Cours de DEA

Invariants polynômiaux des groupes finis - Groupes de réflexions

(Besançon 2004)

21 h de cours, 7h de TD

Partie 0. Préliminaires

Idéaux maximaux, idéaux premiers.

Soit A un anneau (commutatif, unitaire).

Lemme chinois. *Soient $\mathfrak{a}_1,\dots,\mathfrak{a}_r$ des idéaux de A tels que $\mathfrak{a}_i+\mathfrak{a}_j=A$ pour tous $1\leqslant i<j\leqslant r$. Alors l'application canonique*

$$A\longrightarrow\prod_{i=1}^{r}A/\mathfrak{a}_i$$

est surjective.

Lemme de Nakayama. *Supposons A local et notons $\mathfrak{m}$ son idéal maximal. Soit M un A-module de type fini. Alors $\mathfrak{m}M=M$ si et seulement si $M=0$.*

Preuve - Si $M=0$, alors $\mathfrak{m}M=0=M$. Réciproquement, supposons que $\mathfrak{m}M=M$. Soient $u_1,\dots,u_r$ des générateurs du A-module M. Puisque $\mathfrak{m}M=M$, il existe une matrice $X=(m_{ij})_{1\leqslant i,j\leqslant r}$ à coefficients dans $\mathfrak{m}$ telle que

$$u_i=\sum_{j=1}^{r}m_{ij}u_j$$

pour tout $1\leqslant j\leqslant r$. En multipliant par la transposée de la comatrice de Id_r-X, on obtient que

$$\det(\mathrm{Id}_r-X).u_j=0$$

pour tout $1\leqslant j\leqslant r$. Or, $\det(\mathrm{Id}_r-X)$ est inversible dans A car A est local. Donc $M=0$. ■

Corollaire A. *Supposons A local. Soient M et N deux sous-A-modules de A^n tels que $M\oplus N=A^n$. Alors M et N sont libres.*

Preuve - Notons $\mathfrak{m}$ l'idéal maximal de A et soit $k=A/\mathfrak{m}$. Soit $\pi:A^n\to k^n$ la projection canonique. Tout d'abord, M et N sont de type fini comme facteurs directs d'un module de type fini. De plus $M/\mathfrak{m}M\oplus N/\mathfrak{m}N=k^n$. Soient $(u_1,\dots,u_r)$ et $(v_1,\dots,v_s)$ des éléments de M et N respectivement tels que $(\pi(u_1),\dots,\pi(u_r))$ et $(\pi(v_1),\dots,\pi(v_s))$ soient des bases de $M/\mathfrak{m}M$ et $N/\mathfrak{m}N$ respectivement. Alors $r+s=n$ et, d'après le lemme de Nakayama, $(u_1,\dots,u_r)$ engendre M et $(v_1,\dots,v_s)$ engendre N. Pour conclure, il suffit de montrer que $(u_1,\dots,u_r,v_1,\dots,v_s)$ est libre sur A, ce qui est trivial. ■

Un idéal $\mathfrak{p}$ de A est dit *premier* si $A/\mathfrak{p}\neq 0$ est intègre. On note $\operatorname{Spec}A$ l'ensemble des idéaux premiers de A.

On fixe un morphisme d'anneaux $\pi:A\to B$, de sorte que B sera vu comme une A-algèbre via π.

Proposition B. *Si $\mathfrak{q}$ est un idéal premier de B, alors $\pi^{-1}(\mathfrak{q})$ est un idéal premier de A.*

Preuve - En effet, π induit un morphisme injectif $A/\pi^{-1}(\mathfrak{q})\hookrightarrow B/\mathfrak{q}$. Le résultat découle alors du fait qu'un sous-anneau d'un anneau intègre est intègre. ■

On notera $\pi^* : \operatorname{Spec} B \to \operatorname{Spec} A$, $\mathfrak{q} \mapsto \pi^{-1}(\mathfrak{q})$. C'est une application croissante. Commençons par deux résultats élémentaires.

REMARQUE - Si $A \subset B$ et $\pi : A \hookrightarrow B$ est l'injection canonique, alors $\pi^{-1}(\mathfrak{q}) = \mathfrak{q} \cap A$. □

Lemme C. *Soit I un idéal de A et soit S une partie multiplicative de A.*

(a) *Notons $\pi : A \to A/I$ l'application canonique. Alors $\pi^* : \operatorname{Spec} A/I \to \operatorname{Spec} A$ induit une bijection croissante entre $\operatorname{Spec} A/I$ et l'ensemble des idéaux premiers de A contenant I.*

(b) *Notons $\pi : A \to S^{-1}A$ l'application canonique. Si $\mathfrak{p}$ est un idéal premier de A ne rencontrant pas S, alors $S^{-1}\mathfrak{p} = \mathfrak{p}(S^{-1}A)$ est un idéal premier de $S^{-1}A$ et $\pi^*(S^{-1}\mathfrak{p}) = \mathfrak{p}$. Par suite, l'application $\pi^* : \operatorname{Spec} S^{-1}A \to \operatorname{Spec} A$ induit une bijection croissante entre l'ensemble des idéaux premiers de $S^{-1}A$ et l'ensemble des idéaux premiers de A ne rencontrant pas S.*

Si $\mathfrak{p} \in \operatorname{Spec} A$, alors $A - \mathfrak{p}$ est une partie multiplicative de A et on notera $A_\mathfrak{p}$ le localisé de A par rapport à cette partie. Alors $A_\mathfrak{p}$ est un anneau local (contenant A car $A - \mathfrak{p}$ ne contient pas de diviseurs de zéro) : son unique idéal maximal est $\mathfrak{p}A_\mathfrak{p}$. De plus, $\mathfrak{p}A_\mathfrak{p} \cap A = \mathfrak{p}$ et $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ est le corps des fractions de $A/\mathfrak{p}$. Si M est un A-module, alors on pose $M_\mathfrak{p} = A_\mathfrak{p} \otimes_A M$. C'est un $A_\mathfrak{p}$-module. Par exemple, $B_\mathfrak{p}$ est un $A_\mathfrak{p}$-algèbre. Nous noterons $\pi_\mathfrak{p} : A_\mathfrak{p} \to B_\mathfrak{p}$ le morphisme induit par π.

Proposition D. *Soit $\mathfrak{p}$ un idéal premier de A. Alors l'application*

$$\begin{array}{ccc} \pi^{*-1}(\mathfrak{p}) & \longrightarrow & \pi_\mathfrak{p}^{*-1}(\mathfrak{p}A_\mathfrak{p}) \\ \mathfrak{q} & \longmapsto & A_\mathfrak{p} \otimes_A \mathfrak{q} \end{array}$$

est bijective. La bijection réciproque est donnée par $\mathfrak{q} \mapsto i^{-1}(\mathfrak{q})$ où $i : B \to B_\mathfrak{p}$, est l'injection canonique.

