/x\mathrm{A} \longrightarrow 0$$

Soit $\mathrm{I}_n$ l'idéal des $a \in \mathrm{A}$ tels que $ax \in \mathfrak{m}^n$. On a une suite exacte

$$0 \longrightarrow \mathrm{A}/\mathrm{I}_n \xrightarrow{x} \mathrm{A}/\mathfrak{m}^n \longrightarrow \mathrm{A}/(\mathfrak{m}^n, x) \longrightarrow 0$$

ce qui prouve que $\mathrm{A}/\mathrm{I}_n$ est de longueur finie, et que c'est un polynôme pour $n$ assez grand. De plus, la filtration $\mathrm{I}_n$ est une $\mathfrak{m}-$filtration qui, d'après le théorème d'Artin-Rees, est $\mathfrak{m}-$stable ; il existe donc un entier $n_0$ tel que pour $n \geq n_0$ on ait $\mathrm{I}_n = \mathfrak{m}^{n-n_0}\mathrm{I}_{n_0}$, et donc

$$\mathfrak{m}^n \subset \mathrm{I}_n \subset \mathfrak{m}^{n-n_0}$$

Donc

$$\ell(\mathrm{A}/\mathfrak{m}^{n-n_0}) \leq \ell(\mathrm{A}/\mathrm{I}_n) \leq \ell(\mathrm{A}/\mathfrak{m}^n)$$

Pour $n$ assez grand, nous sommes en présence de trois polynômes en $n$ dont les termes dominants sont les mêmes. Donc le polynôme caractéristique de l'idéal maximal de $\mathrm{A}/x\mathrm{A}$, donné pour $n$ assez grand par $n \mapsto \ell(\mathrm{A}/(\mathfrak{m}^n, x))$ est de degré $\leq d(\mathrm{A}) - 1$. □

*Inégalité* $\dim \mathrm{A} \leq d(\mathrm{A})$

On démontre cette inégalité par récurrence sur $d(\mathrm{A})$. Si $d(\mathrm{A}) = 0$, la longueur $\ell(\mathrm{A}/\mathfrak{m}^n)$ est constante pour $n$ assez grand, et donc d'après le lemme de Nakayama $\mathfrak{m}^n = 0$ pour $n$ assez grand. Alors A est un anneau artinien, donc de dimension de Krull nulle.

Considérons maintenant une chaîne d'idéaux premiers de A

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$$

Soit $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$. Alors la classe $\overline{x}$ de $x$ dans l'aneau intègre $\mathrm{A}' = \mathrm{A}/\mathfrak{p}_0$ n'est pas nulle, donc ce n'est pas un diviseur de 0. Si $\mathfrak{m}'$ est l'idéal maximal de $\mathrm{A}'$ on a un morphisme surjectif $\mathrm{A}/\mathfrak{m}^n \longrightarrow \mathrm{A}'/\mathfrak{m}'^n$ et par conséquent $\mathrm{P}_{\mathfrak{m}'}(\mathrm{A}')(n) \leq \mathrm{P}_{\mathfrak{m}}(\mathrm{A})(n)$ pour $n$ assez grand. Par suite $d(\mathrm{A}') \leq d(\mathrm{A})$. D'après le lemme ci-dessus, on a alors

$$d(\mathrm{A}'/\overline{x}\mathrm{A}') \leq d(\mathrm{A}') - 1 \leq d(\mathrm{A}) - 1.$$

L'hypothèse de récurrence montre que $\mathrm{A}'/x\mathrm{A}'$ est de dimension de Krull finie $\leq d(\mathrm{A}) - 1$. Alors $r-1 \leq d(\mathrm{A})-1$, et par suite $r \leq d(\mathrm{A})$. Donc A est aussi de dimension de Krull finie et $\dim \mathrm{A} \leq d(\mathrm{A})$.

*L'inégalité* $\delta(\mathrm{A}) \leq \dim \mathrm{A}$.
Commençons par un lemme utile, appelé lemme d'évitement.

LEMME 3.39. — *Soit* $\mathfrak{a}$ *un idéal d'un anneau* A, *et* $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ *des idéaux premiers tels que* $\mathfrak{a} \subset \cup_{i=1}^{k} \mathfrak{p}_i$. *Alors* $\mathfrak{a}$ *est contenu dans l'un des* $\mathfrak{p}_i$.

*Démonstration.* Par récurrence sur $k$ ; il n'y a rien à prouver pour $k = 1$. Supposons que $\mathfrak{a}$ ne soit contenu dans aucun des $\mathfrak{p}_i$. D'après l'hypothèse de récurrence, pour tout $j$ on a $\mathfrak{a} \not\subset \cup_{i \neq j} \mathfrak{p}_i$. Donc il existe $a_j \in \mathfrak{a}$, tel que $a_j \notin \cup_{i \neq j} \mathfrak{p}_i$. Alors $a_j$ appartient à $\mathfrak{p}_j$ et $b = a_1 + a_2 \ldots a_\ell$ appartient à $\mathfrak{a}$. Il n'appartient pas à aucun des $\mathfrak{p}_j$, ce qui fournit une contradiction. □

Si $\dim \mathrm{A} = 0$, l'anneau A est de longueur finie, donc $\{0\}$ est un idéal primaire. Ainsi $\delta(\mathrm{A}) = 0$. Supposons maintenant $\dim \mathrm{A} > 0$. On va construire, pour $i \leq n = \dim \mathrm{A}$, une suite $x_1, \ldots, x_i \in \mathfrak{m}$ telle que pour tout idéal premier $\mathfrak{p}$ contenant l'idéal $(x_1, \ldots, x_i)$ on ait $\mathrm{ht}(\mathfrak{p}) \geq i$. On raisonne par récurrence sur $i$. On choisit $x_1 \in \mathfrak{m} \setminus \cup_{\mathrm{ht}(\mathfrak{p})=0} \mathfrak{p}$. C'est possible d'après le lemme d'évitement. Supposons choisis $(x_1, \ldots, x_i)$. Si $i < n$ considérons les idéaux premiers de hauteur $i$ qui contiennent $(x_1, \ldots, x_i)$ : vu le choix de $(x_1, \ldots, x_i)$ ces idéaux premiers correspondent aux idéaux premiers minimaux de $\mathrm{A}/(x_1, \ldots, x_i)$. Ils sont donc en nombre fini, et le lemme d'évitement permet de choisir $x_{i+1} \in \mathfrak{m}$ et n'appartenant à aucun de ces idéaux premiers. Alors tout idéal premier contenant $(x_1, \ldots, x_{i+1})$ est de hauteur $\geq i + 1$.

Considérons l'idéal $\mathfrak{q} = (x_1, \ldots, x_n)$. Tout idéal premier contenant l'idéal $(x_1, \ldots, x_n)$ est de hauteur $n$ : un tel idéal premier est donc forcément l'idéal maximal $\mathfrak{m}$ de A. Ainsi, $\mathrm{A}/(x_1, \ldots, x_n)$ est un anneau artinien, et l'idéal $(x_1, \ldots, x_n)$ est un idéal $\mathfrak{m}-$primaire. Par suite, $\delta(\mathrm{A}) \leq \dim \mathrm{A}$. □

COROLLAIRE 3.40. — *Soit* A *un anneau local noethérien, d'idéal maximal* $\mathfrak{m}$ *et de corps résiduel* $k$. *On a*

$$\dim \mathrm{A} \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$$

*Démonstration.* Soit $d = \dim_k \mathfrak{m}/\mathfrak{m}^2$. Soient $(x_1, \ldots, x_d)$ des éléments de $\mathfrak{m}$ dont les classes dans $\mathfrak{m}/\mathfrak{m}^2$ forment une base. D'après le lemme de Nakayama, $(x_1, \ldots, x_d)$ engendrent l'idéal maximal $\mathfrak{m}$. Ainsi, $\dim \mathrm{A} \leq d$. □

COROLLAIRE 3.41. — *Soit* A *un anneau local noethérien et* $(x_1, \ldots, x_r) \in \mathrm{A}$. *Pour tout idéal premier* $\mathfrak{p}$ *minimal dans* $\mathrm{Ass}_{\mathrm{A}}(\mathrm{A}/(x_1, \ldots, x_r))$ *on a* $\mathrm{ht}(\mathfrak{p}) \leq r$.

*Démonstration.* L'anneau $\mathrm{A}_{\mathfrak{p}}$ est un anneau local noethérien et l'idéal $(x_1, \ldots, x_r)\mathrm{A}_{\mathfrak{p}}$ est primaire de radical $\mathfrak{p}\mathrm{A}_{\mathfrak{p}}$. Donc $r \geq \mathrm{ht}(\mathfrak{p})$. □

COROLLAIRE 3.42. — (Théorème de l'idéal principal de Krull) *Soit* A *un anneau local noethérien et* $x \in \mathrm{A}$ *un élément de* A *qui n'est pas inversible, ni un diviseur de* 0.

(i) *Les idéaux premiers minimaux de* $\mathrm{Ass}_{\mathrm{A}}(\mathrm{A}/x\mathrm{A})$ *sont de hauteur 1.*

(ii) *On a* $\dim \mathrm{A}/x\mathrm{A} = \dim \mathrm{A} - 1$.

*Démonstration.* (i) Un tel idéal premier $\mathfrak{p}$ est de hauteur $\leq 1$ d'après le corollaire qui précède. Cet idéal premier ne peut être de hauteur 0, sinon il appartiendrait à $\mathrm{Ass}(\mathrm{A})$, et $x$ serait un diviseur de 0.

(ii) D'après le lemme 3.38, on a $\dim \mathrm{A}/x\mathrm{A} \leq \dim \mathrm{A} - 1$. Soit $k = \dim \mathrm{A}/x\mathrm{A}$. Considérons des éléments $(x_1, \ldots, x_k)$ dont les images dans $\mathrm{A}/x\mathrm{A}$ engendrent un idéal $\mathfrak{m}/(x)-$primaire. Alors $(x, x_1, \ldots, x_k)$ est un idéal $\mathfrak{m}-$primaire. Donc $k + 1 \geq \dim \mathrm{A}$. D'où l'égalité $k = \dim \mathrm{A} - 1$. □

Exercice 3.3

1) Soit M un A-module tel que pour tout idéal maximal $\mathfrak{m}$ de A le localisé $\mathrm{M}_{\mathfrak{m}}$ soit nul. Montrer que M est nul.

2) Soit M′ un sous-module de M tel que pour tout idéal maximal $\mathfrak{m}$ de A l'application linéaire

$$\mathrm{M}'_{\mathfrak{m}} \longrightarrow \mathrm{M}_{\mathfrak{m}}$$

soit surjective. Montrer que $\mathrm{M}' = \mathrm{M}$.

Exercice 3.4

Soit $\mathcal{X}$ un ensemble, dont les éléments seront appelées indéterminées.

1) Définir le monoïde $\mathbb{N}^{(\mathcal{X})}$ des monômes en les indéterminées $X \in \mathcal{X}$.

2) Soit $k$ un corps. Définir l'algèbre $k[\mathcal{X}]$ des polynômes en les indéterminées $X \in \mathcal{X}$. Caractériser $k[\mathcal{X}]$ par une propriété universelle.

3) Montrer que $k[\mathcal{X}]$ est l'union des sous-anneaux $k[\mathcal{Y}]$, où $\mathcal{Y}$ parcourt les parties finies de $\mathcal{X}$. En déduire que $k[\mathcal{X}]$ est intègre.

4) Démontrer que si $\mathcal{X}$ n'est pas fini, cet anneau n'est pas noethérien.

Exercice 3.5

On se propose de construire un anneau noethérien dont la dimension de Krull n'est pas finie. Cet exemple est dû à Nagata.

On considère une union disjointe dénombrable $\mathcal{X}$ d'ensembles finis $\mathcal{X}_i$

$$\mathcal{X} = \coprod_{i \in \mathbb{N}} \mathcal{X}_i$$

et l'algèbre $k[\mathcal{X}]$ des polynômes avec indéterminées dans $\mathcal{X}$. On désigne par $\mathfrak{p}_i$ l'idéal de $A = k[\mathcal{X}]$ engendré par $\mathcal{X}_i$.

1) Montrer que $A/\mathfrak{p}_i$ est isomorphe à un anneau de polynômes. En déduire que $\mathfrak{p}_i$ est un idéal premier de A. Montrer que $\mathfrak{p}_i \cap k[\cup_{j \neq i} \mathcal{X}_j] = \{0\}$.

2) Soit $P \in k[\mathcal{X}]$, non nul. Montrer qu'il n'existe qu'un nombre fini d'idéaux $\mathfrak{p}_i$ contenant P.

3) On considère le complémentaire S de l'union des $\mathfrak{p}_i$. Montrer que S est une partie multiplicative. Montrer que tout idéal non nul de A qui ne rencontre pas S est contenu dans l'un des idéaux $\mathfrak{p}_i$. (On pourra observer que cet idéal est contenu dans une union finie de $\mathfrak{p}_i$, et utiliser le lemme d'évitement.)

4) Démontrer que $A_{\mathfrak{p}_i}$ est isomorphe à un anneau de fractions de l'anneau de polynômes $K_i[\mathcal{X}_i]$, où $K_i$ est le corps des fractions de $k[\mathcal{X} \setminus \mathcal{X}_i]$. En déduire que l'anneau $A_{\mathfrak{p}_i}$ est noethérien.

5) Soit $\mathfrak{a}$ un idéal non nul de A qui ne rencontre pas S. Montrer que l'on peut trouver un idéal de type fini $\mathfrak{b} = (P_1, \ldots, P_k)$ tels que si $\mathfrak{p}_i$ contient $\mathfrak{b}$ on ait

$$\mathfrak{b}_{\mathfrak{p}_i} = \mathfrak{a}_{\mathfrak{p}_i}$$

(On pourra commencer par les idéaux premiers $\mathfrak{p}_i$ qui contiennent $\mathfrak{a}$ en appliquant la question 4) et agrandir éventuellement l'idéal obtenu). Montrer qu'alors $\mathfrak{a} = \mathfrak{b}$.

6) En déduire que $S^{-1}A$ est un anneau noethérien.

7) Montrer que $\mathfrak{p}_i$ a pour hauteur le nombre d'éléments $\#\mathcal{X}_i$ de $\mathcal{X}_i$. En déduire que si la suite $i \mapsto \#\mathcal{X}_i$ n'est pas bornée, l'anneau $S^{-1}A$ n'est pas de dimension de Krull finie.

### 3.9. Anneaux locaux réguliers

En géométrie algébrique, si $k$ est un corps algébriquement clos, on associe à un fermé algébrique de $k^n$ l'algèbre des fonctions régulières $\mathcal{O}(X)$. Si $x \in X$, on lui associe l'anneau local $\mathcal{O}_{X,x} = \mathcal{O}(X)_{\mathfrak{m}_x}$, localisé en l'idéal maximal. Sur cet anneau local, on pourra lire le fait que le point $x$ est ou non singulier : c'est la notion d'anneau local régulier.

THÉORÈME 3.43. — *Soit* A *un anneau local régulier de dimension d d'idéal maximal* $\mathfrak{m}$, *de corps résiduel* $k = A/\mathfrak{m}$. *Les assertions suivantes sont équivalentes*

(i) *L'algèbre graduée* $\mathrm{gr}_{\mathfrak{m}}(A)$ *est isomorphe à l'algèbre des polynômes sur k à nd indéterminées ;*

(ii) $\dim \mathfrak{m}/\mathfrak{m}^2 = d$;

(iii) *L'idéal maximal* $\mathfrak{m}$ *est engendré par d éléments.*

*Démonstration.* (i) $\Rightarrow$ (ii) : Un isomorphisme d'algèbres graduées devant respecter les graduations, on a bien $\dim \mathfrak{m}/\mathfrak{m}^2 = d$.

(ii) $\Rightarrow$ (iii) : c'est le lemme de Nakayama (Voir la démonstration du lemme 3.40).

(iii) $\Rightarrow$ (i) L'énoncé est évident pour $d = 0$. Supposons $d \geq 1$. Considérons un système de $d$ générateurs $x_1, \ldots, x_d$ de $\mathfrak{m}$; désignons par $\overline{x}_1, \ldots, \overline{x}_d$ leur classe dans $\mathrm{gr}_{\mathfrak{m}}(\mathrm{A})$. Ces éléments définissent un morphisme de $k-$algèbres graduées

$$\alpha : k[\mathrm{X}_1, \ldots, \mathrm{X}_d] \longrightarrow \mathrm{gr}_{\mathfrak{m}}(\mathrm{A}).$$

qui est évidemment surjectif. Considérons le noyau N de ce morphisme : c'est un idéal gradué $\mathfrak{a} = \oplus_{n \geq 0} \mathfrak{a}_n$. Soit $\mathrm{B} = k[\mathrm{X}_1, \ldots, \mathrm{X}_d]$ l'algèbre graduée des polynômes à coeffcients dans $k$. Supposons que N soit non nul, et considérons un élément $f \in \mathrm{N}$, homogène de degré $m$. Un tel élément définit un morphisme injectif de modules gradués

$$\mathrm{B}[-m] \xrightarrow{f} \mathrm{B}$$

et le conoyau Q est un module gradué de type fini dont la série de Poincaré $\sum_{n \geq 0} \ell(\mathrm{Q}_n) t^n$ satisfait à la condition suivante : la longueur $n \mapsto \ell(\mathrm{Q}_n)$ est pour $n$ assez grand un polynôme en $n$ de degré $\leq d - 2$. Or, $\alpha$ se factorise en un morphisme surjectif $\mathrm{Q} \longrightarrow \mathrm{gr}_{\mathfrak{m}}(\mathrm{A})$. Alors pour tout $n$, $\ell(\mathrm{gr}_n(\mathrm{A})) \leq \ell(\mathrm{Q}_n)$ ce qui contredit le fait que $n \longrightarrow \ell(\mathrm{gr}_n(\mathrm{A}))$ est un polynôme en $n$ de degré $d - 1$. □

DÉFINITION 3.44. — (i) *Un anneau local noethérien de dimension $n$, d'idéal maximal $\mathfrak{m}$ est régulier s'il satisfait une des conditions équivalentes du théorème ci-dessus.*

(ii) *Un système de $n$ générateurs de l'idéal maximal $\mathfrak{m}$ s'appelle un système régulier de paramètres.*

(iii) *Un anneau noethérien* A *est dit régulier si pour tout idéal maximal $\mathfrak{m}$ de* A *le localisé* $\mathrm{A}_{\mathfrak{m}}$ *est un anneau local régulier.*

*Exemple*

Soient $k$ un corps, et $\mathfrak{m}$ l'idéal maximal $(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ dans $\mathrm{A} = k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. Alors l'anneau local $\mathrm{A}_{\mathfrak{m}}$ est régulier. En effet, cet anneau local est de dimension $n$.

PROPOSITION 3.45. — *Un anneau local régulier est intègre.*

*Démonstration.* En effet, si A est un anneau local régulier d'idéal maximal $\mathfrak{m}$ l'anneau gradué $\mathrm{gr}(\mathrm{A}) = \mathrm{gr}_{\mathfrak{m}}(\mathrm{A})$ est un anneau de polynômes, donc intègre. Maintenant, si $x \in \mathrm{A}$ et $y \in \mathrm{A}$ sont deux éléments non nuls, il existe d'après le théorème de Krull des entiers $i$ et $j$ tels que $x \in \mathfrak{m}^i \setminus \mathfrak{m}^{i+1}$ et $y \in \mathfrak{m}^j \setminus \mathfrak{m}^{j+1}$. Alors les classes $\overline{x}$ dans $\mathrm{gr}_i(\mathrm{A})$ et $\overline{y} \in \mathrm{gr}_j(\mathrm{A})$ sont non nulles, donc le produit $\overline{x}.\overline{y}$ est non nul dans $\mathrm{gr}_{i+j}(\mathrm{A})$. Mais par définition, cette classe est aussi la classe de $xy$, qui est donc non nul.

PROPOSITION 3.46. — *Soit* A *un anneau local régulier de dimension $n$, d'idéal maximal $\mathfrak{m}$ et $f_1, \ldots, f_m$ des éléments de $\mathfrak{m}$ dont les classes dans $\mathfrak{m}/\mathfrak{m}^2$ sont indépendantes. L'anneau quotient $\mathrm{A}/(f_1, \ldots, f_m)$ est un anneau local régulier de dimension $n - m$.*

*Démonstration.* La démonstration ci-dessus montre que $f_1$ n'est diviseur de 0 dans A. D'après le lemme 3.42, on a $\dim \mathrm{A}/(f_1) = n-1$ et l'idéal maximal de $\mathrm{A}/(f_1)$ est engendré par $n-1$ éléments : le quotient $\mathrm{A}/(f_1)$ est donc un anneau local régulier de dimension $n-1$. On peut bien sûr continuer par récurrence sur $i$. □

*Exemple.*

Soient $k$ un corps algébriquement clos, et $P_1, \ldots, P_m \in A = k[X_1, \ldots, X_n]$ des polynômes. Si $x$ est un point de $k^n$, l'application $A \longrightarrow \mathfrak{m}_x/\mathfrak{m}_x^2$ définie par

$$P \mapsto [P - P(x)] \in \mathfrak{m}_x/\mathfrak{m}_x^2$$

s'appelle la différentielle de P en $x$, et se note $d_x P$. Elle est $k-$linéaire, et satisfait à la règle de Leibniz

$$d_x(PQ) = P(x)d_xQ + Q(x)d_xP$$

L'espace vectoriel $\mathfrak{m}_x/\mathfrak{m}_x^2$ est de dimension $n$, avec pour base $d_xX_i$, et l'on a pour tout $P \in A$

$$d_xP = \sum_j \frac{\partial P}{\partial X_j}(x) d_xX_i$$

L'énoncé ci-dessus dit que si les différentielles $d_xP_i$ sont indépendantes en tout point $x$ où les polynômes $P_i$ s'annulent l'anneau quotient $A/(P_1, \ldots, P_m)$ est un anneau régulier de dimension $n - m$. En termes de différentielles, l'hypothèse signifie que la matrice jacobienne

$$\left(\frac{\partial P_i}{\partial X_j}(x)\right)$$

est de rang $m$ : c'est ce qu'on appelle le critère jacobien.