On dit que B est *fini(e)* sur A (ou que π est un morphisme *fini*) si B, vu comme A-module, est de type fini. On dit que B est *de type fini* sur A (ou que π est un morphisme *de type fini*) si B, vu comme A-algèbre, est de type fini. On dit que B est *entier* sur A si tout élément de B est entier sur A. On appelle *clôture intégrale* de A dans B l'ensemble des éléments de B qui sont entiers sur A. C'est un sous-anneau de B.

Proposition E. *π est fini si et seulement si π est de type fini et entier.*

Lemme F. *Supposons π injectif et entier et B intègre. Alors A est un corps si et seulement si B est un corps.*

PREUVE - Pous simplifier nous supposerons que $A \subset B$ et que π est l'injection canonique. Notons que A est intègre comme sous-anneau d'un anneau intègre.

(1) $\Rightarrow$ (2) : Supposons que A est un corps. Soit $b \in B$, $b \neq 0$. Il existe un polynôme unitaire, irréductible (car B est intègre) $P \in A[X]$ tel que $P(b) = 0$. Écrivons $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ avec $a_i \in A$. Alors $a_0 \neq 0$. Puisque A est un corps, a_0 est inversible. De plus,

$$b.\Big(-a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)\Big) = 1,$$

ce qui montre que b est inversible dans B. Donc B est un corps.

(2) $\Rightarrow$ (1) : Supposons que B est un corps. Soit $a \in A$, $a \neq 0$. Alors a est inversible dans B. Il existe un polynôme unitaire, irréductible $P \in A[X]$ tel que $P(a^{-1}) = 0$. Écrivons $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ avec $a_i \in A$. On a alors

$$a^{-1} = -(a_{n-1} + a_{n-2}a + \cdots + a_1a^{n-2} + a_0a^{n-1}).$$

Donc $a^{-1} \in A$. Donc A est un corps. ■

Corollaire G. *Supposons π entier. Soit $\mathfrak{q}$ un idéal maximal de B. Alors $\mathfrak{q}$ est maximal si et seulement si $\pi^{-1}(\mathfrak{q})$ est maximal.*

Si A est intègre, on notera $\mathrm{Frac}(A)$ son corps des fractions. Dans ce cas, on dit que A est intégralement clos s'il est égal à sa clôture intégrale dans $\mathrm{Frac}(A)$.

Théorème H. *Supposons π entier et injectif. Alors $\pi^* : \mathrm{Spec}\, B \to \mathrm{Spec}\, A$ est surjective et strictement croissante. Si π est fini, alors les fibres de π sont finies.*

Preuve - Nous supposerons pour simplifier que $A \subset B$ et que π est l'injection canonique.

Montrons tout d'abord que π^* est surjective. Soit $\mathfrak{p}$ un idéal premier de A. D'après la proposition D, on peut supposer que A est local d'idéal maximal $\mathfrak{p}$. Soit $\mathfrak{q}$ un idéal maximal de B. Alors $\mathfrak{q} \cap A$ est un idéal maximal de A d'après le corollaire G. Donc $\mathfrak{q} \cap A = \mathfrak{p}$.

Revenons au cas général et montrons que π^* est strictement croissante. Soient $\mathfrak{q}$ et $\mathfrak{q}'$ deux idéaux premiers de B tels que $\mathfrak{q} \cap A = \mathfrak{q}' \cap A = \mathfrak{p}$ et $\mathfrak{q} \subset \mathfrak{q}'$. Alors $S^{-1}\mathfrak{q} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$ et $S^{-1}\mathfrak{q}' \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$. D'après le corollaire G, $S^{-1}\mathfrak{q}$ et $S^{-1}\mathfrak{q}'$ sont des idéaux maximaux de $S^{-1}B$. Donc $S^{-1}\mathfrak{q} = S^{-1}\mathfrak{q}'$. Donc $\mathfrak{q} = \mathfrak{q}'$.

Pour finir, supposons π fini et montrons que les fibres de π sont finies. Soit $\mathfrak{p}$ un idéal premier de A. Comme précédemment, on peut supposer que A est local et que $\mathfrak{p}$ est son idéal maximal. Alors $B/\mathfrak{p}B$ est une k-algèbre de dimension finie (où $k = A/\mathfrak{p}$) et $\pi^{-1}(\mathfrak{p})$ est en bijection avec les idéaux premiers (i.e. maximaux) de $B/\mathfrak{p}B$. Il n'y en a bien sûr qu'un nombre fini. ■

Action d'un groupe fini.

Soit G un groupe fini agissant sur A. Posons

$$A^G = \{a \in A \mid \forall\ g \in G,\ {}^g a = a\}.$$

Proposition I. *On a :*

(a) *A est entier sur A^G.*

(b) *Le groupe G agit transitivement sur les fibres de l'application $\mathrm{Spec}\, A \to \mathrm{Spec}\, A^G$ (qui est surjective).*

Preuve - (a) Soit $a \in A$. Posons

$$P = \prod_{g \in G} (X - {}^g a) \in A[X].$$

Alors P est invariant sous l'action de G, donc $P \in A^G[X]$. De plus, P est unitaire et $P(a) = 0$.

(b) La surjectivité de l'application $\mathrm{Spec}\, A \to \mathrm{Spec}\, A^G$ découle du (a) et du théorème H. Soit $\mathfrak{p}$ un idéal premier de A^G. Pour montrer que G agit transitivement sur la fibre de π^* au-dessus de $\mathfrak{p}$ nous pouvons, grâce au lemme D, supposer que A est local d'idéal maximal $\mathfrak{p}$. Soient $\mathfrak{q}$ et $\mathfrak{q}'$ deux idéaux premiers de A tels que $\mathfrak{q} \cap A^G = \mathfrak{q}' \cap A^G = \mathfrak{p}$. Puisque A est entier sur A^G (voir

proposition I) et puisque $\mathfrak{p}$ est maximal, on en déduit que $\mathfrak{q}$ et $\mathfrak{q}'$ sont des idéaux maximaux de A (voir proposition G). Supposons que $\mathfrak{q}' \neq {}^g\mathfrak{q}$ pour tout $g \in G$. D'après le lemme chinois, il existe $a \in A$ tel que

$$a \equiv 0 \bmod \mathfrak{q}'$$

et

$$a \equiv 1 \bmod {}^g\mathfrak{q}$$

pour tout $g \in G$. Posons $x = \prod_{g\in G} {}^g a$. Puisque ${}^g a \notin \mathfrak{q}$ pour tout $g \in G$, on a $x \notin \mathfrak{q}$. Mais, $x \in \mathfrak{q}' \cap A^G = \mathfrak{p} \subset \mathfrak{q}$, ce qui contredit l'hypothèse. D'où le résultat. ■

Corollaire J. *Les fibres de l'application* $\operatorname{Spec} A \to \operatorname{Spec} A^G$ *sont finies.*

Supposons maintenant que A est intègre. Notons L le corps des fractions de A et K le corps des fractions de A^G.