## 4. Représentations des groupes finis

Si V est un espace vectoriel, on désigne par GL(V) le groupe des applications linéaires inversibles de V dans lui-même. Soit G un groupe fini d'ordre $n$, et V un espace vectoriel sur un corps $k$. L'élément neutre de G sera noté $e$.

### 4.1. Définitions

DÉFINITION 4.1. — *Une représentation linéaire de* G *dans* V *est un homomorphisme de groupes* $\rho : \mathrm{G} \to \mathrm{GL(V)}$.

Soit $e$ l'élément neutre de G. On a donc pour $s$ et $t \in \mathrm{G}$

$$\rho(st) = \rho(s)\rho(t) \ ; \ \rho(e) = \mathrm{id_V}$$

Il en résulte que $\rho(s^{-1}) = \rho(s)^{-1}$.

On dit aussi que V est un G−module. Pour expliquer cette terminologie, nous allons montrer que se donner une telle représentation revient à se donner un module sur une algèbre associée à G, notée $k$[G].

*L'algèbre* $k$[G] *du groupe* G.

Rappelons d'abord qu'une algèbre (unitaire) A sur un corps $k$ est la donnée d'un anneau unitaire A (non obligatoirement commutatif) et d'un homomorphisme d'anneaux unitaires $k \to \mathrm{A}$. Si G est un groupe fini, l'algèbre $k$[G] du groupe G est définie par l'espace vectoriel $k^{\mathrm{G}}$ (de dimension $|\mathrm{G}|$) des applications $u : s \mapsto u_s$ de G dans $k$, équipé de la multiplication, avec élément unité, définie pour $s \in \mathrm{G}$ par la formule

$$(uv)_s = \sum_{\substack{(t,r)\in \mathrm{G}\times\mathrm{G} \\ tr=s}} u_t v_r$$

Considérons pour $g \in \mathrm{G}$ l'application $\epsilon_g : \mathrm{G} \to k$ définie pour $s \in \mathrm{G}$ par $\epsilon_{g,s} = 0$ si $s \neq g$ et $\epsilon_{g,g} = 1$. L'application $\epsilon : \mathrm{G} \to k$[G] définie par $g \mapsto \epsilon_g$ est alors injective : elle identifie G à une base de $k$[G]. Tout élément $u \in k$[G] s'écrit en effet de manière unique $u = \sum_{g\in \mathrm{G}} u_g \epsilon_g$, avec $u_g \in k$. On a de plus

$$\epsilon_{st} = \epsilon_s \epsilon_t \ ; \ \epsilon_e = 1 \qquad (*)$$

Ainsi, l'application $\epsilon$ est un isomorphisme de G sur un sous-groupe du groupe des éléments inversibles de $k$[G]. La multiplication qu'on a définie est la seule possible pour que la formule $(*)$ soit vraie. Dans la pratique, on identifiera l'élément $g \in \mathrm{G}$ avec l'élément $\epsilon_g \in k$[G]. Ainsi, G est identifié à une partie de $k$[G], et les éléments $u \in k$[G] s'écrivent avec cette convention

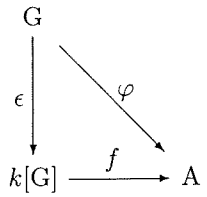
$$u = \sum_{g\in \mathrm{G}} u_g g.$$

*Propriété universelle*

L'algèbre $k$[G] ainsi définie possède la propriété universelle suivante : toute application $\varphi : \mathrm{G} \to \mathrm{A}$ de G dans une algèbre A satisfaisant à la propriété

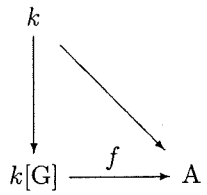
$$\varphi(st) = \varphi(s)\varphi(t) \ ; \varphi(e) = 1$$

pour tout $s$ et $t \in \mathrm{G}$ se factorise de manière unique suivant le diagramme




où $f$ est un homomorphisme de $k-$algèbres.

Par homomorphisme de $k-$algèbres, on entend un homomorphisme d'anneaux qui soit $k-$linéaire. Il est équivalent de dire que le diagramme




est commutatif. Etant donnée une représentation $\rho$ de G dans un $k-$espace vectoriel V on obtient par la propriété universelle ci-dessus un homomorphisme d'algèbres $f : k[\mathrm{G}] \to \mathrm{End}_k(\mathrm{V})$. Il en résulte que l'espace V peut-être muni d'une structure de $k[\mathrm{G}]-$module (à gauche) en posant, pour tout $u \in k[\mathrm{G}]$ et $x \in \mathrm{V}$

$$u.x = f(u)(x).$$

Réciproquement, étant donné un $k[\mathrm{G}]-$module à gauche, on obtient un homomorphisme de $k-$algèbres $k[\mathrm{G}] \to \mathrm{End}_k(\mathrm{V})$ et la restriction à G (via le plongement $\epsilon$) définit une représentation.

*Homomorphismes de représentations*

Soient $\rho$ et $\rho'$ deux représentations dans V et V′ respectivement. Un homomorphisme de $\rho$ dans $\rho'$ est une application $k-$linéaire $f : \mathrm{V} \to \mathrm{V}'$ telle que pour tout $s \in \mathrm{G}$

$$f \circ \rho(s)) = \rho'(s) \circ f.$$

Il revient au même de dire que, pour les structures de $k[\mathrm{G}]-$modules, l'application $f$ est $k[\mathrm{G}]-$linéaire. On dira aussi que $f$ est G$-$linéaire.

*Exemples*

1. Une représentation de G de dimension 1 est définie par un homomorphisme de groupes

$$\rho : \mathrm{G} \to k^*$$

Comme G est fini, les éléments de G sont d'ordre fini : alors l'image d'un si $g \in \mathrm{G}$, $\rho(g)$ est une racine de l'unité.

2. Considérons l'espace vectoriel $\mathrm{V} = k[\mathrm{G}]$. C'est un $k[\mathrm{G}]-$module sur lui-même, et par conséquent on peut lui associer une représentation, définie pour $s$ et $t \in \mathrm{G}$ par

$$\rho(s)(\epsilon_t) = \epsilon_{st}$$

Cette représentation est appelée la représentation régulière ; sa dimension est égale au nombre d'éléments de G.

3. Plus généralement, soit B un ensemble fini. Une action de G sur B est la donnée d'un homomorphisme de groupes

$$\varphi : \mathrm{G} \to \mathfrak{S}(\mathrm{B})$$

de G dans le groupe $\mathfrak{S}(\mathrm{B})$ des permutations de B. Si V est un espace vectoriel de base B, une telle action définit une représentation linéaire $\rho : \mathrm{G} \longrightarrow \mathrm{GL}(\mathrm{V})$ en considérant pour $g \in \mathrm{G}$ l'unique application linéaire inversible $\rho(g)$ qui coïncide avec $\varphi(g)$ sur la base B.

### 4.2. Le théorème de Maschke

DÉFINITION 4.2. — *Soit $\rho$ une représentation d'un groupe fini dans un $k$-espace vectoriel* V. *Un sous-espace vectoriel* $W \subset V$ *est dit* $G-$*invariant si pour tout* $g \in G$ *on a* $\rho(g)(W) \subset W$.

Dans ce cas, la restriction $\rho(g)|_W$ définit une représentation de G, appelée sous-représentation, ou sous- G-module, et le quotient V/W une représentation de G appelée représentation quotient.

*Exemple*
Soit $W = V^G$ le sous-espace vectoriel des $x \in V$ tels que $\rho(g)x = x$ pour tout $g \in G$. Alors le sous-espace $V^G$ est $G-$invariant ; la représentation associée est évidemment la représentation triviale définie par $\rho(g) = \mathrm{id}_W$.

THÉORÈME 4.3. — *Soit* G *un groupe fini d'ordre* $n$. *On suppose que la caractéristique de* $k$ *ne divise pas* $n$. *Soient* V *un* $G-$*module, et* $W \subset V$ *un sous-espace vectoriel* $G-$*invariant. Alors* W *a un supplémentaire* $W'$ *lui-aussi* $G-$*invariant.*

Commençons par un cas particulier. Remarquons que l'hypothèse signifie que $n$ est inversible dans $k$.

LEMME 4.4. — *Soit* V *un* $G-$*module. L'application linéaire* $V \to V$

$$\mu = \frac{1}{n} \sum_{g \in G} \rho(g)$$

*prend ses valeurs dans* $V^G$ *et définit une projection* $V \to V^G$ *; pour tout* $g \in G$, *on a* $\mu \circ \rho(g) = \mu$.

*Démonstration.* Soit $t \in G$. On a pour $x \in V$

$$\begin{aligned} \rho(s)\mu(x) &= \frac{1}{n} \sum_{g \in G} \rho(sg)x \\ &= \frac{1}{n} \sum_{t \in G} \rho(t)x \\ &= \mu(x) \end{aligned}$$

Ceci prouve que $\mu$ prend ses valeurs dans $V^G$. Maintenant si $x \in V^G$, on a $\rho(g)x = x$, et par suite $\mu(x) = \frac{1}{n} nx = x$. Par suite, $\mu$ est une projection. La dernière égalité se vérifie de la même manière que ci-dessus. □

COROLLAIRE 4.5. — *Le sous-espace vectoriel* $\ker \mu$ *est un supplémentaire* $G-$*invariant de* $V^G$.

*Démonstration du théorème 4.3*
Soit $W \subset V$ un sous-espace de V, $G-$invariant. Il s'agit de montrer qu'il existe une projection $p : V \to W$ telle que pour tout $g \in G$ on ait $p\rho(g) = \rho(g)p$ : le noyau d'une telle projection est alors un sous-espace $G-$invariant supplémentaire de W. Considérons l'espace vectoriel $\mathrm{Hom}_k(V, W)$ des applications $k-$linéaires de V dans W. Pour $f \in \mathrm{Hom}_k(V, W)$ on pose $g.f = \rho(g)f\rho(g^{-1})$. Cette formule définit une représentation de G dans $\mathrm{Hom}_k(V, W)$. Le sous-espace invariant est constitué des applications $G-$linéaires de V dans W. Considérons la projection introduite dans le lemme ci-dessus

$$f \mapsto \mu(f) = \frac{1}{n} \sum_{g \in G} g.f$$

Si $f$ est une projection quelconque de V sur W, il découle de cette formule que l'on a $\mu(f)|_W = \mathrm{id}_W$. Par suite $\mu(f)$ est encore une projection, et G−linéaire d'après ce que l'on vient de dire. D'où le théorème.

*Exemple*
On suppose $k = \mathbb{C}$. Etant donnée une représentation V de G, on peut toujours trouver, par le procédé de moyenne ci-dessus, un produit scalaire invariant par G : ceci signifie que les applications $\mathbb{C}$−linéaires $\rho(g)$ sont unitaires. Dans ce cas, l'orthogonal $W^\perp$ d'un sous-espace vectoriel G−invariant W est encore G−invariant.

DÉFINITION 4.6. — *Soient* $(V', \rho')$ *et* $(V'', \rho'')$ *deux représentations d'un groupe fini* G *; la représentation de* G *dans* $V = V' \oplus V''$ *définie par*

$$\rho(g) = \rho'(g) \oplus \rho''(g)$$

*est appelée la somme directe des représentations* $\rho'$ *et* $\rho''$.

On définit de même la somme directe d'une famille finie de représentations linéaires.

DÉFINITION 4.7. — *Une représentation* $\rho$ *dans un espace vectoriel* V *est dite irréductible si* $V \neq 0$ *et si les seuls sous-espaces vectoriels* G−*invariants de* V *sont* $\{0\}$ *et* V.

Une représentation est donc irréductible si et seulement si le $k$[G]−module associé est un module simple. Les représentations de dimension 1 sont évidemment irréductibles. On verra (*cf.* proposition 4.31) que pour tout groupe fini non abélien il existe au moins une représentation irréductible de dimension $> 1$.

THÉORÈME 4.8. — *On suppose que la caractéristique de* $k$ *ne divise pas l'ordre de* G. *Alors toute représentation linéaire de dimension finie de* G *est somme directe de représentations irréductibles.*

*Démonstration.* On raisonne par récurrence sur la dimension. Le théorème est vrai en dimension 1, puisque toute représentation linéaire de dimension 1 est irréductible. Supposons le théorème démontré pour une représentation linéaire de dimension $< m$. Si $\rho$ est une représentation linéaire de G dans un espace vectoriel V le résultat est trivial si cette représentation est irréductible. Sinon, d'après le théorème 4.3 on peut écrire $V = V' \oplus V''$ où $V'$ sont des sous-espaces vectoriels non nuls invariants par $\rho$. Ils définissent des représentations linéaires irréductibles de dimension $< m$ auxquelles on applique l'hypothèse de récurrence. D'où le théorème. □

### 4.3. Lemme de Schur

Dans la suite, toutes les représentations considérées seront de dimension finie. De plus on supposera que la caractéristique de $k$ ne divise pas l'ordre de G.

LEMME 4.9. — *(Lemme de Schur) Soient* $\rho$ *et* $\rho'$ *deux représentations irréductibles de* G. *Tout homomorphisme non nul* $f : \rho \to \rho'$ *est inversible.*

*Démonstration.* La représentation de G définie par $\ker f$ n'est pas égale à $\rho$, donc nulle. La représentation définie par $\mathrm{Im}\, f$ n'est pas nulle, donc égale à $\rho'$. Ainsi, $f$ est un isomorphisme de représentations.

COROLLAIRE 4.10. — *Soit* $\rho$ *une représentation irréductible, et* $\mathsf{End}(\rho)$ *l'algèbre des endomorphisme de* $\rho$. *Alors tout élément non nul de* $\mathsf{End}(\rho)$ *est inversible.*

COROLLAIRE 4.11. — *On suppose que $k$ est algébriquement clos. Si $\rho$ est une représentation de* G *l'inclusion $k \hookrightarrow \mathsf{End}(\rho)$ est un isomorphisme d'algèbres.*

*Démonstration.* Il s'agit de montrer que tout endomorphisme non nul de $\rho$ est une homothétie. Soit $f \in \mathsf{End}(\rho)$ un endomorphisme non nul. Considérons l'algèbre $k[f]$ engendrée par $f$. D'après le corollaire 4.10 ci-dessus, c'est un corps ; c'est donc une extension algébrique de $k$. Puisque $k$ est algébriquement clos, $k = k[f]$ ce qui achève la démonstration. □

COROLLAIRE 4.12. — *A isomorphisme près, il n'y a qu'un nombre fini de représentations irréductibles de* G*, et chacune de ces représentations est de dimension $\leq n$.*

*Démonstration.* Soit $\rho$ une représentation irréductible de G dans un espace vectoriel E. Si $e$ est un vecteur non nul de E, le sous-espace vectoriel $k[\mathrm{G}]e$ doit être égal à E. Autrement dit, l'application canonique $f : k[\mathrm{G}] \to \mathrm{E}$ définie par $e$ est surjective ([1]). Cette application est évidemment G−linéaire, et donc le suite exacte de G−modules

$$0 \to \ker f \to k[\mathrm{G}] \to \mathrm{E} \to 0$$

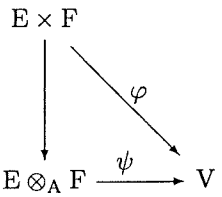
est scindée. Par conséquent E est isomorphe à un sous-module de la représentation régulière, donc $\dim \rho \leq n$. Considérons une décomposition en somme directe de représentations irréductibles $k[\mathrm{G}] = \oplus_i \mathrm{R}_i$. Alors $\mathsf{Hom}(\mathrm{E}, k[\mathrm{G}]) = \oplus \mathsf{Hom}(\mathrm{E}, \mathrm{R}_i)$ puisque le premier membre est non nul, l'un des termes du second membre est aussi non nul. Par suite, E est isomorphe à l'un des $\mathrm{R}_i$. □

### 4.4. Produit tensoriel

On se donne un anneau commutatif et unitaire A, et deux A−modules E et F.

PROPOSITION 4.13. — *Il existe un* A*−module* $\mathrm{E} \otimes \mathrm{F}$ *et une application bilinéaire* $\mathrm{E} \times \mathrm{F} \to \mathrm{E} \otimes_{\mathrm{A}} \mathrm{F}$*, notée* $(x, y) \mapsto x \otimes y$ *satisfaisant à la propriété universelle suivante :*

*Toute application* A*−bilinéaire* $\varphi : \mathrm{E} \times \mathrm{F} \to \mathrm{V}$ *dans un* A*−module* V *se factorise de manière unique suivant le diagramme*




*où $\psi$ est une application* A*-linéaire.*

Ce A−module $\mathrm{E} \otimes_{\mathrm{A}} \mathrm{F}$, muni de l'application bilinéaire $\mathrm{E} \times \mathrm{F} \longrightarrow \mathrm{E} \otimes \mathrm{F}$ définie par $(x, y) \mapsto x \otimes y$ est appelé le produit tensoriel des A−modules E et F. Les éléments de $\mathrm{E} \otimes_{\mathrm{A}} \mathrm{F}$ sont appelés les tenseurs. A cause de l'unicité de la factorisation, les tenseurs sont des sommes de tenseurs de la forme $x \otimes y$ : ces tenseurs sont dits décomposables. Quand il n'y a pas risque de confusion, ce produit tensoriel sera simplement noté $\mathrm{E} \otimes \mathrm{F}$.

*Démonstration.* Soit $\mathrm{A}[\mathrm{E} \times \mathrm{F}] := \mathrm{A}^{(\mathrm{E} \times \mathrm{F})}$ le A−module libre engendré par $\mathrm{E} \times \mathrm{F}$. Les éléments de ce A−module libre sont donc les combinaisons linéaires finies

$$\sum_{(x,y)} \lambda_{(x,y)}(x, y)$$

([1]) Le même argument prouve qu'il n'y a pas de représentation irréductible de dimension infinie

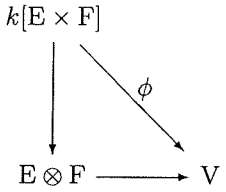
où les $\lambda_{(x,y)}$ sont des scalaires de A nuls sauf un nombre fini d'ntre eux. On considère le sous-module S engendré par les éléments

$$(ax + a'x', y) - a(x, y) - a'(x', y)$$
$$(x, by + b'y') - b(x, y) - b'(x, y')$$

où $x$ et $x'$ sont des éléments de E, $y$ et $y'$ des éléments de F et $a, a', b, b' \in$ A. On pose

$$\mathrm{E} \otimes \mathrm{F} = \mathrm{A}[\mathrm{E} \times \mathrm{F}]/\mathrm{S}$$

et $x \otimes y = \text{classe}(x, y)$. L'application $(x, y) \mapsto x \otimes y$ est évidemment bilinéaire. Vérifions la propriété universelle : $\varphi$ définit une application linéaire $\phi : \mathrm{A}[\mathrm{E} \times \mathrm{F}] \to \mathrm{V}$ qui coïncide avec $\varphi$ sur les éléments de la forme $(x, y)$. Cette application linaire s'annule sur le sous-module S et par conséquent se factorise suivant le diagramme




Il en résulte évidemment que le diagramme de l'énoncé est commutatif. Vérifions l'unicité : si $\psi'$ est une autre application linéaire qui rend commutatif le diagramme de l'énoncé, $\psi$ et $\psi'$ coïncident sur les éléments de la forme $x \otimes y$. D'après la définition de E ⊗ F, ces éléments engendrent E ⊗ F. Par suite $\psi = \psi'$. □

*Fonctorialité*

Considérons des A−modules E, E′, F, F′ et des applications A−linéaire $f$ : E ⟶ E′ et $g$ : F ⟶ F′. L'application E × F ⟶ E′ ⊗ F′ définie par $(x, y) \mapsto f(x) \otimes g(y)$ est bilinéaire, et il existe par conséquent une application linéaire $f \otimes g$ : E ⊗ F ⟶ E′ ⊗ F′ caractérisée par la propriété suivante :

$$(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$$

pour $x \in$ E et $y \in$ F.

PROPOSITION 4.14. — *Si* E *et* F *sont des* A*−modules libres de rang fini sur* A, *il en est de même de* E ⊗ F *et on a* dim E ⊗ F = dim E dim F.

*Démonstration.* Soient $(e_i)$ et $(f_j)$ des bases pour E et F respectivement. Alors les éléments $e_i \otimes f_j$ engendrent E ⊗ F. Par suite E ⊗ F est de type fini. Montrons que ces éléments constituent une base de E ⊗ F. Soient $\lambda_{i,j}$ des scalaires tels que

$$\sum \lambda_{i,j} e_i \otimes f_j = 0.$$

Considérons les bases duales $e^i$ et $f^j$. Alors $(x, y) \mapsto e^i(x) f^j(y)$ est une application bilinéaire sur E × F qui d'après la propriété universelle se factorise en une forme linéaire $\psi_{i,j}$ : E ⊗ F → $k$. En appliquant cette forme linéaire à l'égalité ci-dessus, on trouve $\lambda_{i,j} = 0$. D'où l'énoncé. □

Exercice 4.1

On suppose que E est un A−module libre de rang fini. Soit E* le dual de E. Il existe une application linéaire et une seule $\alpha$ : E ⊗ F → L(E*, F) de E ⊗ F dans le module L(E*, F) des applications linéaires du dual E* dans F telle que pour $x \in$ E, $y \in$ F et $\xi \in$ E* on ait

$$\alpha(x \otimes y) = \xi(x) y.$$

Cette application linéaire est un isomorphisme.

Exercice 4.2
Montrer que si E est un A−module libre de rang $n$, le produit tensoriel $\mathrm{E} \otimes \mathrm{F}$ est isomorphe à $\mathrm{F}^n$.

Exercice 4.3
Soient $\mathfrak{a}$ un idéal de A, et F un A−module. Démontrer que

$$(\mathrm{A}/\mathfrak{a}) \otimes \mathrm{F} \simeq \mathrm{F}/\mathfrak{a}\mathrm{F}$$

Exercice 4.4
Soit $0 \longrightarrow \mathrm{F}' \longrightarrow \mathrm{F} \longrightarrow \mathrm{F}'' \longrightarrow 0$ une suite exacte de A−modules.

1. Montrer que l'on a une suite exacte

$$\mathrm{E} \otimes \mathrm{F}' \longrightarrow \mathrm{E} \otimes \mathrm{F} \longrightarrow \mathrm{E} \otimes \mathrm{F}'' \longrightarrow 0$$

2. Montrer que la première flèche n'est pas en général injective. Montrer que c'est cependant le cas si $\mathrm{F}''$ est un A−module libre.

*Produit tensoriel de représentations*

Si E et E′ sont des $k$−espaces vectoriels de dimension $m$ et $m'$ respectivement, l'espace vectoriel $\mathrm{E} \otimes \mathrm{E}'$ est de dimension $mm'$. Si $u : \mathrm{E} \to \mathrm{E}$ et $u' : \mathrm{E}' \to \mathrm{E}'$ sont des endomorphismes des espaces vectoriels E et E′ respectivement, la propriété universelle du produit tensoriel fournit un endomorphisme

$$u \otimes v : \mathrm{E} \otimes \mathrm{E}' \to \mathrm{E} \otimes \mathrm{E}'$$

caractérisé par la propriété suivante : pour tout $x \in \mathrm{E}, x' \in \mathrm{E}'$ on a $(u \otimes u')(x \otimes x') = u(x) \otimes u'(x')$. Si $u \in \mathrm{GL}(\mathrm{E})$ et $u' \in \mathrm{GL}(\mathrm{E}')$, alors $u \otimes u' \in \mathrm{GL}(\mathrm{E} \otimes \mathrm{E}')$, et l'application

$$\mathrm{GL}(\mathrm{E}) \times \mathrm{GL}(\mathrm{E}') \to \mathrm{GL}(\mathrm{E} \otimes \mathrm{E}')$$

définie par $(u, v) \mapsto u \otimes v$ est un homomorphisme de groupes. Il en résulte en particulier que si $\rho$ et $\rho'$ sont des représentations linéaires de G dans les espaces vectoriels E et E′ on obtient une représentation de G, notée $\rho \otimes \rho'$, définie pour $g \in \mathrm{G}$ par $(\rho \otimes \rho')(g) = \rho(g) \otimes \rho'(g)$
Cette représentation est appelée le produit tensoriel des représentations $\rho$ et $\rho'$.

*Puissance symétrique et puissance extérieure*
Soit E un espace vectoriel. La propriété universelle du produit tensoriel fournit une involution $\sigma : \mathrm{E} \otimes \mathrm{E} \to \mathrm{E} \otimes \mathrm{E}$ et une seule caractérisée par la formule

$$\sigma(x \otimes y) = y \otimes x$$

pour $x$ et $y \in \mathrm{E}$. Supposons que $k$ soit de caractéristique différente de 2. On a une décomposition en somme directe

$$\mathrm{E} \otimes \mathrm{E} = \mathrm{S}^2\mathrm{E} \oplus \wedge^2\mathrm{E}$$

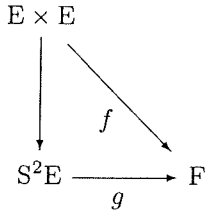
où $\mathrm{S}^2\mathrm{E}$ et $\wedge^2\mathrm{E}$ désignent les sous-espaces vectoriels de $\mathrm{E} \otimes \mathrm{E}$ correspondant aux valeurs propres 1 et $-1$ respectivement. Ces espaces vectoriels, qui sont invariant par l'action naturelle de GL(E), s'appellent puissance symétrique ou produit tensoriel symétrique (resp. alterné, ou puissance extérieure) de E. On pose $xy = \frac{1}{2}(x \otimes y + y \otimes x)$ dans $\mathrm{S}^2\mathrm{E}$ et $x \wedge y = \frac{1}{2}(x \otimes y - y \otimes x)$

PROPOSITION 4.15. — *Si* E *est un espace vectoriel de dimension* $m$, *les espaces vectoriels* $\mathrm{S}^2\mathrm{E}$ *et* $\wedge^2\mathrm{E}$ *sont de dimensions respectives* $\frac{1}{2}m(m+1)$ *et* $\frac{1}{2}m(m-1)$.

*Démonstration.* Soit $(e_i)_{i=1,\ldots,n}$ une base de E. Les tenseurs $e_i e_j =$ pour $i \leq j$ et $e_i \wedge e_j$ pour $i < j$ constituent une base de $\mathrm{S}^2\mathrm{E}$ et $\wedge^2\mathrm{E}$ respectivement. D'où le résultat. □

Exercice 4.5

1. Montrer que tout application bilinéaire symétrique $f : \mathrm{E} \times \mathrm{E} \longrightarrow \mathrm{F}$ se factorise de manière unique suivant le diagramme




où $g$ est une application linéaire, et où l'application verticale est l'application bilinéaire symétrique donnée par $(x, y) \mapsto xy$.

2. Enoncer et démontrer la propriété universelle analogue pour la puissance extérieure $\wedge^2\mathrm{E}$.

Exercice 4.6

Soit $k$ un corps de caractéristique 0.

1. Soit E un $k-$espace vectoriel de dimension $m$. Définir la puissance tensorielle

$$\otimes^n \mathrm{E} = \underbrace{\mathrm{E} \otimes \ldots \otimes \mathrm{E}}_{n \text{ fois}}$$

Montrer que $\otimes^n\mathrm{E}$ a pour dimension $m^n$.

2. Montrer que le groupe symétrique $\mathfrak{S}_n$ opère linéairement sur $\otimes^n\mathrm{E}$.

3. On définit la puissance symétrique $\mathrm{S}^n\mathrm{E}$ comme quotient de $\otimes^n\mathrm{E}$ par le sous-espace vectoriel engendré par les tenseurs $g(u) - u$ pour $u \in \mathrm{E}^{\otimes n}$ et $g \in \mathfrak{S}_n$. On considère l'application $n-$linéaire $\mathrm{E}^i \longrightarrow \mathrm{S}^n\mathrm{E}$ définie par

$$(x_1, \ldots, x_n) \mapsto x_1 \ldots x_n := \mathrm{classe}(x_1 \otimes \ldots \otimes x_n)$$

Montrer que cette application est $n-$linéaire symétrique. Enoncer et démontrer la propriété universelle satisfaite par $\mathrm{S}^n\mathrm{E}$, muni de cette application $n-$linéaire symétrique. Montrer que la puissance symétrique est $\mathrm{GL(E)}-$isomorphe à un sous-espace vectoriel de $\otimes^n\mathrm{E}$ invariant par l'action naturelle de GL(E).

4. Définir de même la puissance extérieure $\wedge^n\mathrm{E}$.

5. Préciser la dimension des espaces vectoriels $\mathrm{S}^n\mathrm{E}$ et $\wedge^n\mathrm{E}$.

6. Soit $f \in \mathsf{End}(\mathrm{E})$, et $\wedge^m f : \wedge^m\mathrm{E} \longrightarrow \wedge^m \mathrm{E}$ l'endomorphisme de $\wedge^m\mathrm{E}$ associé. Montrer que $\wedge^m f$ est l'homothétie de rapport $\det f$.

Si $\rho$ est une représentation linéaire de G dans un espace vectoriel E, le groupe G opère linéairement sur la puissance symétrique $\mathrm{S}^n\mathrm{E}$ et la puissance extérieure $\wedge^n\mathrm{E}$. Ceci définit donc des représentations de G notées $\mathrm{S}^i\rho$ et $\wedge^i\rho$.

*Produit tensoriel de deux anneaux*

Soit A et B deux anneaux commutatifs et unitaires. Le groupe abélien $\mathrm{A} \otimes \mathrm{B}$ peut être muni d'une multiplication $\mathbb{Z}-$bilinéaire caractérisée sur les tenseurs décomposables par la propriété suivante :

$$a \otimes b.a' \otimes b' = aa' \otimes bb'.$$

Cette multiplication a $1 \otimes 1$ pour élément unité. On obtient ainsi un anneau commutatif et unitaire.

Exercice 4.7

Construire un isomorphisme d'anneaux

$$\mathbb{Z}[\mathrm{X}] \otimes \mathbb{Z}[\mathrm{Y}] \simeq \mathbb{Z}[\mathrm{X}, \mathrm{Y}].$$

### 4.5. Caractère d'une représentation

Soit G un groupe fini d'ordre $n$.

DÉFINITION 4.16. — *Soit $\rho$ une représentation linéaire de* G *dans un espace vectoriel* V *de dimension finie. On appelle caractère de $\rho$ la fonction $\chi : \mathrm{G} \to k$ définie par*

$$\chi_\rho(g) = \operatorname{trace} \rho(g).$$

On a $\rho(g)^n = 1$, et $n$ est inversible dans $k$ : cette hypothèse entraîne que le polynôme minimal de $\rho(g)$ (sur la clôture algébrique $\overline{k}$ de $k$) a ses racines distinctes. Ainsi, $\rho(g)$ est diagonalisable sur $\overline{k}$. Si $\lambda_1, \ldots, \lambda_n$ sont les valeurs propres de $\rho(g)$, et $r_i$ leur multiplicité dans le polynôme caractéristique, on a donc

$$\chi_\rho(g) = \sum_{i=1,\ldots,n} r_i \lambda_i$$

PROPOSITION 4.17. — *Soient $\rho$ et $\tau$ deux représentations linéaires de* G *dans des espaces vectoriels* V *et* W *respectivement.*
(1) *Si $\rho$ et $\tau$ sont isomorphes, elles ont même caractère.*
(2) $\chi_\rho(e) = \dim \rho$ *dans* $k$.
(3) $\chi_{\rho+\tau} = \chi_\rho + \chi_\tau$
(4) $\chi_{\rho\otimes\tau} = \chi_\rho \chi_\tau$

*Démonstration.* Soit $f : \rho \to \tau$ un isomorphisme et $(e_i)$ une base de V ; l'espace vectoriel W sera muni de la base $\epsilon_i = f(e_i)$. Dans ces bases les matrices de $\rho(g)$ et $\tau(g)$ sont les mêmes, et par conséquent ces applications linéaires ont même trace, ce qui démontre l'assertion (1). Les assertions (2) et (3) sont évidentes. Vérifions l'assertion (4). Soient V et W les espaces vectoriels correspondant aux représentations $\rho$ et $\tau$. On sait que si $e_i$ et $\epsilon_j$ sont des bases de V et W, les tenseurs $e_i \otimes \epsilon_j$ constituent une base de $\mathrm{V} \otimes \mathrm{W}$. On écrit $\rho(g)(e_i) = \sum_j a_i^j e_j$ et $\tau(g)(\epsilon_\ell) = \sum_t b_\ell^t \epsilon_t$ ; par définition de $\rho \otimes \tau$ on a alors

$$\rho \otimes \tau(g)(e_i \otimes \epsilon_\ell) = \sum_{j,t} a_i^j b_\ell^t e_j \otimes \epsilon_t.$$

Par suite

$$\chi_{\rho\otimes\tau} = \sum_{i,\ell} a_i^i b_\ell^\ell$$

et donc $\chi_{\rho\otimes\tau} = \chi_\rho \chi_\tau$. □

LEMME 4.18. — *Soit $\rho$ une représentation d'un groupe fini d'ordre $n$ dans un espace vectoriel* V, *et* $\mathrm{V}^\mathrm{G}$ *le sous-espace vectoriel des points fixes sous* G. *On suppose que la caractéristique de $k$ ne divise pas $n$. Soit $\chi_\rho$ la caractère de la représentation $\rho$. Alors*

$$\dim \mathrm{V}^\mathrm{G} = \frac{1}{n} \sum_{g\in\mathrm{G}} \chi_\rho(g).$$

*Démonstration.* On sait que $\mathrm{V}^\mathrm{G}$ est l'image de la projection

$$\mu = \frac{1}{n} \sum_{g\in\mathrm{G}} \rho(g).$$

Le lemme est donc une conséquence de la formule $\dim \mathrm{V}^\mathrm{G} = \operatorname{trace} \mu$ et de la linéarité de la trace. □

PROPOSITION 4.19. — *On suppose que la caractéristique de $k$ ne divise pas $n$. Soit $\rho$ et $\tau$ deux représentations de* G *dans des espaces vectoriels* V *et* W *respectivement. On a*

$$\dim \operatorname{Hom}(\tau, \rho) = \frac{1}{n} \sum_{g\in\mathrm{G}} \chi_\rho(g) \chi_\tau(g^{-1})$$

*Démonstration.* La représentation duale $W^*$ de W définie par $g \mapsto^t \tau(g^{-1})$ a pour caractère la fonction

$$g \mapsto \chi_\tau(g^{-1}).$$

Considérons la représentation $\mathrm{Hom}(W, V) = W^* \otimes V$; d'après la proposition 4.17 elle a pour caractère $g \mapsto \chi_\rho(g)\chi_\tau(g^{-1})$. L'espace vectoriel des invariants $\mathrm{Hom}(V, W)^G$ est exactement $\mathrm{Hom}(\tau, \rho)$. La proposition est donc une conséquence immédiate de 4.18.

Exercice 4.8
On suppose que $k$ est de caractéristique différente de 2. Montrer que pour tout $g \in G$

$$\chi_{S^2\rho}(g) = \frac{1}{2}(\chi_\rho(g)^2 + \chi_\rho(g^2)$$

et

$$\chi_{\wedge^2\rho}(g) = \frac{1}{2}(\chi_\rho(g)^2 - \chi_\rho(g^2).$$

Exercice 4.9
Soient B un ensemble fini sur lequel le groupe G opère, V l'espace vectoriel $k[B]$ de base B et $\rho : G \to GL(V)$ la représentation correspondante. Montrer que, pour $g \in G$, $\chi_\rho(g)$ est le nombre de points fixes de $g$.

Considérons sur l'espace vectoriel $k^G$ des fonctions $G \to k$ la forme bilinéaire à valeurs dans $k$ définie par

$$\langle u, v\rangle = \frac{1}{n}\sum_{g\in G} u(g)v(g^{-1})$$

Cette forme bilinéaire est symétrique, et non dégénérée.

*On suppose désormais que le corps k est un corps algébriquement clos, dont la caractéristique ne divise pas l'ordre de* G.

THÉORÈME 4.20. — *Les caractères des représentations irréductibles sont deux à deux orthogonaux, et si $\chi$ est le caractère d'une telle représentation irréductible, on a $\langle\chi, \chi\rangle = 1$.*

*Démonstration.* Si $\rho$ et $\tau$ sont les caractères de deux représentations irréductibles dans les espaces vectoriels V et W respectivement, on a d'après la proposition 4.19

$$\dim \mathrm{Hom}(\tau, \rho) = \langle\chi_\rho, \chi_\tau\rangle$$

Par conséquent, l'énoncé est une conséquence immédiate du lemme de Schur. □

Pour tout entier $r$, $r\rho$ désigne la représentation

$$\underbrace{\rho \oplus \ldots \oplus \rho}_{r \text{ fois}}.$$

Soient $\rho_1, \ldots, \rho_\ell$ des représentants pour les classes d'isomorphisme de représentations irréductibles.

COROLLAIRE 4.21. — *Soit $\rho$ une représentation de* G, *de caractère $\chi$, et*

$$\rho = \sum_i r_i\rho_i$$

*une décomposition en somme directe de représentations irréductibles $\rho_i$, de caractère $\chi_i$. On a*

$$r_i = \langle\chi, \chi_i\rangle.$$

*Démonstration.* On a $\langle\chi, \chi_i\rangle = \sum_j r_j\langle\chi_j, \chi_i\rangle = r_i$. □

COROLLAIRE 4.22. — *L'entier $r_i$ ne dépend pas de la décomposition choisie.*

Cet entier est aussi $\dim \mathrm{Hom}(\rho_i, \rho)$.

COROLLAIRE 4.23. — *Deux représentations de même caractère sont isomorphes.*

En effet, l'entier $r_i$ se calcule à partir du caractère correspondant.

COROLLAIRE 4.24. — *Une représentation $\rho$ de caractère $\chi$ est irréductible si et seulement si $\langle \chi, \chi \rangle = 1$.*

*Démonstration.* Dans la décomposition $\rho = \sum_i r_i \rho_i$, on a alors

$$\sum_i {r_i}^2 = 1$$

Cette égalité entraîne $r_i = 0$ sauf pour un $i$. D'où le résultat. □

*Représentation régulière*

PROPOSITION 4.25. — *Le caractère $\chi_{\mathrm{reg}}$ de la représentation régulière est donné par*

$$\chi_{\mathrm{reg}}(g) = \begin{cases} n \text{ si } g = e \\ 0 \text{ si } g \neq e \end{cases}$$

*Démonstration.* Soit $\rho$ la représentation régulière. L'endomorphisme $\rho(g)$ est l'identité pour $g = e$, et induit une permutation sur les vecteurs de la base G de $k$[G] qui, pour $g \neq e$ ne laisse aucun de ces vecteurs de base invariant. Ainsi, la matrice qui représente l'application linéaire $\rho(g)$ a sa diagonale nulle, donc est de trace nulle. □

COROLLAIRE 4.26. — *Soit $k[\mathrm{G}] = \sum_i r_i \rho_i$ une décomposition de la représentation régulière en somme directe de représentations irréductibles. Alors*

1. *On a $r_i = \dim \rho_i$*
2. *On a $\sum_i {r_i}^2 = n$*
3. *Pour tout $g \neq e$, on a*

$$\sum_i r_i \chi_i(g) = 0$$

*Démonstration.* La définition de la forme bilinéaire $\langle\ ,\ \rangle$ et le corollaire 4.21 montrent que l'on a dans $k$,

$$r_i = \langle \chi_{\mathrm{reg}}, \chi_i \rangle = \frac{n\chi_i(e)}{n} = \dim \rho_i,$$

ce qui implique (1). L'égalité $k[\mathrm{G}] = \sum_i r_i \rho_i$, entraîne l'égalité des caractères $\chi_{\mathrm{reg}} = \sum_i r_i \chi_i$. Si on prend la valeur en un point $g = e$, on obtient (2) et (3) en un point $g \neq e$.

Exercice 4.10

Soit $\rho$ une représentation complexe de G, et $\rho^*$ la représentation duale.

1. Montrer que $\chi_{\rho^*} = \overline{\chi_\rho}$.
2. En déduire que si $\rho$ et $\tau$ sont deux représentations complexes de G

$$\dim \mathrm{Hom}(\tau, \rho) = \frac{1}{n} \sum_{g \in \mathrm{G}} \chi_\rho(g) \overline{\chi_\tau}(g)$$

3. On considère sur l'espace vectoriel $\mathbb{C}^{\mathrm{G}}$ des fonctions sur G à valeurs complexes la forme hermitienne positive non dégénérée définie par

$$(u, v) = \frac{1}{n} \sum_{g \in \mathrm{G}} u(g) \overline{v(g)}$$

Déduire de 2 que les caractères des représentations complexes sont deux à deux orthogonaux et de norme 1 pour cette forme hermitienne.