Proposition K. *Avec les notations précédentes, on a :*

(a) *Si $x \in L$, il existe $a \in A$ et $u \in A^G$, $u \neq 0$ tel que $x = a/u$.*
(b) $K = L^G$.

Preuve - (a) Soit $x \in L$. Il existe $a \in A$ et $u \in A$, $u \neq 0$, tel que $x = a/u$. Posons

$$a' = a \prod_{\substack{g\in G \\ g\neq 1}} {}^g u \qquad \text{et} \qquad u' = \prod_{g\in G} {}^g u.$$

Alors $a' \in A$, $u' \in A^G$, $u' \neq 0$ et $x = a'/u'$.

(b) découle immédiatement de (a). ■

Proposition L. *Si A est intègre et intégralement clos, alors A^G est intègre et intégralement clos.*

Preuve - Si $x \in K$ est entier aur A^G, alors il est entier sur A, donc il appartient à A car A est supposé intégralement clos. Donc $x \in A \cap K = A^G$. ■

Si $|G|$ est inversible dans un anneau commutatif R, on pose

$$e_G = \frac{1}{|G|} \sum_{g\in G} g \in R[G].$$

Notons que $ge_G = e_G g = e_G$ pour tout $g \in G$. En particulier, e_G est un *idempotent* (i.e. $e_G^2 = e_G$) central. La proposition suivante est immédiate.

Proposition M. *Supposons $|G|$ inversible dans R. Soit M un $R[G]$-module. Alors*

$$M^G = e_G M.$$

En d'autres termes, pour $m \in M$, on a $m \in M^G$ si et seulement si $e_G m = m$.

Corollaire N. *Supposons $|G|$ inversible dans R. Soit M un $R[G]$-module et N un sous-$R[G]$-module. Alors l'application canonique $M^G \to (M/N)^G$ est surjective.*

Algèbre symétrique.

Soit k un corps commutatif et soit V un k-espace vectoriel de dimension finie. On pose $T^0(V) = k$ et, pour $r \geqslant 1$,

$$T^r(V) = \underbrace{V \otimes_k V \otimes_k \cdots \otimes_k V}_{r \text{ fois}}.$$

On pose ensuite

$$T(V) = \bigoplus_{r \geqslant 0} T^r(V).$$

Alors le produit tensoriel $\otimes_k$ induit une application bilinéaire

$$T^r(V) \times T^s(V) \longrightarrow T^{r+s}(V)$$

qui fait de $T(V)$ une k-algèbre associative : on l'appelle l'*algèbre tensorielle de V* (sur k). Si $f : V \to W$ est une application linéaire, on note $T^r(f) : T^r(V) \to T^r(W)$ l'unique application linéaire telle que

$$T^r(f)(v_1 \otimes \cdots \otimes v_r) = f(v_1) \otimes \cdots \otimes f(v_r)$$

pour tous $v_1, \ldots, v_r \in V$. Alors $T(f) = \oplus_{r \geqslant 0} T^r(f) : T(V) \to T(W)$ est un morphisme de k-algèbres.

Propriété universelle. *Soit $f : V \to A$ une application linéaire, où A est une k-algèbre associative. Alors il existe un unique morphisme de k-algèbres $\tilde{f} : T(V) \to A$ étendant f.*

Notons I_r le sous-k-espace vectoriel de $T^r(V)$ engendré par les $v_1 \otimes \cdots \otimes v_r - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(r)}$ pour tous $v_1, \ldots, v_r \in V$ et $\sigma \in \mathfrak{S}_r$ (groupe symétrique de degré r). Alors $I = \oplus_{r \geqslant 0} I_r$ est un idéal bilatère de $T(V)$. On pose

$$S(V) = T(V)/I = \bigoplus_{r \geqslant 0} T^r(V)/I_r = \bigoplus_{r \geqslant 0} S^r(V).$$

Alors $S(V)$ est une k-algèbre associative et commutative, appelée *algèbre symétrique de V* (sur k). Puisque $\mathfrak{S}_r$ est engendré par des transpositions, il est facile de vérifier que I est l'idéal bilatère de $T(V)$ engendré par les $v \otimes v' - v' \otimes v \in T^2(V) = V \otimes V$, où v et v' parcourent V. Le produit dans $S(V)$ sera noté usuellement.

Propriété universelle. *Soit $f : V \to A$ une application linéaire, où A est une k-algèbre associative COMMUTATIVE. Alors il existe un unique morphisme de k-algèbres $\tilde{f} : S(V) \to A$ étendant f.*

Proposition O. *Soit $X_1, \ldots, X_n$ une k-base de V. Alors $X_1, \ldots, X_n$ sont algébriquement indépendants dans $S(V)$ et ils engendrent $S(V)$.*

Corollaire P. *Si $n = \dim V$ et si $r \geqslant 0$, alors*

$$\dim S^r(V) = \begin{pmatrix} r+n-1 \\ n-1 \end{pmatrix}.$$

Proposition Q. *Soient V et W deux k-espaces vectoriels de dimension finie. Alors l'application naturelle $\oplus_{i=0}^r S^i(V) \otimes_k S^{r-i}(W) \to S^r(V \oplus W)$ est un isomorphisme de k-espaces vectoriels. Ces isomorphismes induisent un isomorphisme de k-algèbres $S(V) \otimes_k S(W) \simeq S(V \oplus W)$.*

Preuve - Ceci revient à dire que

$$k[X_1, \ldots, X_m] \otimes_k k[X_{m+1}, \ldots, X_{m+n}] \simeq k[X_1, \ldots, X_{m+n}]. \; \square$$

Notons $\mathrm{Fonc}(V, k)$ l'ensemble des fonctions quelconques $V \to k$. C'est une k-algèbre commutative pour la multiplication naïve. Alors V^* est un sous-espace vectoriel de $\mathrm{Fonc}(V, k)$. Par

la propriété universelle des algèbres symétriques, on obtient ainsi un morphisme de k-algèbres $S(V^*) \to \mathrm{Fonc}(V,k)$ dont l'image est la k-algèbre des fonctions *polynômiales* $V \to k$, notée $\mathrm{Pol}(V,k)$.

Proposition R. *Si k est infini, l'application $S(V^*) \to \mathrm{Pol}(V,k)$ est un isomorphisme de k-algèbres.*

Supposons maintenant que V est un k-espace vectoriel gradué de dimension finie, c'est-à-dire $V = V_1 \oplus \cdots \oplus V_d$, où V_i est appelé la *composante homogène de degré i* de V. Par la proposition Q, on a

$$S(V) = S(V_1) \otimes \cdots \otimes S(V_N).$$

Les éléments de $S^r(V_i)$ sont dits *homogènes de degré ri*, ce qui munit $S(V_i)$ d'une structure de k-algèbre commutative graduée. Par produit tensoriel, $S(V)$ devient une k-algèbre commutative graduée.

Exemple - Le cas le plus fréquent est celui où $V = V_1$ est concentré en degré 1. On retrouve alors la structure usuelle de k-algèbre graduée de $S(V)$. □

Exemple - Le groupe symétrique $\mathfrak{S}_n$ agit sur la k-algèbre $k[X_1,\ldots,X_n]$ par permutations des indéterminées : ${}^\sigma X_i = X_{\sigma(i)}$. Il est bien connu que la k-algèbre des polynômes symétriques $k[X_1,\ldots,X_n]^{\mathfrak{S}_n}$ est engendrée par les polynômes symétriques élémentaires $\sigma_1 = X_1 + \cdots + X_n$, $\ldots$, $\sigma_n = X_1 \ldots X_n$, et que ces derniers sont algébriquement indépendants. Si on pose $V_i = k\Sigma_i$ et $V = V_1 \oplus \cdots \oplus V_n \subset k[X_1,\ldots,X_n]$, cela signifie que l'application $S(V) \to k[X_1,\ldots,X_n]^{\mathfrak{S}_n}$ est un isomorphisme de k-algèbres graduées. □

Algèbres de type fini. Soit k un corps commutatif. Soit A une k-algèbre de type fini.

Proposition S. *A est un anneau nœthérien.*

Proposition T. *Si A est un corps, alors A est une extension algébrique finie de k.*

Corollaire U. *Si k est algébriquement clos, alors l'application $\mathrm{Hom}_{k-\mathrm{alg}}(A,k) \to \mathrm{Max}(A)$, $\varphi \mapsto \mathrm{Ker}\,\varphi$ est bijective.*

Preuve - En effet, si $\mathfrak{m}$ est un idéal maximal de $\mathrm{Max}(A)$, alors $A/\mathfrak{m}$ est une k-algèbre de type fini et c'est un corps. C'est donc, d'après la proposition T, une extension algébrique finie de k. Ce dernier étant algébriquement clos, l'application naturelle $k \to A \to A/\mathfrak{m}$ est un isomorphisme. ■

Corollaire V. *Supposons k algébriquement clos. Soient X_1, $\ldots$, X_n des indéterminées sur k et soient $P_1, \ldots P_r \in k[X_1,\ldots,X_n]$ et notons I l'idéal qu'ils engendrent. Soit*

$$\mathcal{V}(I) = \{(x_1,\ldots,x_n) \in k^n \mid P_1(x_1,\ldots,x_n) = \cdots = P_r(x_1,\ldots,x_n) = 0.$$

Si $P \in k[X_1,\ldots,X_n]$ s'annule sur $\mathcal{V}$, alors il existe $e \geqslant 1$ tel que $P^e \in I$.

Preuve - Soit $A = k[X_1,\ldots,X_n][T]/(P_1,\ldots,P_r,1-PT)$. Posons

$$\mathcal{V}' = \{(x_1,\ldots,x_n,t) \in k^{n+1} \mid P_1(x_1,\ldots,x_n) = \cdots = P_r(x_1,\ldots,x_n) = 1 - tP(x_1,\ldots,x_n) = 0\}.$$

Alors, par hypothèse, $\mathcal{V}' = \varnothing$. Or, d'après le corollaire U, $\mathcal{V}'$ est en biijection avec les idéaux maximaux de A. Donc $(P_1,\ldots,P_r,1-PT) = k[X_1,\ldots,X_n][T]$. En d'autres termes, il existe α_1, $\ldots$, α_r, $\beta \in k[X_1,\ldots,X_n,T]$ tel que $\alpha_1 P_1 + \cdots + \alpha_r P_r + \beta(1-TP) = 1$. Soit $f : k[X_1,\ldots,X_n,T] \to k(X_1,\ldots,X_n)$, $X_i \mapsto X_i$, $T \mapsto 1/P$. En appliquant f à l'égalité

précédente, et en multipliant par une puissance suffisamment grande de P, on obtient le résultat souhaité. ■

Proposition W. *Soit k' une extension algébrique de k. Posons $A' = k' \otimes_k A$. Alors $A \subset A'$. De plus, l'application* $\mathrm{Spec}(A') \to \mathrm{Spec}(A)$, $\mathfrak{p} \mapsto \mathfrak{p} \cap A$ *est surjective et a ses fibres finies. D'autre part, $\mathfrak{p}$ est maximal si et seulement si $\mathfrak{p} \cap \bar{A}$ est maximal.*

Exercices de la partie 0

Exercice X. Soit A un anneau et soit G un sous-groupe fini de $\mathrm{Aut}_{\mathrm{anneau}} A$. On suppose A intègre et intégralement clos. On note K le corps des fractions de A. Soit A_0 un sous-anneau de A^G intégralement clos et soit K_0 son corps des fractions. On suppose que $[K : K_0] = |G|$ et que A^G et entier sur A_0. Montrer que $A_0 = A^G$.

Partie I. Introduction

Sauf mention explicite du contraire, tous les anneaux et toutes les algèbres de ce cours seront commutatifs (commutatives).

Le théorème de base, bien que facile, de la théorie des invariants d'un groupe fini agissant sur une k-algèbre de type fini est le suivant :

Théorème 0. *Soit A un anneau commutatif et soit G un groupe fini agissant sur A (par automorphismes d'anneau). Alors :*

(a) *A est entier sur A^G.*
(b) *L'application $\operatorname{Spec} A \to \operatorname{Spec} A^G$, $\mathfrak{p} \mapsto \mathfrak{p} \cap A^G$ est surjective. Ses fibres sont des G-orbites. De plus, si $\mathfrak{p} \in \operatorname{Spec} A$, alors $\mathfrak{p} \in \operatorname{Max} A$ si et seulement si $\mathfrak{p} \cap A^G \in \operatorname{Max} A^G$.*
(c) *Si A est réduit, alors A^G est réduit.*
(d) *Si A est intègre, alors A^G est intègre.*
(e) *Si A est intègre et intégralement clos, alors A^G est intègre et intégralement clos.*
(f) *Si k est un corps, si A est une k-algèbre de type fini et si G agit sur A par automorphismes de k-algèbre, alors A est un A^G-module de type fini et A^G est une k-algèbre de type fini.*