### 4.6. Fonctions centrales

*Comme ci-dessus, on suppose que le corps k est un corps algébriquement clos, de caractéristique* 0.

Le groupe G opère sur lui-même par l'opération $G \to \mathrm{Aut}(G)$ qui associe à $s \in G$ associe l'automorphisme $g \mapsto sgs^{-1}$. La relation d'équivalence associée est appelée conjugaison, et ses classes d'équivalence, ou orbites, les classes de conjugaison. Une fonction $f : G \to k$ est dite centrale si elle est invariante par conjugaison, c'est-à-dire constante sur les classes de conjugaison. Ceci signifie donc que $f(sgs^{-1}) = f(g)$ pour tout $g \in G$ et $s \in G$. Ainsi, les fonctions centrales forment un espace vectoriel $\mathcal{C}(G)$ de dimension égale au nombre de classes de conjugaison de G.

*Exemples*

(1) Si G est un groupe abélien, les classes de conjugaison sont réduites à un élément.

(2) Soit $\mathfrak{S}_3$ le groupe de permutations d'un ensemble à trois éléments. Alors il y a trois classes de conjugaison : la classe de l'élément neutre, celle des trois transpositions, et celle des deux permutations circulaires.

(3) Le caractère d'une représentation est évidemment une fonction centrale.

THÉORÈME 4.27. — *Les caractères des représentations irréductibles constituent une base orthonormale de* $\mathcal{C}(G)$.

*Démonstration.* En vertu du théorème 4.20, il suffit de démontrer que l'orthogonal du sous-espace engendré par les caractères $(\chi_i)_{i=1\ldots,\ell}$ des représentations irréductibles est réduit à 0. En effet, si $f$ est une fonction centrale,

$$f - \sum_{i=1}^{\ell} \langle f, \chi_i \rangle \chi_i$$

est une fonction orthogonale à tous les $\chi_i$; elle devrait être nulle. Ainsi, les caractères $\chi_i$ engendrent l'espace vectoriel $\mathcal{C}(G)$.

Soient $f : G \to k$ une fonction centrale. Pour toute représentation linéaire $\rho : G \to \mathrm{GL}(V)$ dans un espace vectoriel V on pose

$$f_\rho = \frac{1}{n} \sum_{g \in G} f(g)\rho(g^{-1})$$

On obtient ainsi un endomorphisme de V.

LEMME 4.28. — *Si* $\rho$ *est une représentation irréductible,* $f_\rho$ *est une homothétie de rapport*

$$\frac{1}{\dim \rho} \langle f, \chi \rangle.$$

*Démonstration.* D'après le lemme de Schur, il suffit de vérifier que $f_\rho$ est en fait un endomorphisme de la représentation $\rho$. On a pour tout $h \in G$

$$\begin{aligned} \rho(h) f_\rho \rho(h^{-1}) &= \frac{1}{n} \sum_{g \in G} f(g)\rho(hg^{-1}h^{-1}) \\ &= \frac{1}{n} \sum_{g \in G} f(h^{-1}gh)\rho(g^{-1}) \\ &= f_\rho \end{aligned}$$

Ainsi, $f_\rho$ est une homothétie. Pour calculer le rapport de l'homothétie, il suffit de prendre la trace. Compte-tenu de la définition de la forme bilinéaire $\langle\ ,\ \rangle$ ceci conduit au résultat. □

Terminons maintenant la démonstration du théorème : si $f$ est orthogonal à tous les $\chi_i$, pour toute représentation irréductible $\rho$ on a $f_\rho = 0$. Il en résulte que l'on a la même chose pour toute représentation $\rho$. Si on applique ceci à la représentation régulière on obtient en particulier dans $k[G]$

$$\sum_{g\in G} f(g)g^{-1} = 0$$

Par suite, $f(g) = 0$ pour tout $g \in G$. □

COROLLAIRE 4.29. — *Le nombre $\ell$ de classes d'isomorphisme de représentations irréductibles est égal au nombre de classes de conjugaison de* G.

COROLLAIRE 4.30. — *Soit $g \in G$, et $n(g)$ le nombre d'éléments dans la classe de conjugaison de $g$. On a*

$$\sum_{i=1}^{\ell} \chi_i(g^{-1})\chi_i(g) = \frac{n}{n(g)}$$

*et si $h \in G$ n'est pas conjugué à $g$ :*

$$\sum_{i=1}^{\ell} \chi_i(g^{-1})\chi_i(h) = 0$$

*Démonstration.* On considère la fonction centrale $f$ qui vaut 1 sur la classe de conjugaison de $g$ et 0 sur les autres classes. Alors

$$f = \sum_i \langle f, \chi_i\rangle \chi_i$$

et les coefficients $\langle f, \chi_i\rangle$ sont donnés par la formule

$$\langle f, \chi_i\rangle = \frac{n(g)}{n}\chi_i(g^{-1}).$$

Les deux formules de l'énoncé s'obtiennent alors en prenant les valeurs de $f$ aux points $g$ et $h$ respectivement. □

Exercice 4.11

On considère les représentations complexes de G. Soient $g_1, \ldots, g_\ell$ un système de représentants pour les classes de conjugaison de G, et $n_i$ le nombre d'éléments dans la classe de conjugaison de $g_i$.

1. Montrer que la matrice transposée de la matrice carrée $C = (C_{i,j})$ définie par

$$C_{i,j} = \sqrt{\frac{n_j}{n}}\chi_i(g_j)$$

est unitaire.

2. La matrice C est aussi unitaire. Retrouver à partir de là les relations ci-dessus dans le cas où $k = \mathbb{C}$.

### 4.7. Exemples

(1) Représentations complexes de $G = \mathfrak{S}_3$

Soit $\mathfrak{S}_3$ le groupe des permutations de trois éléments. Soient $\tau$ une transposition, et $\gamma$ une permutation circulaire. On a vu que G a trois classes de conjugaisons : celles de $e$, $\tau$, et $\gamma$. Par conséquent, dans un corps algébriquement clos $k$ de caractéristique 0 il y a trois représentations

complexes irréductibles non isomorphes, auxquelles correspondent trois caractères. Evidemment, il y déjà deux représentations $\rho_1$ et $\rho_2$ de dimension 1, donnés par les homomorphismes $G \to k^*$ correspondant à l'homomorphisme trivial, et à la signature. La troisième représentation irréductible $\rho_i$ est de dimension 2, et la représentation $\rho_1 \oplus \rho_2 \oplus 2\rho_3$ est la représentation régulière. On connaît le caractère de la représentation régulière : on a $\chi_{\text{reg}}(e) = 6$, $\chi_{\text{reg}}(\tau) = 0, \chi_{\text{reg}}(\gamma) = 0$. La relation $\chi_1 + \chi_2 + 2\chi_3 = \chi_{\text{reg}}$ permet de dresser la table des caractères $\chi_i = \chi_{\rho_i}$ de G :

| | e | $\tau$ | $\gamma$ |
|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 |
| $\chi_2$ | 1 | -1 | 1 |
| $\chi_3$ | 2 | 0 | -1 |

Exercice 4.12

Expliquer pourquoi les vecteurs colonnes de la matrice ci-dessus sont deux à deux orthogonaux. Vérifier les relations d'orthogonalité des caractères $\chi_i$.

Exercice 4.13

On considère la représentation $\rho$ de $G = \mathfrak{S}_3$ sur $k^3$ qui permute les vecteurs de base. Considérons la forme linéaire

$$\varphi : k^3 \to k$$

définie par $\varphi(x_i) = \sum_i x_i$.

(1) Vérifier que cette forme linéaire est invariante.

(2) Déterminer le caractère de la représentation $\rho$. Montrer que

$$\rho = \rho_1 \oplus \rho_3$$

Exercice 4.14

On considère la représentation $S^2\rho_3$. Ecrire sa décomposition en somme de composantes irréductibles.

(2) Groupes abéliens

On démontre ici que tout groupe non abélien a au moins une représentation irréductible de dimension $> 1$. Soit $k$ un corps algébriquement clos de caractéristique 0.

PROPOSITION 4.31. — *Soient* G *un groupe fini d'ordre* $n$. *Alors* G *est abélien si et seulement si toutes ses représentations irréductibles sont de dimension* 1.

*Démonstration.* Soient $(\rho_i)_{i=1,\dots,\ell}$ les représentations irréductibles de G, $r_i$ la dimension de $\rho_i$. D'après le corollaire 4.26 on a l'identité

$$\sum_{i=1}^{\ell} r_i^2 = n$$

et le nombre de classes de conjugaison de G est $n$ si et seulement si le groupe G est un groupe abélien. Par suite, on a $n = \ell$ si et seulement si G est un groupe abélien. Ceci équivaut à $r_i = 1$ pour tout $i$. □

COROLLAIRE 4.32. — *Soit* G *un groupe d'ordre* $n$ *contenant un sous-groupe abélien* A, *d'ordre* $a$. *Alors toute représentation irréductible de* G *est de dimension* $\leq \frac{n}{a}$.

*Démonstration.* Soit $\rho$ une représentation irréductible de G dans un espace vectoriel V. Cette représentation fournit par restriction à A une représentation $\rho_A : A \to GL(V)$, dont les composantes irréductibles sont d'après la proposition ci-dessus de dimension 1. Soit $W \subset V$ un sous-espace A−invariant de dimension 1. Considérons le sous-espace vectoriel

$$V' = \sum_{g \in G} \rho(g)(W).$$

Ce sous-espace vectoriel est évidemment non nul et G−invariant. Puisque la représentation $\rho$ est irréductible, on a $V' = V$. D'autre part, si $g' = gs$, avec $s \in A$, on a $\rho(g')(W) = \rho(g)\rho(s)(W) = \rho(g)(W)$. Par conséquent, dans la somme ci-dessus il y a au plus $\frac{n}{a}$ termes distincts, tous de dimension 1, et par suite, la dimension de l'espace vectoriel V est au plus $\frac{n}{a}$. □

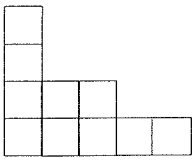
(3) Représentations complexes irréductibles de $\mathfrak{S}_4$.

Considérons le groupe $\mathfrak{S}_n = \mathfrak{S}(E)$ des permutations d'un ensemble E à $n$ éléments. Une partition de $n$ est une suite décroissante d'entiers $\nu_1 \geq \nu_2 \geq \ldots \geq \nu_\ell$ tels que

$$\sum_j \nu_j = n.$$

LEMME 4.33. — *L'ensemble des classes de conjugaison* $\mathfrak{S}(E)$ *est en bijection avec l'ensemble des partitions de n.*

*Démonstration.* Une permutation de E se décompose de manière unique en produit de cycles de supports disjoints. A une telle permutation $f$, on associe les orbites de $f$, dont on ordonne par ordre décroissant le nombre d'éléments, de façon à former un tableau appelé tableau de Young de $f$ :



Ainsi, dans l'exemple ci-dessus, le tableau de Young est celui d'une permutation d'un ensemble E à 10 éléments qui se décompose en produit d'un 4-cycle et de 2 transpositions de supports disjoints. Il est clair que $f \in \mathfrak{S}(E)$ et $g \in \mathfrak{S}(E)$ sont conjuguées, si et seulement si elles ont même tableau de Young. □

On peut associer une autre partition de $n$ à $f$. En effet, soit $\nu_i$ le nombre d'orbites ayant au moins $i$ éléments. Alors $\nu_i$ est décroissante, et $\alpha_i = \nu_i - \nu_{i+1}$ est exactement le nombre d'orbite ayant $i$ éléments. On a alors

$$\sum_{i=1}^{\ell} i\alpha_i = n$$

Il est clair que si l'on forme un tableau à partir de la suite $\nu_i$, ce nouveau tableau s'obtient à partir du précédent en échangeant les lignes et les colonnes.

La partition associée $\nu_i$ de $n$ est appelée partition duale.

Exercice 4.15
Le nombre de partitions $p(n)$ de $n$ se calcule de la manière suivante : le produit

$$\prod_{i\geq 0}\frac{1}{1-t^i} = \sum_{n\geq 0} p(n)t^n$$
$$= 1 + t + 2t^2 + 3t^3 + 5t^4 + 7t^5 + 11t^6 + \dots$$

converge pour $|t| < 1$. Il est donné par la somme de la série figurant au membre de droite.

LEMME 4.34. — *Le nombre d'éléments dans la classe de conjugaison de $f$ est*

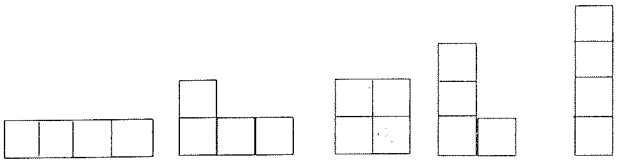
$$\frac{n!}{\prod_j j^{\alpha_j}\alpha_j!}$$

*Démonstration.* Il suffit de trouver le nombre de permutations $g$ qui commutent avec $f$. Soit $C_f$ le sous-groupe des éléments $g$ qui commutent avec $f$. Soit $E_i$ l'ensemble des orbites à $i-$éléments. Une permutation $g \in C_f$ induit une permutation de $E_i$. On a alors un homomorphisme

$$C_f \longrightarrow \prod_i \mathfrak{S}(E_i)$$

dont le noyau est constitué des permutations qui laissent globalement invariant $A_i$ et commute avec $f$. Cet homomorphisme est surjectif, et le noyau a $\prod_j j^{\alpha_j}$ éléments.

Revenons au cas $n = 4$. Il résulte des considérations ci-dessus qu'il y a 5 classes de conjugaison $C_j$, correspondant aux tableaux de Young



On prendra pour représentants les éléments de E étant numérotés et les permutations écrites sous forme de produit de cycles : $g_1 = \mathrm{id}_E, g_2 = (12), g_3 = (12)(34), g_4 = (123), g_5 = (1234)$. D'après la formule ci-dessus le nombre de représentants $n_j$ dans les classes de conjugaison est 1,6,3,8,6. On sait alors qu'il y a 5 représentations irréductibles, toutes de dimension $\leq 6$ puisque le groupe $\mathfrak{S}$ a un sous-groupe abélien d'ordre 4. Il y a deux représentations de dimension 1 : la représentation triviale $\rho_1$, et la représentation $\rho_2$ donnée par la signature. La représentation $w$ associée à l'action de $\mathfrak{S}(E)$ sur E est de dimension 4 mais elle n'est pas irréductible : en effet, le point $\sum_{x\in E} x$ est invariant par $\mathfrak{S}(E)$, et donc la représentation triviale est une sous-représentation et la représentation quotient $\rho_3$ est de dimension 3. Pour voir si cette représentation est irréductible, il suffit de dresser la table des caractères : si on désigne par $\chi_i$ le caractère correspondant à $\rho_i$, on a $\chi_3 = \chi_w - \chi_1$.

| | $C_1$ | $C_2$ | $C_3$ | $C_4$ | $C_5$ |
|---|---|---|---|---|---|
| $n_j$ | 1 | 6 | 3 | 8 | 6 |
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | -1 | 1 | 1 | -1 |
| $\chi_3$ | 3 | 1 | -1 | 0 | -1 |

On en déduit que $(\chi_3, \chi_3) = 1$ et par conséquent $\rho_3$ est bien irréductible. Il en est de même de la repréentation de dimension 3 définie par

$$\rho_4 = \wedge^2\rho_3 = \rho_3 \otimes \rho_2$$

Il reste donc une représentation irréductible, laquelle est obligatoirement de dimension 2. On peut maintenant compléter la table des caractères, on écrivant que $\sum_i r_i\chi_i = \chi_{\text{reg}}$ :

| | $C_1$ | $C_2$ | $C_3$ | $C_4$ | $C_5$ |
|---|---|---|---|---|---|
| $n_j$ | 1 | 6 | 3 | 8 | 6 |
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | -1 | 1 | 1 | -1 |
| $\chi_3$ | 3 | 1 | -1 | 0 | -1 |
| $\chi_4$ | 3 | -1 | -1 | 0 | 1 |
| $\chi_5$ | 2 | 0 | 2 | -1 | 0 |

Table des caractères de $\mathfrak{S}_4$

Pour trouver sous forme explicite la dernière représentation, on remarque que la bitransposition (12)(34) fournit une involution de l'espace vectoriel W associé à cette représentation. Comme elle a pour trace 2, c'est obligatoirement l'identité. Il en résulte que cette représentation provient de la représentation irréductible de dimension 2 de $\mathfrak{S}_3$ par l'homomorphisme

$$\lambda : \mathfrak{S}(E) \longrightarrow \mathfrak{S}_3$$

de noyau le groupe abélien des bitranspositions, isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. Cet homomorphisme $\lambda$ se réalise en considérant l'action, par conjugaison, sur la classe de conjugaison $C_3$ des bitranpositions. Les permutations $\lambda(g_2)$ et $\lambda(g_5)$ sont des transpositions, la permutation $\lambda(g_4)$ est une permutation circulaire. On constate que le caractère de la représentation obtenue à partir de la représentation de dimension 2 de $S_3$ est bien celle qui figure dans le tableau ci-dessus.

(4) Représentations complexes du groupe alterné $\mathfrak{A}_4$.

Le groupe $\mathfrak{A}_4$ des permutations paires agit par conjugaison sur chaque classe de conjugaison $C_i$ de $\mathfrak{S}_4$ : on n'a donc à considérer que les classes de conjugaison $C_1, C_2$ et $C_3$. Les orbites des éléments de $\mathfrak{A}_4$ sont les classes de conjugaison de $\mathfrak{A}_4$. Il est clair que $\mathfrak{A}_4$ agit transitivement sur la classe $C_3$, et il y a deux orbites dans la classe $C_4$ représentée par les cycles (123) et (132). Par suite, il y a 4 classes de conjugaison $C_1, C_3, C_4'$ et $C_4''$, qui contiennent respectivement $1, 3, 4, 4$ éléments. Donc le groupe $\mathfrak{A}_4$ a quatre représentations complexes irréductibles. D'après le lemme qui précède, ces représentations sont de dimension au plus 3.

Considérons le sous-groupe $(\mathbb{Z}/2\mathbb{Z})^2$. Ce sous-groupe est distingué dans $\mathfrak{A}_4$ et le quotient est isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Les représentations qui proviennent de représentation irréductibles de $\mathbb{Z}/3\mathbb{Z}$ sont donnés par les homomorphismes de groupes $\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{C}^*$, c'est-à-dire par une racine cubique de l'unité. Ceci fournit trois représentations irréductibles. La dernière représentation est forcément de dimension 3. On peut maintenant, en utilisant la relation

$$\sum_i r_i\chi_i = \chi_{\text{reg}}$$

dresser la table des caractères. On pose $j = \frac{1}{2}(1 + i\sqrt{3})$.

| | $C_1$ | $C_3$ | $C_4'$ | $C_4''$ |
|---|---|---|---|---|
| $n_j$ | 1 | 3 | 4 | 4 |
| $\chi_1$ | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | $j$ | $j^2$ |
| $\chi_3$ | 1 | 1 | $j^2$ | $j$ |
| $\chi_w$ | 3 | -1 | 0 | 0 |

Table des caractères de $\mathfrak{A}_4$

Il est clair que la représentation $w$ de dimension 3 obtenue est induite par l'une des représentations irréductibles de dimension 3 de $\mathfrak{S}_4$.

Exercice 4.16

Soit $\lambda : \mathfrak{A}_4 \longrightarrow \mathfrak{S}_4$ l'inclusion canonique, et V l'unique représentation irréductible de dimension 2 de $\mathfrak{S}_4$. Trouver la décomposition en facteurs irréductibles de la représentation de $\mathfrak{A}_4$ induite par V .

Exercice 4.17

Soit E un ensemble à $n$ éléments, $w$ la représentation standard de dimension $n$ de $\mathfrak{S}(E)$ dans l'espace vectoriel $W = \mathbb{C}[E]$ engendré par E, et $v$ la représentation quotient de $w$ par la représentation triviale de dimension 1.

1) Démontrer que $v$ est irréductible.

2) Démontrer que pour tout $1 \leq m \leq n-1$ on a

$$\wedge^m w = \wedge^m v \oplus \wedge^{m-1} v.$$

3) Soit $\chi$ le caractère de $w$. Démontrer que $\langle w, w \rangle = 2$.

4) En déduire que la représentation $\wedge^m v$ est irréductible pour $1 \leq m \leq n-1$.

### 4.8. L'anneau des représentations

On considère comme ci-dessus un groupe fini G d'ordre $n$, et un corps algébriquement clos $k$ de caractéristique 0. Considérons l'ensemble Rep(G) des classes d'isomorphisme de $k-$représentations du groupe G, équipé des deux opérations suivantes :

— l'addition définie par la somme directe $\rho \oplus \rho'$;

— la multiplication, définie par le produit tensoriel $\rho \otimes \rho'$.