Preuve - (a), (b), (c), (d) et (e) ont été montrés dans la partie . Montrons (f). Soient $x_1, \ldots, x_n$ des générateurs de la k-algèbre A. Posons $P_i = \prod_{\sigma \in G}(X - {}^{\sigma}x_i) \in A^G[X]$. Notons B la sous-algèbre de A engendrée par les coefficients des P_i, $1 \leqslant i \leqslant n$. Alors $B \subset A^G \subset A$. De plus, A est entière sur B et, puisque $A = B[x_1, \ldots, x_n]$, A est un B-module de type fini. Par suite, A^G est un B-module de type fini car B est nœthérienne. Donc A^G est une k-algèbre de type fini. ■

Exemple 0 - Polynômes symétriques. Le groupe fini $\mathfrak{S}_n$ agit sur $k[X_1, \ldots, X_n]$ par permutations des indéterminées :

$$ {}^{\sigma}X_i = X_{\sigma(i)}. $$

On a $k[X_1, \ldots, X_n]^{\mathfrak{S}_n} = k[\sigma_1, \ldots, \sigma_n]$ où les σ_j sont les polynômes symétriques élémentaires :

$$ \sigma_j = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_j \leqslant n} X_{i_1} X_{i_2} \ldots X_{i_j}. $$

De plus, σ_1, σ_2,..., σ_n sont algébriquement indépendants. □

Remarque 0 - Effectivité. La preuve du théorème 0 (f) n'est pas effective. Par contre, lorsque $|G|$ est inversible dans k, alors on peut rendre cette preuve effective. En effet, on remarque tout d'abord que l'anneau B de la preuve est construit explicitement. Posons $g = |G|$. Alors D'autre part, $A = \sum_{(i_1,\ldots,i_n) \in \{0,1,\ldots,g-1\}^n} B x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$. Par suite,

$$ A^G = \sum_{(i_1,\ldots,i_n) \in \{0,1,\ldots,g-1\}^n} B e_G(x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}) $$

car $e_G(xy) = xe_G(y)$ si $x \in A^G$. □

Proposition 0. *Soit k un corps, soit A une k-algèbre de type fini et soit G un groupe fini agissant sur A par automorphisme de k-algèbre. Alors il existe un sous-espace vectoriel de dimension finie V de A, engendrant A comme k-algèbre et stable sous G. On obtient ainsi un morphisme surjectif G-équivariant de k-algèbres $S(V) \to A$.*

Si de plus $|G|$ est inversible dans k, alors l'application induite $S(V)^G \to A^G$ est surjective.

PREUVE - Soient $x_1, \ldots, x_n$ des générateurs de la k-algèbre A. Posons $V = \sum_{\substack{\sigma \in G \\ 1 \leqslant i \leqslant n}} k\ {}^{\sigma}x_i$. Alors V est bien sûr G-stable, de dimension finie et il engendre A. ■

Dans ce cours, nous étudierons essentiellement la situation suivante :

- k est un corps commutatif ;
- V est un k-espace vectoriel de dimension finie ;
- G est un sous-groupe fini de $\mathbf{GL}_k(V)$.
- **Problème :** Étudier l'algèbre $S(V)^G$...

On appelle *pseudo-réflexion* un élément $s \in \mathbf{GL}_k(V)$ tel que $\dim \mathrm{Im}(s-1) = 1$. On appelle *réflexion* une pseudo-réflexion d'ordre 2. Si $G \subset \mathbf{GL}_k(V)$, on notera Réf$(G)$ l'ensemble des pseudo-réflexions de G. Un des buts du cours est de montrer le théorème suivant :

Théorème (Shephard-Todd, Chevalley). *Soit k un corps commutatif de caractéristique 0, soit V un k-espace vectoriel de dimension finie n et soit G un sous-groupe fini de $\mathbf{GL}_k(V)$. Alors les assertions suivantes sont équivalentes :*

(1) *G est engendré par des pseudo-réflexions.*
(2) *$S(V)$ est un $S(V)^G$-module libre de rang $|G|$.*
(3) *$S(V)^G$ est engendrée par n polynômes (homogènes) algébriquement indépendants.*

Si ces conditions sont satisfaites et si $d_1, \ldots, d_n$ sont les degrés des n polynômes homogènes algébriquement indépendants engendrant $S(V)^G$, alors

(a) *La suite $(d_1, \ldots, d_n)$ ne dépend pas (à permutation près) du choix des n générateurs homogènes algébriquement indépendants.*
(b) $|G| = d_1 \ldots d_n$.
(c) $|\text{Réf}(G)| = d_1 + \cdots + d_n - n$

EXEMPLE 0.1 - Soit $V = k^n$ et notons $(X_1, \ldots, X_n)$ sa base canonique. Le groupe symétrique $\mathfrak{S}_n$ agit sur V par permutation des vecteurs de la base : ${}^{\sigma}X_i = X_{\sigma(i)}$. On a $S(V) = k[X_1, \ldots, X_n]$ et $S(V)^G$ est l'algèbre des polynômes symétriques. Elle est donc engendrée par n éléments homogènes algébriquement indépendants, de degrés 1, 2, ..., n. Si on applique le théorème de Shephard-Todd-Chevalley, on obtient que $\mathfrak{S}_n$ est engendré par des pseudo-réflexions, ce qui équivaut au fait bien connu que $\mathfrak{S}_n$ est engendré par les transpositions. En appliquant (b) et (c), on obtient que $|\mathfrak{S}_n| = 1.2.\ldots.n = n!$ et que le nombre de transpositions de $\mathfrak{S}_n$ est $n(n-1)/2$. □

Exercices de la partie I

On se fixe ici un corps commutatif k et un k-espace vectoriel V de dimension finie $n \geqslant 1$.

Exercice I.1*. Soit G un sous-groupe fini de $\mathbf{GL}_k(V)$. Montrer qu'il existe un sous-k-espace vectoriel M de $S(V)$, stable par l'action de G et tel que M soit isomorphe à la représentation régulière de G (Indication : travailler avec les corps des fractions de $S(V)$ et $S(V)^G$ et utiliser le théorème de la base normale en théorie de Galois).

Exercice I.2. Supposons k de caractéristique différente de 2 et que $G =< \sigma >$ où $\sigma : V \to V$, $v \mapsto -v$. Alors $|G| = 2$.

(a) Montrer que $S(V)^G = \oplus_{r \geqslant 0} S^{2r}(V)$.
(b) Montrer que $S(V)^G$ est engendrée par $S^2(V)$.
(c) Si $n = 1$, montrer que $S(V)^G \simeq k[T]$, où T est une indéterminée.
(d) Si $n = 2$, montrer que $S(V)^G \simeq k[T_1, T_2, T]/(T^2 - T_1T_2)$, où T_1, T_2 et T sont des indéterminées. En particulier, il existe une sous-k-algèbre A de $S(V)^G$ engendrée par deux polynômes homogènes de degrés 2 et un élément $v \in S^2(V)$ tel que $S(V)^G = A \oplus Av$.

Exercice I.3. Supposons k de caractéristique différente de 2. Soit A la k-algèbre $k[X, Y]/(X^2 + Y^2 - 1)$. Notons x l'image de X dans A et y l'image de Y. Soit $G =< \sigma >$, où $\sigma^2 = 1$ et où ${}^\sigma x = -x$ et ${}^\sigma y = -y$. Montrer que $A^G \simeq k[T, U]/(T^2 + U^2 - U)$ (Indication : utiliser l'exercice I.2).

Exercice I.4. Soit A une k-algèbre commutative, G un groupe agissant sur A par automorphismes de k-algèbres, k' une extension de k. Montrer que l'application $G \times (k' \otimes_k A) \to k' \otimes_k A$, $\sigma \mapsto \mathrm{Id}_{k'} \otimes_k \sigma$ munit la k'-algèbre commutative $k' \otimes_k A$ d'une action de G et que $(k' \otimes_k A)^G = k' \otimes_k A^G$.

Exercice I.5. Soient V et V' deux k-espaces vectoriels de dimension finie. Soient $G \subset \mathbf{GL}_k(V)$ et $\mathbf{GL}_k(V')$. Alors $G \times G' \subset \mathbf{GL}_k(V \oplus V')$. Montrer que $S(V \oplus V')^{G \times G'} \simeq S(V)^G \otimes S(V')^{G'}$.

Exercice I.6. Soit $A = k[X, X^{-1}] \simeq k[X, Y]/(XY - 1)$ et soit σ l'automorphisme de A tel que ${}^\sigma X = X^{-1}$. On note $G =< \sigma >$ (on a bien sûr $|G| = 2$). Montrer que $A^G = k[X + X^{-1}]$.

Exercice I.7. Supposons que $k = \mathbb{R}$, que $n = 2$, que V est euclidien et que G est le groupe des automorphismes de V stabilisant un polygone régulier Γ à $r \geqslant 2$ côtés centré en l'origine. Soient $v_1, v_2, \ldots, v_r$ les sommets du polygône régulier.

(a) Montrer que $|G| = 2r$ et que G est engendré par deux réflexions s et t telles que $(st)^r = 1$.
(b) Soit $T = v_1^2 + \cdots + v_r^2 \in S^2(V)$. Montrer que $T \in S(V)^G$. Montrer que $T \neq 0$.
(c) Montrer que $U = v_1 v_2 \ldots v_r \in S^r(V)^G$.
(d) Montrer que, si $r \geqslant 3$, alors T et U sont algébriquement indépendants.
(e) Montrer, sans utiliser le théorème de Shephard-Todd-Chevalley, que $S(V)^G = \mathbb{R}[T, U]$ (si $r \geqslant 3$).

Exercice I.8. Supposons que k est un corps fini, que $V = k^2$ et que $G = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in k\}$. Soit (X_1, X_2) la base canonique de V. Soit W le sous-espace vectoriel de V engendré par X_2. Montrer que W est G-stable, que G agit trivialement sur V/W et que l'application $V^G \to$

$(V/W)^G$ n'est pas surjective. En particulier, l'application $S(V)^G \to S(V/W)^G = S(V/W)$ n'est pas surjective.

Exercice I.9. Supposons que k est un corps fini. Le groupe additif $(k,+)$ agit sur $k[X]$ *par translation* : si $a \in k$, on pose ${}^aX = X + a \in k[X]$. Montrer que $k[X]^{(k,+)} = k[X^q - X]$, où $q = |k|$.

Exercice I.10. Soit $V = k^2$, où k est un corps fini à q éléments. Soit $G = \mathbf{GL}_k(V) = \mathbf{GL}_2(k)$. Posons

$$G_1 = \mathbf{SL}_2(k) = \{\sigma \in G \mid \det\sigma = 1\}$$

et

$$H = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in k\}.$$

Soit (X,Y) la base canonique de V. On pose

$$T = XY^q - YX^q, \qquad U = \sum_{i=0}^{q} (X^{q-1})^i (Y^{q-1})^{q-i} = \frac{XY^{q^2} - YX^{q^2}}{XY^q - YX^q}$$

et

$$T' = Y^q - YX^{q-1} = \frac{T}{X}.$$

(a) Montrer que $T' = \prod_{\lambda\in k}(Y + \lambda X)$.
(b) Montrer que T' et X sont algébriquement indépendants et que $S(V)^H = k[X,T']$.
(c) Montrer que, pour tout $\sigma \in G$, on a ${}^\sigma T = (\det\sigma)T$. En déduire que $T \in S(V)^{G_1}$ et $U \in S(V)^G$.
(d) Montrer que T et U sont algébriquement indépendants et que $S(V)^{G_1} = k[T,U]$.
(e) En déduire que $S(V)^G = k[T^{q-1}, U]$.

Exercice I.11 (Bourbaki, "Groupes et algèbres de Lie", chapitre V, §5, exercice 6). Supposons que k est un corps fini de cardinal q, que $V = k^n$ et que $G = \mathbf{GL}_n(k) = \mathbf{GL}_k(V)$. On note $(X_1, \dots, X_n)$ la base canonique de V. Posons

$$G_1 = \mathbf{SL}_n(k) = \{\sigma \in G \mid \det\sigma = 1\}.$$

Si $\mathbf{e} = (e_1, \dots, e_n)$ est une suite d'entiers naturels non nuls, on pose

$$L_{\mathbf{e}} = \det(X_i^{q^{e_j}})_{1 \leqslant i,j, \leqslant n} \in S(V) = k[X_1, \dots, X_n].$$

Posons $T = \prod_{j=1}^{n} \Big(\prod_{(a_{j+1},\dots,a_n)\in k^{n-j}} (X_j + \sum_{i=j+1}^{n} a_i X_i) \Big)$.

(a) Montrer que, pour tout $\sigma \in G$, ${}^\sigma L_{\mathbf{e}} = (\det\sigma) L_{\mathbf{e}}$. En particulier, $L_{\mathbf{e}} \in S(V)^{G_1}$.
(b) Montrer que T divise tous les $L_{\mathbf{e}}$.
(c) Montrer que $T = L_{(0,1,2,\dots,n-1)}$ et que T est homogène de degré $1 + q + q^2 + \cdots + q^{n-1}$.
(d) Si $1 \leqslant i \leqslant n$, on note $\mathbf{e}_i$ la suite $(0,1,2,\dots,n)$ à laquelle on a retiré i. Si $1 \leqslant i \leqslant n-1$, on pose $Y_i = L_{\mathbf{e}_i}/T$. Montrer que $Y_i \in S(V)^G$ et que Y_i est homogène de degré $q^n - q^i$.