Ces deux opérations sont associatives et commutatives. L'addition possède un élément neutre définie par la représentation nulle, et la multiplication est munie d'un élément unité, défini par la représentation triviale de dimension 1, souvent notée 1. De plus, l'addition satisfait à la règle de simplication

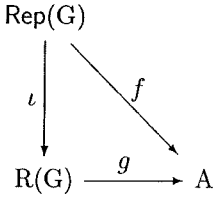
$$\rho \oplus \rho' = \rho \oplus \rho'' \Rightarrow \rho' = \rho''.$$

Ceci se voit par exemple en examinant les caractères correspondants, compte-tenu des formules 4.17. Il en résulte que l'on peut plonger cet ensemble dans un anneau commutatif R(G), obtenu comme quotient de l'ensemble des couples $(\rho, \tau)$ où $\rho \in \mathrm{Rep(G)}$ et $\tau \in \mathrm{Rep(G)}$ par la relation d'équivalence

$$(\rho, \tau) \sim (\rho', \tau') \Leftrightarrow \rho \oplus \tau' = \rho' \oplus \tau$$

muni des opérations évidentes : la construction est analogue à celle de $\mathbb{Z}$ à partir de $\mathbb{N}$. L'application $\iota : \mathrm{Rep(G)} \longrightarrow \mathrm{R(G)}$ qui associe la classe de $(\rho, 0)$ est injective et compatible avec l'addition et la multiplication ; tout élément de R(G) s'écrit sous la forme $\iota(\rho) - \iota(\tau)$ où $\rho$ et $\tau \in \mathrm{Rep(G)}$. Dans la suite, on identifiera Rep(G) avec son image dans R(G).

PROPOSITION 4.35. — *L'anneau* R(G) *possède la propriété universelle suivante : pour toute application* $f : \mathrm{Rep(G)} \longrightarrow \mathrm{A}$ *dans un anneau commutatif* A *compatible avec l'addition et la multiplication, il existe un unique homomorphisme d'anneaux* $g : \mathrm{R(G)} \longrightarrow \mathrm{A}$ *rendant commutatif le diagramme suivant*



L'homomorphisme $g$ est en effet défini par $g([\rho,\tau]) = f(\rho) - f(\tau)$ : on vérifie que le second membre ne dépend pas du choix du représentant $(\rho,\tau)$ de la classe $[\rho,\tau]$.

DÉFINITION 4.36. — *L'anneau* $\mathrm{R}(\mathrm{G})$, *muni de l'inclusion* $\mathsf{Rep}(\mathrm{G}) \hookrightarrow \mathrm{R}(\mathrm{G})$, *s'appelle l'anneau des représentations de* G. *Les éléments de* $\mathrm{R}(\mathrm{G})$ *sont souvent appelées représentations virtuelles.*

Considérons par exemple l'application $\mathsf{Rep}(\mathrm{G}) \mapsto \mathcal{C}(\mathrm{G})$ qui associe à $\rho$ le caractère $\chi_\rho$. Cette application est compatible avec la somme et le produit des représentations d'après la proposition 4.17. Elle s'étend donc en un homomorphisme d'anneaux $\chi : \mathrm{R}(\mathrm{G}) \longrightarrow \mathcal{C}(\mathrm{G})$. Par composition avec la forme bilinéaire symétrique sur $\mathcal{C}(\mathrm{G})$, on obtient une application $\mathbb{Z}-$bilinéaire symétrique

$$\mathrm{R}(\mathrm{G}) \times \mathrm{R}(\mathrm{G}) \longrightarrow \mathbb{Z}$$

définie par $(\rho,\tau) \mapsto \langle \chi_\rho, \chi_\tau \rangle$ qui sera encore notée $\langle \rho,\tau \rangle$.

PROPOSITION 4.37. — *Soit* $\mathsf{Irr}(\mathrm{G})$ *l'ensemble des classes d'isomorphisme de représentations irréductibles de* G.

(1) *Le groupe additif* $\mathrm{R}(\mathrm{G})$ *est un groupe abélien libre de base* $\mathsf{Irr}(\mathrm{G})$.

(2) *L'homomorphisme* $\chi : \mathrm{R}(\mathrm{G}) \longrightarrow \mathcal{C}(\mathrm{G})$ *est injectif.*

*Démonstration.* Il est clair que $\mathsf{Irr}(\mathrm{G})$ engendre $\mathrm{R}(\mathrm{G})$. Montrons que ces éléments sont indépendants. Considérons une relation

$$\sum_{\rho \in \mathsf{Irr}(\mathrm{G})} a_\rho \rho = 0$$

à coefficients $a_\rho \in \mathbb{Z}$. Par application de la forme linéaire $\langle \rho, - \rangle$ on obtient $a_\rho = 0$. Considérons la forme quadratique $\rho \mapsto q(\rho) = \langle \rho, \rho \rangle$. Elle s'écrit dans la base $\mathsf{Irr}(\mathrm{G})$ ci-dessus

$$q\Big(\sum_{\rho \in \mathsf{Irr}(\mathrm{G})} a_\rho \rho\Big) = \sum_{\rho \in \mathsf{Irr}(\mathrm{G})} {a_\rho}^2$$

Elle est donc non dégénérée. Par suite, $\chi$ est injective. □

THÉORÈME 4.38. — *L'homomorphisme* $\chi$ *induit un isomorphisme de* $k-$*algèbres*

$$\phi : \mathrm{R}(\mathrm{G}) \otimes k \longrightarrow \mathcal{C}(\mathrm{G})$$

*Démonstration.* La structure d'anneau sur $\mathrm{R}(\mathrm{G}) \otimes k$ a été définie dans la section 4.4. La structure de $k-$algèbre s'obtient en considérant l'homomorphisme $k \longrightarrow \mathrm{R}(\mathrm{G}) \otimes k$ défini par $\lambda \longrightarrow 1 \otimes \lambda$. L'application $\phi$ est obtenue en appliquant la propriété universelle qui définit le produit tensoriel à l'application bilinéaire $(\rho,\lambda) \mapsto \lambda\chi_\rho$. Ainsi, par définition, pour $\rho \in \mathsf{Rep}(\mathrm{G})$ et $\lambda \in k$, on a $\phi(\rho \otimes \lambda) = \lambda\chi_\rho$. Il résulte de la définition de la structure d'anneau sur $\mathrm{R}(\mathrm{G}) \otimes k$ que $\phi$ est un homomorphisme d'anneaux. Les deux membres héritent en particulier d'une structure de $k-$espace vectoriels de dimension finie ; l'application

$$\mathrm{R}(\mathrm{G}) \longrightarrow \mathrm{R}(\mathrm{G}) \otimes k$$

définie par $\rho \mapsto \rho \otimes 1$ transforme la base $\mathsf{Irr}(\mathrm{G})$ du $\mathbb{Z}-$module libre $\mathrm{R}(\mathrm{G})$ en une base du $k-$espace vectoriel $\mathrm{R}(\mathrm{G}) \otimes k$. D'après le théorème 4.27, cette base est transformée par $\phi$ en la base $(\chi_\rho)_{\rho \in \mathsf{Irr}(\mathrm{G})}$ de $\mathcal{C}(\mathrm{G})$. Par suite $\phi$ est un isomorphisme. □

### 4.9. L'algèbre $k[G]$

Désignons par $\rho_\alpha : G \to GL(R_\alpha)$ des représentants pour les classes d'isomorphisme de représentations irréductibles de G. Par la propriété universelle de l'algèbre $k[G]$ on obtient des homomorphismes d'algèbres $\rho_\alpha : k[G] \to \mathsf{End}_k(R_\alpha)$ et par suite un homomorphisme d'algèbres

$$\nu : k[G] \to \prod_\alpha \mathsf{End}_k(R_\alpha)$$

PROPOSITION 4.39. — *L'homomorphisme d'algèbres ainsi défini est un isomorphisme.*

*Démonstration.* Montrons d'abord la surjectivité. Si ce morphisme n'était pas surjectif, son image serait contenue dans un hyperplan, et si on choisit dans chaque espace vectoriel $R_\alpha$ une base, on aurait une relation non triviale entre les éléments des matrices des applications linéaires $\rho_\alpha(g)$ :

$$\sum_{\alpha,j,k} a^j_{\alpha,k}\rho_\alpha(g)^k_j = 0 \tag{1}$$

avec $a^j_{\alpha,k} \in k$. Or, pour toute application $k-$linéaire $f : R_\beta \longrightarrow R_\alpha$ l'application linéaire $\frac{1}{n}\sum_g \rho_\alpha(g) f \rho_\beta(g^{-1})$ est G−linéaire, donc nulle si $\alpha \neq \beta$. Si $\alpha = \beta$ on a une somme directe de représentations

$$\mathsf{End}(R_\alpha) = k\mathrm{id}_{R_\alpha} \oplus \mathsf{End}_0(R_\alpha)$$

où $\mathsf{End}_0(R_\alpha)$ désigne les endomorphismes de trace nulle ; la sous-représentation triviale $k\mathrm{id}_{R_\alpha}$ est le sous-espace vectoriel des points fixes. Par suite, on a encore

$$\frac{1}{n}\sum_g \rho_\alpha(g) f \rho_\alpha(g^{-1}) = 0$$

si $f$ est de trace nulle. Si on applique ceci à l'application $f$ dont la matrice a un seul élément non nul égal à 1, on obtient les relations

$$\frac{1}{n}\sum_{g\in G} \rho_\alpha(g)^k_j \rho_\beta(g^{-1})^i_\ell = \begin{cases} \frac{1}{\dim \rho_\alpha} \text{ si } \alpha = \beta, i = j, \text{ et } k = \ell \\ 0 \text{ autrement} \end{cases}$$

En multipliant l'égalité (1) par $\rho_\beta(g^{-1})^i_\ell$ et en sommant par rapport à $g \in G$ on obtient alors pour tout $\alpha, \ell, i$

$$\frac{1}{\dim \rho_\alpha} a^i_{\alpha,\ell} = 0$$

ce qui fournit une contradiction puisque l'un des coefficients est non nul par hypothèse. Pour voir que $\nu$ est en fait un isomorphisme, il suffit de constater que les deux membres ont même dimension. Mais si l'on pose $r_\alpha = \dim \rho_\alpha$, ceci résulte de la formule

$$n = \sum_\alpha r_\alpha^2,$$

déjà vue dans le corollaire 4.26. □

*Le centre de l'algèbre $k$[G]*

Il s'agit des éléments $u \in k$[G] qui commutent avec tous les éléments de $k$[G]. C'est une sous-algèbre commutative. Etant donnée une classe de conjugaison $c \in$ G, on pose dans $k$[G]

$$e_c = \sum_{g \in c} g$$

LEMME 4.40. — *Le centre de $k$[G] est le sous-espace vectoriel engendré par les éléments $e_c$.*

*Démonstration.* Evidemment, tout élément $e_c$ appartient au centre de $k$[G]. Réciproquement, un élément $u$ du centre s'écrit $u = \sum_g u_g g$ avec $u_{hgh^{-1}} = u_g$ pour tout $g$ et $h \in$ G. Autrement dit, $g \mapsto u_g$ est constante sur les classes de conjugaison de G. Choisissons, pour chaque classe de conjugaison $c$ un représentant $g_c$ et posons $u_c = u_{g_c}$. Alors

$$u = \sum_c u_c e_c$$

et donc $u$ appartient au sous-espace vectoriel engendré par les éléments $e_c$.

LEMME 4.41. — *Le sous-groupe abélien engendré par les éléments $e_c$ est un sous-anneau commutatif de $k$[G].*

*Démonstration.* Il suffit de constater que ce sous-groupe contient l'élément unité, et qu'il reste stable par multiplication. Mais si $c'$ et $c''$ sont deux classes de conjugaisons, on a

$$e_{c'} e_{c''} = \sum_{g' \in c', g'' \in c''} g'g''$$

L'ensemble des éléments obtenus comme produits $g'g''$, avec $g' \in c'$ et $g'' \in c''$ est stable par conjugaison, et par suite une réunion de classes de conjugaison. Par suite, le produit $e_{c'} e_{c''}$ ci-dessus est une somme, à coefficients entiers, d'éléments $e_c$. □

*Entiers algébriques*

Rappelons la notion d'entier algébrique déjà vue au chapitre 1.

DÉFINITION 4.42. — *Soit* A *un anneau commutatif. Un élément $x \in$ A est dit entier (algébrique) sur $\mathbb{Z}$ s'il existe des entiers $a_1, \ldots, a_n \in \mathbb{Z}$ tels que*

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0.$$

LEMME 4.43. — *Soit $x$ un nombre rationnel. Si $x$ est entier algébrique, c'est un entier.*

Cette propriété dit que $\mathbb{Z}$ est intégralement clos (*cf.* §3.4).

PROPOSITION 4.44. — *Soit* A *un anneau commutatif, et $x \in$ A. Les conditions suivantes sont équivalentes :*

(1) *L'élément $x$ est entier sur $\mathbb{Z}$.*
(2) *Le sous-anneau $\mathbb{Z}[x]$ engendré par $x$ est un groupe abélien de type fini.*
(3) *Il existe un sous-groupe abélien de type fini de* A *qui contient $\mathbb{Z}[x]$.*

Cet énoncé a déjà été vu dans la section §1.2. Dans le situation ci-dessus, on peut en donner une démonstration légèrement différente, qui utilise les propriétés des groupes abéliens de type fini :

*Démonstration.* Evidemment, (2) $\Rightarrow$ (3). Puisque $\mathbb{Z}$ est un anneau noethérien, un sous-module d'un module de type fini est encore de type fini, donc (3) $\Rightarrow$ (2). Si $x$ est entier sur $\mathbb{Z}$, il satisfait à une équation

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0.$$

avec $a_i \in \mathbb{Z}$. Alors le sous-groupe abélien engendré par $(1, x, \ldots, x^{n-1})$ est stable par multiplication par $x$, et donc coïncide avec $\mathbb{Z}[x]$. Donc ce groupe abélien est de type fini. Ce montre l'implication (1) $\Rightarrow$ (2). Réciproquement, soit $\mathrm{A}_n$ le groupe abélien engendré par $(1, x, \ldots, x^{n-1})$. Alors la suite $\mathrm{A}_n$ est croissante, et sa réunion est $\mathbb{Z}[x]$. Puisque $\mathbb{Z}[x]$ est de type fini, cette suite est stationnaire pour $n$ assez grand. Alors, pour un tel $n$ on a $x^n \in \mathrm{A}_n$, ce qui signifie que $x$ est entier sur $\mathbb{Z}$. Ainsi, (2) $\Rightarrow$ (1) □

COROLLAIRE 4.45. — *Soit* A *un anneau commutatif. S'il engendré, comme groupe abélien, par un nombre fini d'éléments, tout élément de* A *est entier sur* $\mathbb{Z}$.

COROLLAIRE 4.46. — *Soit* A *un anneau commutatif. L'ensemble des éléments* $x \in \mathrm{A}$ *qui sont entiers sur* $\mathbb{Z}$ *est un sous-anneau de* A.

*Démonstration.* Soient $x$ et $y \in \mathrm{A}$ deux entiers sur $\mathbb{Z}$. Alors le sous-anneau $\mathbb{Z}[x]$ est engendré (comme groupe abélien) par $(1, x, \ldots, x^n)$ pour $n$ assez grand ; de même, $\mathbb{Z}[y]$ est engendré par $(1, y, \ldots, y^p)$ avec $p$ assez grand. Alors le sous-anneau $\mathbb{Z}[x, y]$ engendré par $x$ et $y$ est engendré par les éléments $x^i y^j$, avec $i \leq n, j \leq p$. Donc c'est un groupe abélien de type fini. Il en résulte que $x + y$ et $xy$ sont entiers algébriques. D'où le corollaire. □

*Propriétés d'intégralité des caractères*
Elle vont découler de propriétés d'intégralité de certains éléments du centre de $k[\mathrm{G}]$.

PROPOSITION 4.47. — *Soit* $u = \sum_{g \in \mathrm{G}} u_g g$ *un élément du centre de* $k[\mathrm{G}]$, *avec* $u_g \in k$ *entier sur* $\mathbb{Z}$. *Alors* $u$ *est entier sur* $\mathbb{Z}$.

*Démonstration.* L'élément $u$ s'écrit encore $u = \sum_c u_{g_c} e_c$. Il suffit donc de vérifier que chacun des éléments $e_c$ est entier sur $\mathbb{Z}$. Mais d'après le lemme 4.41, ces éléments appartiennent à un sous-anneau du centre, qui en tant que groupe abélien est de type fini. D'après la proposition 4.44, ces éléments sont entiers sur $\mathbf{Z}$. □

PROPOSITION 4.48. — *Soit* $\rho$ *une représentation de* G *de caractère* $\chi$. *Alors, pour tout* $g \in \mathrm{G}$, *l'élément* $\chi(g) \in k$ *est entier sur* $\mathbf{Z}$.

*Démonstration.* On sait que $\rho(g)^n = 1$, par conséquent les valeurs propres de $\rho(g)$ sont entières sur $\mathbb{Z}$. Il en est de même de la trace. □

LEMME 4.49. — *Soit* $\rho : \mathrm{G} \to \mathrm{GL(R)}$ *une représentation irréductible de* G, *de dimension* $r$ *et de caractère* $\chi$. *Alors le morphisme canonique d'algèbres* $\nu : k[\mathrm{G}] \to \mathsf{End}_k(\mathrm{R})$ *envoie un élément* $\sum_g u_g g$ *du centre de* $k[\mathrm{G}]$ *sur l'homothétie de rapport*

$$\frac{1}{r} \sum_{g \in \mathrm{G}} u_g \chi(g)$$

*Démonstration.* Cet homomorphisme, surjectif d'après la proposition 4.39, envoie évidemment le centre de $k[\mathrm{G}]$ sur le centre de $\mathsf{End}_k(\mathrm{R})$ : ce centre est constitué des homothéties $\mathrm{R} \to \mathrm{R}$.

Ainsi, si l'élément $u = \sum_{g\in G} u_g g$ appartient au centre de $k[G]$, $\nu(u)$ est l'homothétie de rapport $\frac{1}{r}\sum_{g\in G} u_g\chi(g)$. (On peut aussi invoquer le lemme de Schur pour la représentation irréductible $\rho$, ce qui évite l'usage de la proposition 4.39). □

PROPOSITION 4.50. — *Soit $\rho$ est une représentation irréductible de G de dimension $r$ et caractère $\chi$. Si $u = \sum_{g\in G} u_g g$ un élément du centre de $k[G]$, avec $u_g \in k$ entier sur $\mathbb{Z}$ l'élément*

$$\frac{1}{r}\sum_{g\in G} u_g\chi(g)$$

*est entier sur $\mathbb{Z}$.*

*Démonstration.* Cet élément est l'image de $u$ par l'homomorphisme d'algèbres

$$\text{Centre}(k[G]) \to k$$

induit par l'homomorphisme $\nu : k[G] \to \text{End}_k(R)$. Puisque $u$ est entier sur $\mathbb{Z}$, il en est de même de son image. □

COROLLAIRE 4.51. — *La dimension $r$ d'une représentation irréductible $\rho$ divise l'ordre $n$ du groupe G.*

*Démonstration.* Soit $\chi$ le caractère de $\rho$. On considère l'élément du centre de G défini par

$$u = \sum_{g\in G} \chi(g^{-1})g.$$

Les coefficients $\chi(g^{-1})$ sont entiers sur $\mathbb{Z}$. Donc d'après la proposition qu'on vient de démontrer, l'élément

$$\frac{1}{r}\sum_{g\in G} \chi(g^{-1})\chi(g)$$

est entier sur $\mathbb{Z}$. Cet élément est aussi $\frac{n}{r}\langle\chi,\chi\rangle$ et $\langle\chi,\chi\rangle = 1$ puisque la représentation est irréductible. Ainsi, le nombre rationnel $\frac{n}{r}$ est entier sur $\mathbb{Z}$. D'après le lemme 4.43, c'est un entier relatif : ainsi, $r$ divise $n$.

On appelle centre de G l'ensemble C des éléments $g \in G$ qui commutent avec tout autre élément de G. C'est donc le noyau de l'homomorphisme de groupes $G \to \text{Aut}(G)$ qui associe à $g$ l'automorphisme $h \mapsto ghg^{-1}$. C'est un groupe abélien, qui est distingué dans G. L'indice de C est le nombre d'éléments dans le quotient G/C. La proposition ci-dessus améliore encore le corollaire 4.51 :

PROPOSITION 4.52. — *La dimension $r$ d'une représentation irréductible $\rho : G \to GL(E)$ divise l'indice du centre C dans G.*

La démonstration qui suit est due à J. Tate.