(Nous montrerons dans un futur exercice que T, Y_1, …, Y_{n-1} sont algébriquement indépendants et que $S(V)^{G_1} = k[T, Y_1, \dots, Y_{n-1}]$ et $S(V)^G = k[T^{q-1}, Y_1, \dots, Y_{n-1}]$, ce qui généralise l'exercice I.10 ci-dessus.)

Partie II. Objets gradués

Fixons jusqu'à la fin de ce cours un corps commutatif k. Nous noterons $\bar{k}$ une clôture algébrique de k.

1. Espaces vectoriels gradués

On appellera *k-espace vectoriel gradué* tout k-espace vectoriel M muni d'une décomposition $M = \oplus_{r\in\mathbb{Z}} M_r$, où $\dim_k M_r < \infty$ et $M_r = 0$ si $r << 0$. Si $m = \sum_{r\in\mathbb{Z}} m_r \in M$ avec $m_r \in M_r$ et si $m \neq 0$, on appellera *degré de m*, et on notera $\deg m$, le plus grand entier naturel r tel que $m_r \neq 0$. Les éléments de M_r seront dits *homogènes* (*de degré r*).

Soient $M = \oplus_{r\in\mathbb{Z}} M_r$ et $N = \oplus_{r\in\mathbb{Z}} N_r$ deux k-espaces vectoriels gradués. Une application linéaire $f : M \to N$ sera dite *de degré d* ($d \in \mathbb{Z}$) si $f(M_r) \subset N_{r+d}$ pour tout $r \geqslant 0$. On dit que f est un *morphisme de k-espaces vectoriels gradués* si f est de degré 0. Avec ces notations :

- $M \oplus N = \oplus_{r\in\mathbb{Z}}(M_r \oplus N_r)$ est un k-espace vectoriel gradué.
- $M \otimes N = \oplus_{r\in\mathbb{Z}}\Big(\oplus_{i\in\mathbb{Z}}^{r} M_i \otimes N_{r-i}\Big)$ est un k-espace vectoriel gradué.
- Si f est de degré d, alors $\operatorname{Ker} f$ et $\operatorname{Im} f$ sont des k-espaces vectoriels gradués.
- Si $d \in \mathbb{Z}$, alors on peut définir le *décalé de d* de M, noté $M[d]$, de la façon suivante : $M[d]_r = M_{r+d}$. C'est le même k-espace vectoriel, mais sa graduation a été décalée. Une application linéaire $f : M \to N$ est de degré d si et seulement si $f : M \to N[d]$ est un morphisme de k-espace vectoriels gradués.
- Si $M_r \subset N_r$ pour tout $r \geqslant 0$, alors $M \subset N$ et $N/M = \oplus_{r\,\geqslant\,0} N_r/M_r$ est un k-espace vectoriel gradué. On dit alors que M est un *sous-k-espace vectoriel gradué* de N.

On dit que M est *à degrés positifs* (respectivement *strictement positifs*) si $M_r = 0$ dès que $r < 0$ (respectivement $r \leqslant 0$).

Exemple 1.1 - Si M et N sont deux k-espaces vectoriels gradués, on notera $\operatorname{Hom}_k^{\mathrm{grad}}(M, N)$ le k-espace vectoriel des morphismes de k-espaces vectoriels gradués $M \to N$. Si M ou N est de dimension finie, alors

$$\operatorname{Hom}_k^{\mathrm{grad}}(M, N) = \bigoplus_{r\in\mathbb{Z}} \operatorname{Hom}_k(M_r, N_r)$$

est un k-espace vectoriel gradué. □

Si $V = \oplus_{i=d}^{e} V_i$ est un k-espace vectoriel gradué de dimension finie, on appelle *suite des degrés de V* (ou plus simplement *degrés de V*), et on note $\operatorname{Deg}_k(V)$, la suite (finie)

$$\operatorname{Deg}_k(V) = (\underbrace{d, \ldots, d}_{\dim V_d \text{ fois}}, \underbrace{d+1, \ldots, d+1}_{\dim V_{d+1} \text{ fois}}, \ldots, \underbrace{e, \ldots, e}_{\dim V_e \text{ fois}}).$$

En d'autres termes, si $(X_1, \ldots, X_n)$ est une base de V formée d'éléments homogènes tels que $\deg X_1 \leqslant \deg X_2 \leqslant \ldots \leqslant \deg X_n$, alors $\operatorname{Deg}_k(V) = (\deg X_1, \ldots, \deg X_n)$.

2. Algèbres graduées

2.A. Définition. Nous adopterons dans ce cours la définition restrictive suivante. Une k-algèbre A est dite *graduée* si elle est munie d'une décomposition $A = \oplus_{r \geqslant 0} A_r$ telle que :
- A est commutative ;
- $\dim A_r < \infty$ pour tout $r \geqslant 0$;
- $A_r A_s \subset A_{r+s}$;
- A est de type fini ;
- $A_0 = k$.

On se fixe une k-algèbre graduée $A = \oplus_{r \geqslant 0} A_r$. Un idéal I de A est dit *homogène* si $I = \oplus_{r \geqslant 0}(I \cap A_r)$. En d'autres termes, I est homogène si et seulement si il est engendré par des éléments homogènes. Si $I = \oplus_{r \geqslant 0} I_r$ est homogène, $I \neq A$, alors $A/I = \oplus_{r \geqslant 0} A_r/I_r$ est une k-algèbre graduée.

Si $B = \oplus_{r \geqslant 0} B_r$ est une k-algèbre graduée, une application linéaire $f : A \to B$ est appelée *morphisme de k-algèbres graduées* si c'est un morphisme de k-algèbre et si $f(A_r) \subset B_r$ pour tout $r \geqslant 0$. Si $f : A \to B$ est un morphisme de k-algèbres graduées, alors $\mathrm{Ker}\, f$ est un idéal homogène de A. On peut aussi définir de façon évident la notion de *sous-k-algèbre graduée*.

Exemple 2.1 - Si V est un k-espace vectoriel de dimension finie, alors $S(V) = \oplus_{r \geqslant 0} S^r(V)$ est une k-algèbre graduée (en décrétant que les éléments de $S^r(V)$ sont homogènes de degré r).