*Démonstration.* Soit $m$ un entier $\geq 2$. On utilise le produit tensoriel

$$\otimes^m E = \underbrace{E\otimes\ldots\otimes E}_{m\text{fois}},$$

et on considère la représentation $\rho^{(m)}$ du groupe $G^m$ dans $\otimes^m E$ définie par $(g_1,\ldots,g_m) \mapsto \rho(g_1)\otimes\ldots\otimes\rho(g_m)$. Son caractère est donné par la fonction $G^m \to k$ définie par

$$(g_1,\ldots,g_m) \mapsto \chi(g_1)\ldots\chi(g_m)$$

et le critère d'irréductibilité 4.24 montre que cette représentation est irréductible. Pour $g \in C$ l'endomorphisme $\rho(g)$ commute avec tous les $\rho(h)$ ; puisque $\rho$ est irréductible, il résulte du lemme de Schur que c'est une homothétie. Alors pour $(g_1, \ldots, g_m) \in C^m$, $\rho^{(m)}(g_1, \ldots, g_m)$ est une homothétie, et si $g_1 \ldots g_m = e$ c'est l'identité. Ainsi, si on considère le sous-groupe S de $C^m$ des éléments $(g_1, \ldots, g_m)$ satisfaisant à $g_1 \ldots g_m = e$, ce sous-groupe est distingué dans $G^m$, et la représentation $\rho^{(m)}$ se factorise en une représentation

$$G^m/S \to GL(\otimes^m E)$$

Cette représentation est encore irréductible. Par conséquent, on peut appliquer le corollaire 4.51. Si $c$ est l'ordre de C, l'ordre de S est $c^{m-1}$, et celui de $G^m/S$ est $\dfrac{n^m}{c^{m-1}}$. On obtient donc que pour tout entier $m \geq 2$, $r^m$ divise $\dfrac{n^m}{c^{m-1}}$.

Posons $q = \dfrac{n}{r}$. C'est un entier, et pour $m \geq 2$, $c^{m-1}$ divise $q^m$. Nous allons montrer que ceci implique que $c$ divise $q$, ce qui est équivalent à $r$ divise $n/c$ : c'est exactement le résultat de l'énoncé. Considérons un facteur premier $p$ de $c$, et écrivons $q = p^a q'$, $c = p^b c'$ avec $q'$ et $c'$ entiers non divisibles par $p$. On a alors $b(m-1) \leq am$ pour tout $m \geq 2$, ce qui entraîne évidemment $b \leq a$. Par suite, $p^b$ divise $q$. Si on fait cette manipulation avec tous les facteurs premiers de $c$, on obtient que $c$ divise $q$. □

### 4.10. Représentations du groupe symétrique

Soit $k$ un corps algébriquement clos de caractéristique 0.

Considérons le groupe $G = \mathfrak{S}(E)$ des permutations d'un ensemble E à $n$ éléments. On a vu que l'ensemble de Irr(G) est en bijection avec l'ensemble des classes de conjugaison de G, et donc l'ensemble des partitions de $n$. On se propose de construire pour toute partition $\lambda$ de $n$ une représentation irréductible $V_\lambda$ de G.

On considère pour ceci le tableau de Young $T_\lambda$ associé à $\lambda$, dont les cases sont numérotées comme ci-dessous, et représentent les éléments de E.

| | | | | |
|---|---|---|---|---|
| 4 | | | | |
| 3 | | | | |
| 2 | 6 | 8 | | |
| 1 | 5 | 7 | 9 | 10 |

On considère le sous-groupe $P_\lambda$ (resp. $Q_\lambda$) de G des éléments $g$ qui laissent invariant les colonnes (resp. les lignes). Ainsi, dans l'exemple de tableau de Young ci-dessus ci-dessus, les éléments étant numérotés de 1 à 10, le groupe $P_\lambda$ est le groupe $\mathfrak{S}(\{1,2,3,4\}) \times \mathfrak{S}(\{5,6\}) \times \mathfrak{S}(\{7,8\})$ ; le groupe $Q_\lambda$ est $\mathfrak{S}(\{1,5,7,9,10\}) \times \mathfrak{S}(\{2,6,8\})$. Si on changeait la numérotation, les groupes $P_\lambda$ et $Q_\lambda$ sont remplacés par des groupes conjugués sous la même permutation de $\mathfrak{S}(E)$.

On pose dans l'algèbre $A = k[G]$ du groupe symétrique

$$a_\lambda = \sum_{g \in P_\lambda} g \; ; \; b_\lambda = \sum_{g \in Q_\lambda} \epsilon(g) g$$

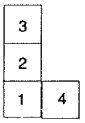
où $\epsilon(g)$ est la signature de la permutation $g$. Ces éléments dépendent de la façon qu'on a choisie de numéroter les cases.

DÉFINITION 4.53. — *L'élément $c_\lambda = a_\lambda b_\lambda$ de $A = k[G]$ s'appelle symétriseur de Young associé à $\lambda$.*

On considère l'idéal (à gauche) $Ac_\lambda$ engendré par $c_\lambda$. Cet idéal peut être vu comme un $k[G]-$module à gauche et donc comme une représentation $V_\lambda$ de G. Si on change la numérotation l'élément $c_\lambda$ est remplacé par un élément conjugué, et la représentation alors obtenue est remplacée par une représentation isomorphe ; donc, la classe d'isomorphisme $[V_\lambda]$ ne dépend en fait que de la partition $\lambda$.

THÉORÈME 4.54. —
(i) *La représentation* $V_\lambda = Ac_\lambda$ *est irréductible.*
(ii) *L'application* $\lambda \mapsto [V_\lambda]$ *de l'ensemble* $\mathrm{Part}(n)$ *des partitions de* $n$ *dans* $\mathrm{Irr}(G)$ *est bijective.*

Exemples
— Si $\lambda = (n)$, le groupe $P_\lambda$ est G lui-même et le groupe $Q_\lambda$ est réduit à l'élément neutre Alors $a_\lambda = \sum_{g\in G} g$ et $V_\lambda = ka_\lambda$ est la représentation triviale de dimension 1.
— Si $\lambda = (1,\dots,1)$, le groupe $P_\lambda$ est réduit à l'identité, et le groupe $Q_\lambda$ est le groupe symétrique. Alors $c_\lambda = \sum_g \epsilon(g)g$. Alors $V_\lambda$ est la représentation alternée de dimension 1.
— Considérons pour $n = 4$ la partition définie par le diagramme de Young ,




Le groupe $P_\lambda$ est isomorphe au groupe des permutations $\mathfrak{S}_3$ des éléments $\{1,2,3\}$, et le groupe $Q_\lambda$ est le groupe engendré par la transposition (14). Le symétriseur de Young est

$$c_\lambda = \sum_{g\in\mathfrak{S}_3} g.(1-(14))$$

Puisque $gc_\lambda = c_\lambda$ pour tout $g \in P_\lambda$, l'espace vectoriel $V_\lambda$ est engendré par les vecteurs $c_\lambda, (14)c_\lambda, (24)c_\lambda, (34)c_\lambda$. Ces vecteurs ne sont pas indépendants : le lemme qui suit montre en effet que $((14)+(24)+(34))c_\lambda$ est de la forme $\alpha c_\lambda$, où $\alpha \in k$.

Exercice 4.18
1) Démontrer que $(14)c_\lambda$, $(24)c_\lambda$, et $(34)c_\lambda$ forment une base de $V_\lambda$.
2) Trouver le caractère de $V_\lambda$. En déduire que $V_\lambda$ est isomorphe à la représentation $\rho$ quotient de la représentation standard de dimension 4 par la représentation triviale de dimension 1.

La démonstration du théorème fait appel à deux lemmes.

LEMME 4.55. —
(i) *Pour* $p \in P_\lambda$ *et* $q \in Q_\lambda$ *on a*

$$\begin{aligned} pa_\lambda &= a_\lambda p = a_\lambda \\ qb_\lambda &= b_\lambda q = \epsilon(q)b_\lambda \\ pc_\lambda q &= \epsilon(q)c_\lambda \end{aligned}$$

(ii) *Soit* $u \in k[G]$ *tel que pour tout* $p \in P_\lambda$ *et* $q \in Q_\lambda$ *on ait* $puq = \epsilon(q)u$. *Alors il existe* $\alpha \in k$ *tel que* $u = \alpha c_\lambda$.

*Démonstration.* L'assertion (i) est évidente. Démontrons (ii). Ecrivons $u = \sum_{g\in G} u_g g$ dans $k[G]$ où $u_g \in k$. Alors $u_{pgq} = \epsilon(q)u_g$ pour tout $p \in P_\lambda$ et $q \in Q_\lambda$. Il suffit de montrer que $u_g = 0$ si $g \notin P_\lambda Q_\lambda$, car du fait que $P_\lambda \cap Q_\lambda = \{1\}$, un élément $g \in G$ s'écrit au plus d'une façon $g = pq$ où $p \in P_\lambda$ et $q \in Q_\lambda$ et on aura alors

$$u = u_1 \sum_{(p,q)\in P_\lambda \times Q_\lambda} \epsilon(q)pq = u_1 c_\lambda$$

Soit donc $g \notin P_\lambda Q_\lambda$. Il suffit de montrer qu'il existe une transposition $t \in P_\lambda$ telle que la transposition $t' = g^{-1}tg \in Q_\lambda$. En effet on aura alors $tgt' = g$ ; de la propriété d'invariance, on tire $u_g = -u_g$ et donc $u_g = 0$.

Montrons l'existence d'une transposition $t \in P_\lambda$ telle que la transposition $t' = g^{-1}tg$ appartienne au sous-groupe $Q_\lambda$. Sinon, pour toute transposition $t \in P_\lambda$ on aurait $g^{-1}tg \notin Q_\lambda$ et par conséquent pour toute paire de cases distinctes $\{i, j\}$ dans une même colonne du tableau de Young $T_\lambda$, les cases $g^{-1}(i)$ et $g^{-1}(j)$ appartiendraient à des lignes distinctes. On travaille d'abord avec la première colonne. Alors pour $1 \leq i \leq \lambda_1$, les cases $g^{-1}(i)$ appartiennent à des lignes deux à deux distinctes. On peut alors trouver $q_1 \in Q_\lambda$ tel que les cases $q_1 g^{-1}(i)$ soient dans la première colonne et deux distinctes. Il existe donc $p_1 \in P_\lambda$ laissant fixes tous les éléments qui ne sont pas dans la première colonne, et $q_1 \in Q_\lambda$ tels que $p_1(i) = q_1 g^{-1}(i)$ pour $1 \leq i \leq \lambda_1$. Si $\lambda_1 < n$, on remplace maintenant $g$ par $p_1 g q_1^{-1}$, qui coïncide avec l'identité pour $1 \leq i \leq \lambda_1$ et satisfait aux mêmes conditions que $g$. On obtient a alors $p_2 \in P_\lambda$ laissant fixes les éléments qui ne sont pas dans la deuxième colonne, et $q_2 \in Q_\lambda$ laissant fixes les éléments de la première colonne, et tels que $p_2(i) = q_2 g^{-1}(i)$ pour $1 \leq i \leq \lambda_1 + \lambda_2$. On continue de la même manière avec les colonnes suivantes : on obtient finalement des éléments $p \in P_\lambda$ et $q \in Q_\lambda$ tel que $p(i) = qg^{-1}(i)$ pour tout $1 \leq i \leq n$. Alors $g \in P_\lambda Q_\lambda$ ce qui contredit l'hypothèse. □

Dans le lemme ci-dessous, on a besoin d'ordonner l'ensemble des partitions de $n$ par ordre lexicographique : si $\lambda$ et $\mu$ sont deux partitions de $n$, $\lambda \succ \mu$ signifie que pour le premier indice $i$ tel que $\lambda_i \neq \mu_i$, on a $\lambda_i > \mu_i$.

LEMME 4.56. — *Soient $x$ un élément de $A = k[G]$, et $\lambda$ et $\mu$ deux partitions de $n$.*

(i) *Si $\lambda \succ \mu$, on a $a_\lambda x b_\mu = 0$. En particulier, $c_\lambda c_\mu = 0$.*

(ii) *Pour tout $x \in A$, $c_\lambda x c_\lambda$ est multiple scalaire de $c_\lambda$. En particulier, il existe $n_\lambda \in k$ tel que $c_\lambda^2 = n_\lambda c_\lambda$.*

*Démonstration.* (i) On peut supposer $x = g \in G$. Ici encore, il suffit de trouver une transposition $t \in P_\lambda$ telle que $t' = g^{-1}tg \in Q_\mu$. En effet, on a alors $g = tgt'$ et par suite

$$a_\lambda g b_\mu = a_\lambda t g t' b_\mu = -a_\lambda g b_\mu.$$

Ainsi $a_\lambda g b_\mu = 0$.

Si une telle transposition n'existait pas, pour toute paire $\{i, j\}$ d'éléments distincts d'une colonne de $T_\lambda$, les éléments $g^{-1}(i)$ et $g^{-1}(j)$ appartiendraient à des lignes différentes dans le tableau numéroté $T_\mu$ et par conséquent $\mu_1 \geq \lambda_1$ et donc $\lambda_1 = \mu_1$ ; en outre il existerait $p_1 \in P_\lambda$ et $q_1 \in Q_\mu$ telles que pour $1 \leq i \leq \lambda_1$ on ait $p_1(i) = q_1 g^{-1}(i)$. En continuant comme dans le lemme précédent avec les colonnes suivantes, on obtient des éléments $p \in P_\lambda$ et $q \in Q_\mu$ tels que $p(i) = qg^{-1}(i)$ pour tout $1 \leq i \leq n$ et les égalités $\lambda_j = \mu_j$ pour tout $j$; ainsi $\lambda = \mu$. Ceci contredit l'hypothèse.

On a alors

$$c_\lambda c_\mu = \sum_{g \in Q_\lambda, g' \in P_\mu} \epsilon(g) a_\lambda g g' b_\mu = 0.$$

(ii) On a pour tout $p \in P_\lambda$ et $q \in Q_\lambda$

$$p c_\lambda x c_\lambda q = \epsilon(q) c_\lambda x c_\lambda$$

Il résulte de l'assertion (iii) du lemme précédent que $c_\lambda x c_\lambda$ est un multiple scalaire de $c_\lambda$. □

*Démonstration du théorème 4.54*

Montrons d'abord que $c_\lambda \neq 0$. La multiplication par $c_\lambda$ fournit une application $k-$linéaire $f_\lambda : A \longrightarrow A$ définie par $x \mapsto xc_\lambda$ ; la matrice de cette application linéaire a ses éléments diagonaux égaux à 1. Par conséquent, elle est non nulle. Remarquons aussi que sa trace est $n!$. Il en résulte que $c_\lambda$ n'est pas nilpotent et donc $c_\lambda^2 \neq 0$. Alors si $c_\lambda^2 = n_\lambda c_\lambda$, le scalaire $n_\lambda$ n'est pas nul. On peut d'ailleurs le déterminer en fonction de $\dim V_\lambda$ de la manière suivante : l'application $k-$linéaire $p_\lambda : A \longrightarrow A$ définie par

$$p_\lambda = \frac{f_\lambda}{n_\lambda}$$

est une projection dont l'image est $V_\lambda$. Par suite

$$n! = n_\lambda \dim V_\lambda.$$

Montrons que la représentation $V_\lambda$ est irréductible. D'après le lemme précédent, on a $c_\lambda(V_\lambda) = kc_\lambda$ et par conséquent si $W \subset V_\lambda$ un sous-A-module de $V_\lambda$, $c_\lambda(W) \subset kc_\lambda$. Par conséquent $c_\lambda(W)$ est égal à $kc_\lambda$ ou nul . Dans la première hypothèse, $c_\lambda$ appartient à $c_\lambda(W) \subset W$ et par conséquent $Ac_\lambda = V_\lambda$ est contenu dans W. Dans le second cas, considérons une projection $\phi : A \longrightarrow W$, définie par un élément $w = \phi(1) \in W$ : il en existe puisque W est un sous-module facteur direct de A. On a alors $w \in V_\lambda$ : il existe un élément $a \in A$ tel que $w = ac_\lambda$. On a alors $w^2 = ac_\lambda w = 0$. Donc $\phi$ est nilpotent, donc de trace nulle, et puisque c'est une projection $\phi = 0$. Donc $W = 0$. La représentation $V_\lambda$ est donc irréductible.

Montrons maintenant que si $\lambda$ et $\mu$ sont deux partitions de $n$ distinctes, les représentations $V_\lambda$ et $V_\mu$ ne sont pas isomorphes. On peut supposer que $\lambda \succ \mu$. On a d'après le lemme 4.56 $c_\lambda(V_\lambda) \neq 0$, tandis que $c_\lambda(V_\mu) = 0$. Par conséquent, $V_\lambda$ n'est pas isomorphe à $V_\mu$. Ainsi, l'application

$$\mathsf{Part}(n) \longrightarrow \mathsf{Irr}(G)$$

qui associe à la partition $\lambda$ la classe d'isomorphisme $[V_\lambda]$ de la représentation irréductible $V_\lambda$ est un isomorphisme. □

Il existe des formules combinatoires, dues à Frobenius (voir [3], page 49), qui calculent le caractère de la représentation irréductible $V_\lambda$. En particulier, la dimension de $V_\lambda$ est facile à calculer. On l'obtient de la manière suivante : pour chaque case $u \in T$ dans le diagramme de Young de $\lambda$, on désigne par $r(u)$ le nombre de case situées stritement à droite de $u$ et $h(u)$ le nombre de de cases situées strictement au-dessus de $u$ et on pose $N(u) = r(u) + h(u) + 1$. Alors la dimension de $V_\lambda$ est donnée par

$$\dim V_\lambda = \frac{n!}{\prod_u N(u)}.$$

Par exemple, pour la représentation irréductible $V_\lambda$ associée à la partition de $\lambda = [4, 2, 2, 1, 1]$ de 10, le nombre $N(u)$ est donné par

| | | | | |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 5 | 2 | 1 | | |
| 8 | 5 | 4 | 2 | 1 |

Ainsi, la représentation irréductible associée a pour dimension

$$\dim V_\lambda = \frac{10!}{8.5^2.2^3.4} = 7.3^4 = 567.$$

### 4.11. Représentations induites

Soit $k$ un corps algébriquement clos de caractéristique 0. Soient G un groupe fini, Rep(G) l'ensemble des classes d'isomorphisme de représentations $k-$linéaires de G. Soit H un sous-groupe de G. On a une application naturelle

$$\mathsf{Rep}(\mathrm{G}) \longrightarrow \mathsf{Rep}(\mathrm{H})$$

qui associe à la représentation $\rho$ la restriction $\rho|_{\mathrm{H}}$ de $\rho$ à H. Cette représentation est souvent notée $\mathsf{Res}(\rho)$. Dans l'autre sens, considérons une représentation $\rho$ de H dans un $k-$espace vectoriel E. Le $k-$espace vectoriel $k[\mathrm{G}] \otimes \mathrm{E}$ est muni d'une action à gauche de H en posant pour $h \in \mathrm{H}$

$$h.(a \otimes v) = ah^{-1} \otimes hv.$$

Considérons l'espace vectoriel quotient

$$\mathrm{F} := k[\mathrm{G}] \otimes \mathrm{E}/\mathrm{S}$$

où S est le sous-espace vectoriel engendré par les vecteurs $ah^{-1} \otimes hv - a \otimes v$ pour $a \in k[\mathrm{G}]$ et $v \in \mathrm{E}$. Cet espace vectoriel est muni d'une structure de G$-$module à gauche obtenue en considérant l'action à gauche de G sur $k[\mathrm{G}] \otimes \mathrm{E}$ définie par $g.a \otimes v = ga \otimes v$ pour $g \in \mathrm{G}, a \in k[\mathrm{G}]$ et $v \in \mathrm{E}$, et en remarquant que l'action de G commute avec l'action de H définie ci-dessus. La représentation $\mathrm{G} \longrightarrow \mathrm{GL(F)}$ ainsi obtenue est appelée représentation induite par la représentation $\rho$ et notée $\mathsf{Ind}(\rho)$.

Exemple : Si on prend pour H le sous-groupe réduit à l'élément neutre, la représentation induite de la représentation triviale de dimension 1 est la représentation régulière.

PROPOSITION 4.57. — *Soient $\tau$ une représentation de* G, *et $\rho$ une représentation de* H. *On a un isomorphisme canonique*

$$\mathsf{Hom}_{\mathrm{H}}(\rho, \mathsf{Res}(\tau)) \simeq \mathsf{Hom}_{\mathrm{G}}(\mathsf{Ind}(\rho), \tau)$$

*Démonstration.* Soient $\rho : \mathrm{H} \longrightarrow \mathrm{E}$ et $\tau : \mathrm{G} \longrightarrow \mathrm{W}$ deux représentations $k-$linéaires de H et G respectivement. Alors l'espace vectoriel W peut-être vu comme une représentation de H, via la représentation $\mathsf{Res}(\tau)$. Soit $f : \mathrm{E} \longrightarrow \mathrm{W}$ une application H$-$linéaire. Considérons l'application linéaire $\phi : k[\mathrm{G}] \otimes \mathrm{E} \longrightarrow \mathrm{W}$ fournie par la propriété universelle du produit tensoriel à partir de l'application bilinéaire $k[\mathrm{G}] \times \mathrm{E} \longrightarrow \mathrm{W}$ définie pour $a \in k[\mathrm{G}]$ et $v \in \mathrm{E}$ par $(a, v) \mapsto af(v)$ : ainsi $\phi(a \otimes v) = af(v)$, et pour $h \in \mathrm{H}$, on a $\phi(ah^{-1} \otimes hv \mapsto ah^{-1}f(hv)) = ah^{-1}hf(v) = af(v)$, de sorte que $\phi(ah^{-1} \otimes hv - a \otimes v) = 0$. Ceci implique que $\phi$ se factorise suivant une application linéaire $\psi : \mathrm{F} \longrightarrow \mathrm{W}$ telle que $\psi([a \otimes v]) = af(v)$. Cette application est clairement G$-$linéaire. On a donc obtenu une application $k-$linéaire

$$\mathsf{Hom}_{\mathrm{H}}(\rho, \mathsf{Res}(\tau)) \longrightarrow \mathsf{Hom}_{\mathrm{G}}(\mathsf{Ind}(\rho), \tau)$$

Dans l'autre sens, étant donnée une application G$-$linéaire $\psi : \mathrm{F} \longrightarrow \mathrm{W}$, on obtient par composition une application linéaire $k[\mathrm{G}] \otimes \mathrm{E} \longrightarrow \mathrm{W}$ et par suite une application H$-$linéaire $f : \mathrm{E} \longrightarrow \mathrm{W}$ définie par $f(v) = \psi([e \otimes v])$, où $e$ est l'élément neutre et $v \in \mathrm{E}$. Pour $h \in \mathrm{H}$, on a alors $f(hv) = \psi([e \otimes hv]) = \psi([h \otimes v]) = h\psi(e \otimes v) = hf(v)$ ce qui montre que $f$ est H$-$linéaire. Il est clair que les applications $f \mapsto \psi$ et $\psi \mapsto f$ sont $k-$linéaires ; du fait que le $k[\mathrm{G}]$-module F est

engendré par les éléments de la forme $e \otimes v$, où $v \in \mathrm{E}$, on voit que ces applications linéaires sont inverses l'une de l'autre. □

COROLLAIRE 4.58. — *(Réciprocité de Frobenius) Considérons les formes bilinéaires symétriques sur $k^{\mathrm{H}}$ et $k^{\mathrm{G}}$ respectivement, définies au § 4.5. Alors*

$$\langle \chi_\rho, \chi_{\mathsf{Res}(\tau)} \rangle_{\mathrm{H}} = \langle \chi_{\mathsf{Ind}(\rho)}, \chi_\tau \rangle_{\mathrm{G}}$$

Cet énoncé signifie en particulier que si $\rho$ et $\tau$ sont des représentations irréductibles, la multiplicité de $\rho$ dans la décomposition de $\mathsf{Res}(\tau)$ en somme de représentations irréductibles est égal à la multiplicité de $\tau$ dans la décomposition de $\mathsf{Ind}(\rho)$ en somme de représentations irréductibles. Considèrons les caractères $\chi_1, \ldots, \chi_\ell$ des représentations irréductibles de G, et les caractères $\varphi_1, \ldots, \varphi_k$ des représentations irréductibles de H. Si on désigne par $\mathsf{Res}(\chi_i)$ la restriction de $\chi_i$ au sous-groupe H et $\mathsf{Ind}(\varphi_i)$ le caractère de la représentation induite par la représentation associée à $\varphi_i$ l'énoncé ci-dessus signifie que

$$\mathsf{Res}(\chi_i) = \sum_{j=1}^{k} m_{i,j} \varphi_j$$

et

$$\mathsf{Ind}(\varphi_i) = \sum_{j=1}^{\ell} m_{j,i} \chi_j$$

où la matrice $(m_{i,j})$ est une matrice à coefficients entiers. On passe donc d'une des formules à l'autre par transposition de cette matrice. L'intérêt de ces formules est qu'elles permettent de construire les représentations de G à partir de représentations de certains sous-groupes de G.

THÉORÈME 4.59. — *(Théorème d'Artin) Le sous-groupe du groupe des caractères de* G *engendré par les caractères des représentations induites par tous les sous-groupes cycliques de* G *est d'indice fini.*

En général, les caractères induits à partir des sous-groupes cycliques ne suffisent pas pour engendrer le groupe des caractères de G. On doit introduire des sous-groupes un peu plus compliqués.

DÉFINITION 4.60. — *Soit $p$ un nombre premier. Un groupe* H *est dit $p-$élémentaire s'il est isomorphe à un produit* $\mathrm{A} \times \mathrm{B}$, *où* B *est un $p-$groupe et* A *un groupe cyclique d'ordre non divisible par $p$.*

THÉORÈME 4.61. — *(Théorème de Brauer) Le groupe des caractères des représentations de* G *est engendré les caractères des représentations induites par tous les sous-groupes $p-$élémentaires* H *de* G.

Ces théorèmes sont démontrés dans le livre de Serre [6]. On se limite ici au calcul des caractères des représentations induites. Si H est un sous-groupe de G, on désigne par G/H l'ensemble des classes $g$H, où $g \in \mathrm{G}$, de sorte que G opère sur G/H par translation à gauche ; le nombre d'éléments $|\mathrm{G/H}|$ est donc l'indice de H dans G.

PROPOSITION 4.62. — *Soient* H *un sous-groupe de* G, *et $\rho$ une représentation de* H.
(i) *On a*

$$\dim \mathsf{Ind}(\rho) = |\mathrm{G/H}| \dim \rho.$$

(ii) *Pour $g \in \mathrm{G}$, on a*

$$\chi_{\mathsf{Ind}(\rho)}(g) = \frac{1}{|\mathrm{H}|} \sum_{s\in\mathrm{G}, sgs^{-1}\in\mathrm{H}} \chi_\rho(sgs^{-1})$$

*Démonstration.* L'assertion (ii) découle évidemment de l'assertion (i) en prenant pour $g$ l'élément neutre. Démontrons (ii). Choisissons pour chaque classe de G/H un représentant $g_i$. Soit une base $v_\alpha$ de E. On vérifie sans difficulté que les classes $[g_i \otimes v_\alpha]$ des éléments $g_i \otimes v_\alpha$ forment une base de F. On écrit pour tout $g \in \mathrm{G}$

$$gg_i = g_j h_{i,j}(g)$$

où $h_{i,j}(g)$ appartient à H, de sorte que

$$\begin{aligned}\mathsf{Ind}(\rho)([g_i \otimes v_\alpha] &= [gg_i \otimes v_\alpha] \\ &= [g_j \otimes h_{i,j}(g)v_\alpha]\end{aligned}$$

Il en résulte en prenant la trace

$$\begin{aligned}\chi_{\mathsf{Ind}(\rho)}(g) &= \sum_{i, g_i^{-1}gg_i\in\mathrm{H}} \chi_\rho(g_i^{-1}gg_i) \\ &= \frac{1}{|\mathrm{H}|} \sum_{s\in\mathrm{G}, s^{-1}gs\in\mathrm{H}} \chi_\rho(s^{-1}gs)\end{aligned}$$

En effet si $s \in \mathrm{G}$ appartient à la classe $g_i\mathrm{H}$, l'élément $s^{-1}gs$ est conjugué à $g_i^{-1}gg_i$ par un élément de H, et par conséquent si $s^{-1}gs$ appartient à H si et seulement si $g_i^{-1}gg_i$ appartient à H, et on a alors $\chi_\rho(s^{-1}gs) = \chi_\rho(g_i^{-1}gg_i)$. Il en résulte l'assertion (ii).

Exemple

Considérons le groupe symétrique $\mathfrak{S}_3$. Il a trois représentations irréductibles décrites au § 4.7. , dont on désigne par $\chi_1, \chi_2, \chi_3$ les caractères. Considérons le sous-groupe $\mathfrak{S}_2$ engendré par une transposition $\tau$ ; il a deux représentations irréductibles de dimension 1, de caractères $\varphi_1$ et $\varphi_2$, correspondant à la représentation triviale et la représentation $-1$. La matrice de l'application linéaire Res est alors dans les bases ci-dessus

| | $\chi_1$ | $\chi_2$ | $\chi_3$ |
|---|---|---|---|
| $\varphi_1$ | 1 | 0 | 1 |
| $\varphi_2$ | 0 | 1 | 1 |

de sorte que la matrice de l'application linéaire Ind est donnée par la matrice transposée :

| | $\varphi_1$ | $\varphi_2$ |
|---|---|---|
| $\chi_1$ | 1 | 0 |
| $\chi_2$ | 0 | 1 |
| $\chi_3$ | 1 | 1 |

On voit que les représentations induites par les représentations correspondant aux caractères $\varphi_i$ sont bien de dimension 3, comme prévu par la proposition 4.62. Le sous-groupe engendré par les images $\varphi_1$ et $\varphi_2$ n'engendre pas le groupe des caractères des représentations de $\mathfrak{S}_3$ ; même si on lui ajoute le caractère de la représentation régulière, dont les composantes sont $(1, 1, 2)$ dans la base $\chi_i$, ceci ne suffit pas pour obtenir le groupe engendré par les caractères de $\mathfrak{S}_3$.

Exercice 4.19

Vérifier que le groupe engendré par les caractères des représentations irréductibles de $\mathfrak{S}_3$ est le groupe engendré par les caractères des représentations irréductibles du sous-groupe $\mathfrak{S}_2$ engendré par une transposition, et $\mathfrak{S}_3$ engendré par une permutation circulaire.

(ii) *Pour $g \in G$, on a*

$$\chi_{\mathsf{Ind}(\rho)}(g) = \frac{1}{|H|} \sum_{s \in G, sgs^{-1} \in H} \chi_\rho(sgs^{-1})$$

*Démonstration.* L'assertion (ii) découle évidemment de l'assertion (i) en prenant pour $g$ l'élément neutre. Démontrons (ii). Choisissons pour chaque classe de G/H un représentant $g_i$. Soit une base $v_\alpha$ de E. On vérifie sans difficulté que les classes $[g_i \otimes v_\alpha]$ des éléments $g_i \otimes v_\alpha$ forment une base de F. On écrit pour tout $g \in G$

$$gg_i = g_j h_{i,j}(g)$$

où $h_{i,j}(g)$ appartient à H, de sorte que

$$\begin{aligned} \mathsf{Ind}(\rho)([g_i \otimes v_\alpha] &= [gg_i \otimes v_\alpha] \\ &= [g_j \otimes h_{i,j}(g) v_\alpha] \end{aligned}$$

Il en résulte en prenant la trace

$$\begin{aligned} \chi_{\mathsf{Ind}(\rho)}(g) &= \sum_{i, g_i^{-1} g g_i \in H} \chi_\rho(g_i^{-1} g g_i) \\ &= \frac{1}{|H|} \sum_{s \in G, s^{-1} g s \in H} \chi_\rho(s^{-1} g s) \end{aligned}$$

En effet si $s \in G$ appartient à la classe $g_i H$, l'élément $s^{-1}gs$ est conjugué à $g_i^{-1} g g_i$ par un élément de H, et par conséquent si $s^{-1}gs$ appartient à H si et seulement si $g_i^{-1} g g_i$ appartient à H, et on a alors $\chi_\rho(s^{-1}gs) = \chi_\rho(g_i^{-1} g g_i)$. Il en résulte l'assertion (ii).

Exemple

Considérons le groupe symétrique $\mathfrak{S}_3$. Il a trois représentations irréductibles décrites au § 4.7. , dont on désigne par $\chi_1, \chi_2, \chi_3$ les caractères. Considérons le sous-groupe $\mathfrak{S}_2$ engendré par une transposition $\tau$ ; il a deux représentations irréductibles de dimension 1, de caractères $\varphi_1$ et $\varphi_2$, correspondant à la représentation triviale et la représentation $-1$. La matrice de l'application linéaire Res est alors dans les bases ci-dessus

| | $\chi_1$ | $\chi_2$ | $\chi_3$ |
|---|---|---|---|
| $\varphi_1$ | 1 | 0 | 1 |
| $\varphi_2$ | 0 | 1 | 1 |

de sorte que la matrice de l'application linéaire Ind est donnée par la matrice transposée :

| | $\varphi_1$ | $\varphi_2$ |
|---|---|---|
| $\chi_1$ | 1 | 0 |
| $\chi_2$ | 0 | 1 |
| $\chi_3$ | 1 | 1 |

On voit que les représentations induites par les représentations correspondant aux caractères $\varphi_i$ sont bien de dimension 3, comme prévu par la proposition 4.62. Le sous-groupe engendré par les images $\varphi_1$ et $\varphi_2$ n'engendre pas le groupe des caractères des représentations de $\mathfrak{S}_3$ ; même si on lui ajoute le caractère de la représentation régulière, dont les composantes sont $(1, 1, 2)$ dans la base $\chi_i$, ceci ne suffit pas pour obtenir le groupe engendré par les caractères de $\mathfrak{S}_3$.

Exercice 4.19

Vérifier que le groupe engendré par les caractères des représentations irréductibles de $\mathfrak{S}_3$ est le groupe engendré par les caractères des représentations irréductibles du sous-groupe $\mathfrak{S}_2$ engendré par une transposition, et $\mathfrak{S}_3$ engendré par une permutation circulaire.

*Joseph Le Potier*

Examen partiel du 3 avril 1998
Durée : 3 heures

Soit A une $\mathbb{Q}$−algèbre de type fini. On désigne par Max(A) l'ensemble des idéaux maximaux de A. Pour tout idéal $\mathfrak{a}$ de A on désigne par $V(\mathfrak{a})$ l'ensemble des idéaux maximaux de A qui contiennent $\mathfrak{a}$. Pour toute partie $X \subset \mathrm{Max}(A)$ on pose

$$I(X) = \bigcap_{\mathfrak{m} \in X} \mathfrak{m}$$

1. Montrer que les parties $V(\mathfrak{a})$ sont les fermés d'une topologie sur Max(A). Dans la suite, l'ensemble Max(A) sera muni de cette topologie.

2. Déterminer pour tout idéal $\mathfrak{a}$ de A, l'idéal $I(V(\mathfrak{a}))$ et pour tout fermé X de Max(A), le fermé $V(I(X))$. En déduire que Max(A) est un espace topologique noethérien.

3. Montrer que Max(A) est irréductible si et seulement si le radical nilpotent de A est un idéal premier.

4. Etablir une bijection entre Spec(A) et l'ensemble des fermés irréductibles de Max(A). A quoi correspondent les composantes irréductibles de Max(A)?

5. Montrer que Max(A) est un ensemble fini si et seulement si l'anneau A est de longueur finie.

6. Démontrer que l'anneau A est de longueur finie si et seulement si le $\mathbb{Q}$−espace vectoriel A est de dimension finie.

7. On suppose que A est une $\mathbb{Q}$−algèbre locale, d'idéal maximal $\mathfrak{m}$. On désigne par $\ell(A)$ la longueur de A. Démontrer que $\dim_{\mathbb{Q}} A = \ell(A)[A/\mathfrak{m} : \mathbb{Q}]$.

8. On suppose que A est de longueur finie. Montrer que A est somme directe d'un nombre fini de $\mathbb{Q}$−algèbres locales de type fini.

9. On considère pour $k$ entier $\geq 1$ l'algèbre quotient

$$A = \mathbb{Q}[X, Y]/\mathfrak{a}$$

où $\mathfrak{a}$ est l'idéal $(X^2 + Y^2, (Y^2 - 2)^k)$. Montrer que A est une $\mathbb{Q}$−algèbre locale de type fini. En déduire que A est de longueur finie et calculer $\ell(A)$ et $\dim_{\mathbb{Q}} A$.

10. On considère l'anneau quotient

$$B = \mathbb{Z}[X, Y]/\mathfrak{b}$$

de $\mathbb{Z}[X, Y]$ par l'idéal $\mathfrak{b} = (X^2 + Y^2, (Y^2 - 2)^k)$. Démontrer que l'homomorphisme canonique $\mathbb{Z} \longrightarrow B$ est injectif, et que B est une extension entière de $\mathbb{Z}$. En déduire que B n'est pas de longueur finie. Préciser la dimension de Krull de B.

Corrigé de l'examen partiel

1. Considérons l'inclusion $\mathrm{Max}(A) \hookrightarrow \mathrm{Spec}(A)$. L'ensemble $V(\mathfrak{a})$ est l'intersection de Max(A) avec le fermé de Spec(A) défini par l'ensemble des $\mathfrak{p}$ tels que $\mathfrak{a} \subset \mathfrak{p}$. Ce sont donc les fermés pour la topologie induite.

2. — L'algèbre A est de type fini. D'après le théorème des zéros de Hilbert (cours, corollaire 1.18), pour tout idéal $\mathfrak{a}$ de A on a $I(V(\mathfrak{a})) = \mathrm{Rad}(\mathfrak{a})$.

— Soit X un fermé de Max(A) : il existe un idéal $\mathfrak{a}$ de A tel que $X = V(\mathfrak{a})$. On a aussi $X = V(\mathfrak{a}) = V(\mathrm{Rad}(\mathfrak{a}))$. Par suite

$$V(I(V(\mathfrak{a})) = V(\mathrm{Rad}(\mathfrak{a})) = V(\mathrm{Rad}(\mathfrak{a})).$$

— Soit $X_n$ une suite décroissante de fermés de Max(A). Puisque A est un quotient d'un anneau de polynômes sur un corps, c'est un anneau noethérien comme quotient d'un anneau noethérien. La suite croissante d'idéaux $I(X_n)$ est alors stationnaire. La suite $X_n = V(I(X_n))$ est donc elle aussi stationnaire. (Autre méthode : on sait d'après le cours que Spec(A) est un espace topologique noethérien ; tout sous-espace d'un espace topologique noethérien est encore noethérien.)

3. Soit $\mathfrak{n}$ le radical nilpotent de A. La projection canonique $\pi : A \mapsto A/\mathfrak{n}$ induit un homéomorphisme

$$\pi^* : \mathrm{Max}(A/\mathfrak{n}) \longrightarrow \mathrm{Max}(A)$$

défini par $\mathfrak{m} \mapsto \pi^{-1}(\mathfrak{m})$. En effet, c'est évidemment une bijection, et les fermés de A sont de la forme $V(\mathfrak{a})$, où $\mathfrak{a}$ est un idéal égal à son radical : un tel idéal contient $\mathfrak{n}$ et on a $\pi^*(V(\mathfrak{a}/\mathfrak{n})) = V(\mathfrak{a})$.

On peut donc supposer que A est réduite . Il s'agit donc de vérifier l'énoncé suivant : soit A une $\mathbb{Q}-$algèbre de type fini réduite ; alors Max(A) est irréductible si et seulement si A est intègre.

— Supposons A non intègre ; montrons que l'espace topologique Max(A) est réductible. Il existe $f$ et $g \in A$ non nuls tels que $fg = 0$. Alors $V(f) \cup V(g) = V(0) = \mathrm{Max}(A)$. De plus, $V(f) \neq \mathrm{Max}(A)$ car sinon $f$ appartiendrait au radical nilpotent de A. et donc serait nul. De même, $V(g) \neq \mathrm{Max}(A)$. Donc Max(A) est réductible.

— Dans l'autre sens, supposons Max(A) réductible ; montrons que A n'est pas intègre. Alors Max(A) est réunion de 2 fermés $F = V(\mathfrak{a})$ et $G = V(\mathfrak{b})$ distincts de Max(A). Alors $\mathrm{Max}(A) = V(\mathfrak{a} \cap \mathfrak{b})$ et donc puisque A est réduite $\mathfrak{a} \cap \mathfrak{b} = \{0\}$. Les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont non nuls, et donc il existe $f \in \mathfrak{a}$ non nul et $g \in \mathfrak{b}$ non nul. Alors $fg = 0$, et donc A n'est pas intègre.

4. Soit $\mathfrak{a}$ un idéal de A. La projection canonique $\pi : A \mapsto A/\mathfrak{a}$ induit un homéomorphisme

$$\pi^* : \mathrm{Max}(A/\mathfrak{a}) \longrightarrow V(\mathfrak{a})$$

défini par $\mathfrak{m} \mapsto \pi^{-1}(\mathfrak{m})$. En particulier, si $\mathfrak{a}$ est un idéal premier, d'après la question 3, l'espace topologique $\mathrm{Max}(A/\mathfrak{a})$ est irréductible, et donc $V(\mathfrak{a})$ est un fermé irréductible.

Dans l'autre sens, si $F = V(\mathfrak{a})$ est un fermé irréductible, le radical nilpotent de l'algèbre $A/\mathfrak{a}$ est un idéal premier. Autrement dit, le radical de $\mathfrak{a}$ est un idéal premier. Ainsi, I(F) est un idéal premier.

Soit Irr(Max(A)) l'ensemble des fermés irréductibles de Max(A). On a donc construit des applications

$$V : \mathrm{Spec}(A) \longrightarrow \mathrm{Irr}(\mathrm{Max}(A)) \text{ et } I : \mathrm{Irr}(\mathrm{Max}(A)) \longrightarrow \mathrm{Spec}(A).$$

D'après la question 2, pour tout idéal premier $\mathfrak{p}$ de A on a $I(V(\mathfrak{p})) = \mathrm{Rad}\,\mathfrak{p} = \mathfrak{p}$ et pour tout fermé X de Max(A) on a $V(I(X)) = X$. Ces deux applications sont donc inverses l'une de l'autre. Dans cette bijection, la relation d'ordre est transformée en la relation d'ordre opposée. Les composantes irréductibles $X_i$ de Max(A) sont les fermés irréductibles maximaux : les idéaux $I(X_i)$ sont donc les idéaux premiers minimaux de A.

5. Les parties de Max(A) réduites à un point sont des fermés irréductibles de Max(A) et correspondent par la bijection I ci-dessus aux idéaux maximaux de A. Si Max(A) est fini, les composantes irréductibles sont réduites à des points. Alors si $\mathfrak{p}$ est un idéal premier minimal de A, $V(\mathfrak{p})$ est une composante irréductible de Max(A) donc réduite à un point. Ainsi $I(V(\mathfrak{p})) = \mathfrak{p}$ est un idéal maximal. Puisque tout idéal premier contient un idéal premier minimal, un tel idéal premier est maximal. Puisque A est un anneau noethérien, A est de longueur finie d'après le cours (proposition 2.43).

Réciproquement, puisque A est un anneau noethérien, on sait que si A est de longueur finie, Spec(A) est fini d'après le cours (corollaire 2.45). En particulier, $\mathrm{Max}(A) \subset \mathrm{Spec}(A)$ est fini.

6. Supposons que A soit de longueur finie. Considérons une filtration de Jordan-Hölder de A

$$0 \subsetneq \mathfrak{a}_\ell \subsetneq \mathfrak{a}_{\ell-1} \subsetneq \ldots \subsetneq \mathfrak{a}_1 \subsetneq A$$

Le A-module quotient $\mathfrak{a}_i/\mathfrak{a}_{i+1}$ est simple, donc isomorphe à un module quotient $A/\mathfrak{m}_i$, où $\mathfrak{m}_i$ est un idéal maximal de A. Puisque A est une $\mathbb{Q}-$algèbre de type fini, l'extension $\mathbb{Q} \hookrightarrow A/\mathfrak{m}_i$ est une extension algébrique finie d'après le théorème des zéros de Hilbert (cours, théorème 1.15), et par suite

$$\dim_{\mathbb{Q}} A/\mathfrak{m}_i < \infty.$$

Par suite $\dim_{\mathbb{Q}} A = \sum_{i=0}^{\ell} \dim_{\mathbb{Q}} A/\mathfrak{m}_i < \infty$.

Réciproquement, supposons que $\dim_{\mathbb{Q}} A < \infty$. Soit $\mathfrak{p}$ un idéal premier associé à A. Alors le A-module $A/\mathfrak{p}$ est isomorphe à un idéal de A et donc $\dim_{\mathbb{Q}} A/\mathfrak{p} < \infty$. Alors l'extension

$$\mathbb{Q} \hookrightarrow A/\mathfrak{p}$$

est entière. Puisque $A/\mathfrak{p}$ est intègre, ceci implique que $A/\mathfrak{p}$ est un corps (cours, lemme 1.17) . Donc $\mathfrak{p}$ est un idéal maximal. Ainsi, tout idéal premier associé est maximal. Donc A est de longueur finie (cours, proposition 2.43).

7. Si A est une $\mathbb{Q}-$algèbre de type fini locale, d'idéal maximal $\mathfrak{m}$, d'après la question 5 l'anneau A est de longueur finie. Considérons une filtration de Jordan-Hölder de A

$$0 \subsetneqq \mathfrak{a}_\ell \subsetneqq \mathfrak{a}_{\ell-1} \subsetneqq \ldots \subsetneqq \mathfrak{a}_1 \subsetneqq A$$

Par définition $\ell$ est la longueur de A. Le A-module quotient $\mathfrak{a}_i/\mathfrak{a}_{i+1}$ est simple, donc isomorphe au module quotient $A/\mathfrak{m}$. Par définition $\dim_{\mathbb{Q}} A/\mathfrak{m} = [A/\mathfrak{m} : \mathbb{Q}]$. Ainsi

$$\dim_{\mathbb{Q}} A = \ell[A/\mathfrak{m} : \mathbb{Q}].$$

8. Supposons que A soit de longueur finie. Alors Max(A) est aussi l'ensemble des idéaux premiers minimaux et tout idéal maximal de A est minimal, et donc l'ensemble des idéaux premiers associés est aussi exactement Max(A). Soit

$$\{0\} = \bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} \mathfrak{a}(\mathfrak{m})$$

l'unique décomposition primaire minimale de $\{0\}$ dans A; l'idéal $\mathfrak{a}(\mathfrak{m})$ est la composante primaire de radical $\mathfrak{m}$. D'après le cours (théorème 2.34) cet idéal est le noyau de l'homomorphisme canonique $A \longrightarrow A_{\mathfrak{m}}$. D'après le cours (proposition 2.47), l'application canonique

$$A \mapsto \oplus_{\mathfrak{m} \in \mathrm{Max}(A)} A/\mathfrak{a}(\mathfrak{m})$$

est un isomorphisme de $\mathbb{Q}-$algèbres. De plus, l'homomorphisme canonique

$$A/\mathfrak{a}(\mathfrak{m}) \longrightarrow A_{\mathfrak{m}}$$

est surjectif et donc un isomorphisme. Il en résulte que $A/\mathfrak{a}(\mathfrak{m})$ est une $\mathbb{Q}-$algèbre de type fini locale.

9. L'algèbre quotient $A = \mathbb{Q}[X, Y]/\mathfrak{a}$ est évidemment de type fini. Montrons qu'elle n'a qu'un idéal maximal. Il revient au même de vérifier que $\mathbb{Q}[X, Y]$ n'a qu'un idéal maximal $\mathfrak{m}$ contenant $\mathfrak{a} = (X^2 + Y^2, (Y^2 - 2)^k)$. Soit $\mathfrak{m}$ un tel idéal maximal ; puisque $\mathfrak{m}$ est un idéal premier, $Y^2 - 2 \in \mathfrak{m}$ et par suite $(X^2 + 2, Y^2 - 2) \subset \mathfrak{m}$.

Or l'idéal $\mathfrak{q} = (X^2+2, Y^2-2)$ est déjà un idéal maximal : en effet, l'homomorphisme d'algèbres $\mathbb{Q}[X, Y] \longrightarrow \mathbb{Q}[\sqrt{2}][X]/(X^2 + 2)$ défini par $P(X, Y) \mapsto P(X, \sqrt{2})$ est surjective de noyau $\mathfrak{q}$ ; elle passe au quotient et fournit un isomorphisme d'algèbres

$$A/\mathfrak{q} \simeq \mathbb{Q}[\sqrt{2}][X]/(X^2 + 2).$$

Puisque $X^2+2$ est un polynôme irréductible sur le corps $\mathbb{Q}[\sqrt{2}]$ l'idéal $(X^2+2)$ est un idéal maximal de $\mathbb{Q}[\sqrt{2}][X]$ et le quotient $K = \mathbb{Q}[\sqrt{2}][X]/(X^2+2)$ est donc un corps (isomorphe à $\mathbb{Q}[\sqrt{2}, i]$). Par suite $\mathfrak{q}$ est un idéal maximal, et donc $\mathfrak{m} = \mathfrak{q}$. Ainsi $\mathfrak{q}$ est le seul idéal maximal de $\mathbb{Q}[X, Y]$ contenant $\mathfrak{a}$.

Le degré de l'extension algébrique finie $\mathbb{Q} \hookrightarrow K$ est alors

$$[K : \mathbb{Q}[\sqrt{2}]][\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 4.$$

Il résulte de la question 5 que l'anneau A est de longueur finie. Pour trouver sa longueur, il suffit de trouver une filtration de Jordan-Hölder de A.

Considérons l'idéal $\mathfrak{a}_i = (X^2+Y^2, (Y^2-2)^i)$ de $\mathbb{Q}[X, Y]$. Alors la suite, strictement décroissante pour $0 \leq i \leq k-1$, $\mathfrak{a}_i/\mathfrak{a}$ est une filtration de Jordan-Hölder de A. En effet, l'application A−linéaire $A \longrightarrow \mathfrak{a}_i/\mathfrak{a}_{i+1}$ qui associe au polynôme P la classe de $P(Y^2-2)^i$ est surjective et son noyau contient l'idéal maximal $\mathfrak{q}$. Puisque ce noyau est un idéal propre, c'est exactement $\mathfrak{q}$. Ainsi le module quotient $\mathfrak{a}_i \longrightarrow \mathfrak{a}_{i+1}$ est un module simple isomorphe à $K = A/\mathfrak{q}$. L'anneau A est donc de longueur $k$. D'après la question 7, on a

$$\dim_{\mathbb{Q}} A = 4k.$$

10. Considérons l'homomorphisme canonique $\mathbb{Z} \longrightarrow B = \mathbb{Z}[X, Y]/\mathfrak{b}$ et supposons que le noyau de ce morphisme contienne un entier $m$ non nul. Il existerait alors des polynômes P et Q à coefficients entiers tels que dans $\mathbb{Z}[X, Y]$

$$m = P(X^2+Y^2) + Q(Y^2-2)^k$$

Si on lit cette relation dans $\mathbb{Q}[X, Y]$ on voit que l'idéal $\mathfrak{a}$ de $\mathbb{Q}[X, Y]$ considéré dans la question 9 ne serait pas propre, ce qui est absurde puisqu'il est contenu dans l'idéal maximal $\mathfrak{q}$.

Montrons que l'extension $\mathbb{Z} \hookrightarrow B$ est entière. La classe $y$ de Y est évidemment entière sur $\mathbb{Z}$ puisqu'elle satisfait à la relation $(y^2-2)^k = 0$. La classe $x$ de X est entière sur l'anneau $\mathbb{Z}[y]$ puisqu'elle satisfait à la relation $x^2+y^2 = 0$. Par suite $x$ est entier sur $\mathbb{Z}$.

Il résulte du cours (proposition 3.3) que B est de même dimension de Krull que $\mathbb{Z}$. Ainsi, $\dim B = 1$ et B n'est pas de longueur finie (cours, proposition 2.43).

*Joseph Le Potier*

Examen du 18 juin 1998
Durée : 3 heures

La section II peut se traiter indépendamment des autres sections. Toutes les représentations considérées dans le problème sont des représentations linéaires complexes.

Soit G un groupe fini d'ordre $n$. On désigne par $\mathcal{C}(G)$ l'algèbre des fonctions centrales $G \longrightarrow \mathbb{C}$. Pour $u$ et $v \in \mathcal{C}(G)$ on pose

$$\langle u, v\rangle = \frac{1}{n}\sum_{g\in G} u(g)\overline{v}(g).$$

Soit R(G) le sous-groupe additif de $\mathcal{C}(G)$ engendré par les caractères des représentations de G.

## I

1) Démontrer que R(G) est un groupe abélien libre de type fini.

2) Soit $e$ l'élément neutre de G. Démontrer qu'un élément $\chi \in R(G)$ est le caractère d'une représentation irréductible si et seulement si $\chi(e) > 0$ et $\langle \chi, \chi\rangle = 1$.

3) Démontrer que R(G) est un sous-anneau de $\mathcal{C}(G)$.

## II

On considère le plan vectoriel $\mathbb{R}^2$ muni de la métrique euclidienne canonique et de l'orientation donnée par la base canonique. Soient $GL(2,\mathbb{R})$ le groupe des applications linéaires inversibles $\mathbb{R}^2 \to \mathbb{R}^2$ et G le sous-groupe de $GL(2,\mathbb{R})$ engendré par la rotation $r$ d'angle $\frac{\pi}{3}$ et par la symétrie $s : (x, y) \mapsto (x, -y)$.

1) Calculer $srs$. Montrer que le sous-groupe H engendré par $r$ est distingué dans G et décrire le groupe quotient G/H. Combien d'éléments a le groupe G ?

2) Décrire les classes de conjugaison de G. En déduire le nombre de classes d'isomorphisme de représentations irréductibles de G.

3) Montrer que le sous-groupe K de G engendré par $r^2$ est distingué et que le groupe quotient G/K est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. En déduire que G a exactement quatre représentations irréductibles de dimension 1.

4) Soit $GL(2,\mathbb{C})$ le groupe des applications linéaires inversibles $\mathbb{C}^2 \to \mathbb{C}^2$. On considère le plongement

$$\rho : G \hookrightarrow GL(2,\mathbb{R}) \hookrightarrow GL(2,\mathbb{C})$$

Calculer le caractère $\chi$ de la représentation $\rho$. En déduire que $\rho$ est une représentation irréductible.

5) Dresser la table des caractères des représentations irréductibles de G.

6) Soit $i$ un entier $> 0$. A quelle condition la fonction $g \mapsto \chi(g^i)$ est-elle le caractère d'une représentation irréductible de G?

## III

Soit E un espace vectoriel complexe de dimension $r$ et $f : E \longrightarrow E$ un endomorphisme de E. On rappelle que si $m$ un entier positif, $\wedge^m f$ est l'endomorphisme de la puissance extérieure $\wedge^m E$ caractérisé par la formule

$$\wedge^m f(x_1 \wedge \ldots \wedge x_m) = f(x_1) \wedge \ldots \wedge f(x_m)$$

pour $x_1, \ldots, x_m \in E$. Par convention, $\wedge^0 E = \mathbb{C}$ et $\wedge^0 f$ est l'identité de $\mathbb{C}$.

On suppose que $f$ est diagonalisable.

1) Soit $e_1, \ldots, e_r$ une base de vecteurs propres pour $f$, et $\lambda_i$ la valeur propre correspondant à $e_i$. Calculer, en termes des valeurs propres, trace $(\wedge^{\mathrm{m}}\mathrm{f})$. Vérifier, pour tout réel $t$, la formule

$$\det(1+tf) = \sum_{m\geq 0} t^m \mathrm{trace}\,(\wedge^{\mathrm{m}}\mathrm{f}).$$

2) On considère pour $t \in \mathbb{R}$ la fonction $\varphi(t) = \det(1+tf)$. Vérifier que si $|t|$ suffisamment petit, $1+tf$ est inversible, et que l'on a

$$\varphi'(t) = \varphi(t)\mathrm{trace}\,((1+\mathrm{tf})^{-1}\mathrm{f}).$$

En déduire que

$$m\mathrm{trace}\,(\wedge^{\mathrm{m}}\mathrm{f}) = \sum_{1\leq \mathrm{i}\leq \mathrm{m}} (-1)^{\mathrm{i}-1}\mathrm{trace}\,(\wedge^{\mathrm{m}-\mathrm{i}}\mathrm{f})\mathrm{trace}\,(\mathrm{f}^{\mathrm{i}}).$$

## IV

Pour tout entier $i$, on désigne par $\phi_i : \mathrm{G} \longrightarrow \mathrm{G}$ l'application définie par $g \mapsto g^i$. On considère une représentation $\rho : \mathrm{G} \longrightarrow \mathrm{GL(E)}$ de dimension $r$ dont on désigne par $\chi$ le caractère.

1) Soit $\wedge^m\rho$ la représentation définie par $g \mapsto \wedge^m\rho(g)$, et $\chi(\wedge^m\rho)$ son caractère. Démontrer la relation

$$m\chi(\wedge^m\rho) = \sum_{1\leq i\leq m} (-1)^{i-1}\chi(\wedge^{m-i}\rho)\ \chi\circ\phi_i$$

Déduire de I que pour tout entier $m > 0$ la fonction $\chi\circ\phi_m$ appartient à R(G).

2) Soit $m$ un entier premier avec l'ordre $n$ de G. Démontrer que $\phi_m : \mathrm{G} \longrightarrow \mathrm{G}$ est une application bijective. (On pourra remarquer que tout élément $g \in \mathrm{G}$ appartient au sous-groupe engendré par $g^m$, et en déduire que $\phi_m$ est injective.)

3) On suppose que $\rho : \mathrm{G} \longrightarrow \mathrm{GL(E)}$ est une représentation irréductible. Démontrer que si $m$ est entier premier avec $n$, la fonction $\chi\circ\phi_m$ est le caractère d'une représentation irréductible (Utiliser I).

*Joseph Le Potier*

Examen du 2 septembre 1998
Durée : 3 heures

Les deux exercices sont indépendants.

## I

Toutes les représentations considérées dans cet exercice sont des représentations linéaires complexes. Soient $B = \{e_i, 1 \leq i \leq 5\}$ un ensemble à 5 éléments et $G = \mathfrak{S}(B)$ le groupe des permutations de B.

1) Déterminer les classes de conjugaison de G et le nombre d'éléments dans chaque classe de conjugaison.

2) On désigne par $\epsilon$ la représentation triviale de dimension 1. Montrer que les représentations irréductibles de dimension un de G constituent un groupe à 2 éléments $\{\epsilon, \sigma\}$.

3) Soit V l'espace vectoriel complexe engendré par B ; on rappelle que l'inclusion canonique $B \hookrightarrow V$ identifie $B = \{e_i, 1 \leq i \leq 5\}$ à une base de V. On considère la représentation linéaire $w : G \longrightarrow GL(V)$ qui prolonge l'action de G sur B : elle est définie pour $g \in G$ par

$$w(g)(e_i) = g(e_i)$$

Montrer que $w$ est somme directe d'une représentation de dimension 1 et d'une représentation $\rho$ de dimension 4. Calculer le caractère de $\rho$ ; en déduire que $\rho$ est une représentation irréductible.

4) Montrer que la représentation $\rho \otimes \sigma$ est une représentation irréductible de dimension 4 non isomorphe à $\rho$.

5) Déterminer le caractère de la puissance extérieure $\tau = \wedge^2 \rho$. En déduire que cette représentation $\tau$ est une représentation irréductible de dimension 6.

6) Montrer que G a deux représentations irréductibles de dimension 5 non isomorphes.

7) Déterminer le caractère de la puissance symétrique $S^2\rho$. En déduire que $S^2\rho$ est somme directe des représentations $\epsilon, \rho$ et d'une représentation $\lambda$ de dimension 5. Vérifier que $\lambda$ est une représentation irréductible.

8) Vérifier que les représentations $\lambda$ et $\lambda \otimes \sigma$ ne sont pas isomorphes. Dresser la table des caractères de G.

## II

Soient A un anneau noethérien, et M un A−module de type fini, non nul. On désigne par $\mathsf{Ass}(M)$ l'ensemble des idéaux premiers associés à M. Le but de l'exercice est d'étudier l'ensemble $\mathsf{Ass}(\mathsf{End}(M))$ des idéaux premiers associés du module $\mathsf{End}(M)$ des endomorphismes A−linéaires de M.

1) Montrer qu'il existe un entier $n > 0$ tel que $\mathsf{End}(M)$ se plonge dans $M^n$. En déduire que $\mathsf{End}(M)$ est un A−module de type fini et que

$$\mathsf{Ass}(\mathsf{End}(M)) \subset \mathsf{Ass}(M).$$

2) Soit $\mathfrak{p}$ un idéal premier appartenant au support de M. On se propose de montrer qu'il existe un homomorphisme non nul $M \longrightarrow A/\mathfrak{p}$.

a) On suppose d'abord que A est un anneau local et que $\mathfrak{p}$ est l'idéal maximal $\mathfrak{m}$ de cet anneau local. Soit $k = A/\mathfrak{m}$ le corps résiduel. Montrer que le $k$−espace vectoriel $M/\mathfrak{m}M$ est non nul. En déduire qu'il existe une application A−linéaire surjective $f : M \longrightarrow A/\mathfrak{m}$.

b) On se place maintenant dans le cas général ; soit $M_\mathfrak{p}$ le localisé de M en $\mathfrak{p}$. Démontrer que $M_\mathfrak{p}$ est un $A_\mathfrak{p}$−module de type fini. Déduire de a) qu'il existe une application A−linéaire non nulle

$$f : M \longrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$$

On rappelle que le corps résiduel de l'anneau local $A_{\mathfrak{p}}$ est aussi le corps des fractions de l'anneau $A/\mathfrak{p}$. Démontrer qu'il existe un élément $s \in A$, tel que $s \notin \mathfrak{p}$ et tel que l'image de $sf$ soit contenue dans $A/\mathfrak{p}$. Vérifier que l'application linéaire $g = sf : M \longrightarrow A/\mathfrak{p}$ est non nulle.

3) Soit $\mathfrak{p} \in \mathsf{Ass}(M)$. Montrer qu'il existe un endomorphisme non nul $\varphi : M \longrightarrow M$ dont l'image est isomorphe à un sous-module de $A/\mathfrak{p}$. Montrer qu'alors $\operatorname{Ann}\varphi = \mathfrak{p}$ et par suite $\mathfrak{p} \in \mathsf{Ass}(\mathsf{End}(M))$.

En conclure que

$$\mathsf{Ass}(M) = \mathsf{Ass}(\mathsf{End}(M)).$$

## Bibliographie

[1] M.F. ATIYAH ET I.G. MACDONALD, *Introduction to commutative algebra,* Addison-Wesley Publishing Company (1969).

[2] N. BOURBAKI, *Algèbre commutative.*

[3] W. FULTON ET J. HARRIS, *Representation theory,* Graduate texts in Mathematics, Springer (1991)

[4] S. LANG, *Algebra,* Addison-Wesley Publishing Company, Inc. (1984)

[5] J. LE POTIER, *Théorie des groupes et applications,* Cours polycopié de licence, Université Paris 7 (1977).

[6] J. P. SERRE, *Linear representations of finite groups,* Springer-Verlag (1977).