Plus généralement, si $V = V_1 \oplus \cdots \oplus V_d$ est un k-espace vectoriel gradué de dimension finie à degrés strictement positifs (V_i étant la composante homogène de degré i), alors $S(V) = S(V_1) \otimes \cdots \otimes S(V_d)$ est une k-algèbre graduée. Il faut cependant bien faire attention : la composante homogène de degré r de $S(V)$ n'est pas $S^r(V)$ en général. C'est

$$\bigoplus_{\substack{(r_1,\ldots,r_d)\in\mathbb{N}^d \\ r_1+2i_2+\cdots+dr_d=r}} S^{r_1}(V_1) \otimes \cdots \otimes S^{r_d}(V_d). \ \square$$

Exemple 2.2 - Si V est un k-espace vectoriel de dimension finie et si $G \subset \mathbf{GL}_k(V)$, alors $S(V)^G = \oplus_{r \geqslant 0} S^r(V)^G$ est une k-algèbre graduée. $\square$

Exemple 2.3 - $A_+ = \oplus_{r \geqslant 1} A_r$ est un idéal homogène de A. C'est l'unique idéal homogène maximal de A. $\square$

Soit I un idéal de A. On appelle radical de I (dans A), et on note $\sqrt{I}$, l'ensemble des éléments $a \in A$ tels que $a^e \in I$ pour un $e \geqslant 1$. On appelle le *nilradical* de A, et on note $\mathrm{nil}(A)$, le radical de l'idéal nul, c'est-à-dire l'ensemble des éléments nilpotents de A. Puisque A est commutative, $\sqrt{I}$ (et donc $\mathrm{nil}(A)$) est un idéal de A.

Lemme 2.4. *Si I est homogène, alors $\sqrt{I}$ est homogène. En particulier,* $\mathrm{nil}(A)$ *est homogène.*

Preuve - Quitte à quotienter par I, on peut supposer que $I = 0$. Soit $a \in A$ un élément nilpotent, $a \neq 0$. Notons $d = \deg a$. Alors $a = a_0 + a_1 + \cdots + a_d$, avec $a_i \in A_i$. Soit $e \geqslant 1$ tel que $a^e = 0$. Alors a_d^e est la composante homogène de degré de de a^e, donc $a_d^e = 0$, ce qui montre que a_d est nilpotent. Par suite, $a - a_d = a_0 + a_1 + \cdots + a_{d-1}$ est nilpotent. On montre alors facilement par récurrence sur $\deg a$ que a_0, a_1, …, a_d sont nilpotents. Donc $\mathrm{nil}(A) = \oplus_{r \geqslant 0}(\mathrm{nil}(A) \cap A_r)$. ■

2.B. Modules gradués. Un A-module M est dit *gradué* s'il est muni d'une décomposition $M = \oplus_{r \in \mathbb{Z}} M_r$ qui en fait un k-espace vectoriel gradué vérifiant de plus $A_r M_s \subset M_{r+s}$.

Exemple 2.5 - Un idéal homogène de A est un A-module gradué. $\square$

Si M et N sont deux A-modules gradués, on appelle *morphisme de A-modules gradués* tout morphisme de A-module $f : M \to N$ tel que $f(M_r) \subset N_r$ pour tout $r \geqslant 0$. Si tel est le cas, alors $\operatorname{Ker} f$ et $\operatorname{Im} f$ sont des A-modules gradués. De plus, $M \oplus N$ est un A-module gradué. On peut définir sur les A-modules gradués les opérations de somme directe, de décalage, les notions d'applications A-linéaires de degré d (le noyau et l'image étant encore des A-modules gradués)...

Lemme de Nakayama gradué. *Soit M un A-module gradué. Alors $A_+M = M$ si et seulement si $M = 0$.*

Preuve - Si $M = 0$, alors $A_+M = 0 = M$. Réciproquement, supposons que $M \neq 0$. Soit r_0 le plus petit entier naturel tel que $M_{r_0} \neq 0$. Alors $A_+M \subset \oplus_{r \geqslant r_0+1} M_r$, donc $A_+M \neq M$. ■

Corollaire 2.6. *Soit N est un sous-A-module gradué de M. Alors $N + A_+M = M$ si et seulement si $N = M$.*

Preuve - Il suffit d'appliquer le lemme de Nakayama gradué à M/N. ■

Corollaire 2.7. *Si $f : M \to N$ est une application A-linéaire de degré d entre A-modules gradués, alors f est surjective si et seulement si $\bar{f} : M/A_+M \to N/A_+N$ est surjective.*

Preuve - Il suffit d'appliquer le corollaire 2.6 à $\operatorname{Im} f \subset N$. ■

Corollaire 2.8. *Soit V un sous-k-espace vectoriel de A.*

(a) *Si V engendre M, alors $V + A_+M = M$.*
(b) *Supposons que V est un sous-k-espace vectoriel gradué de M. Alors M est engendré par V si et seulement si $V + A_+M = M$.*

Preuve - (a) Si V engendre M, alors l'image de V dans M/A_+M engendre le $A/A_+ = k$-espace vectoriel M/A_+M.

(b) D'après (a), il ne nous reste plus qu'à montrer que, si $V + A_+M = M$, alors V engendre M. Mais cela résulte immédiatement du lemme de Nakayama gradué car le sous-A-module de M engendré par V est gradué lui aussi. ■

Corollaire 2.9. *On a :*

(a) *M est de type fini si et seulement si $\dim_k M/A_+M < \infty$.*
(b) *Supposons M de type fini. Alors le nombre $\dim_k M/A_+M$ est égal au nombre minimal de générateurs du A-module M. C'est aussi égal au nombre minimal de générateurs homogènes du A-module M.*

Corollaire 2.10. *Supposons M de type fini sur A. Soit $n = \dim M/A_+M$. Soient $x_1, \ldots, x_n$ des générateurs homogènes de M tels que $\deg x_1 \leqslant \deg x_2 \leqslant \ldots \leqslant \deg x_n$. Alors*

$$(\deg x_1, \deg x_2, \ldots, \deg x_n) = \operatorname{Deg}_k(M/A_+M).$$

Si M est un A-module gradué de type fini, on appelle *suite des degrés de M* (ou plus simplement *degrés de M*), et on note $\operatorname{Deg}_A(M)$, la suite $\operatorname{Deg}_k(M/A_+M)$.

Proposition 2.11. *On a :*

(a) *Si V est un sous-k-espace vectoriel de dimension finie de A_+ tel que l'application canonique $S(V) \to A$ est surjective, alors $V + (A_+)^2 = A_+$.*

(b) *Si V est un sous-k-espace vectoriel gradué de dimension finie de A_+, alors l'application $S(V) \to A$ est surjective si et seulement si $V + A_+^2 = A_+$.*

PREUVE - (a) est clair. Montrons (b). Compte tenu de (a), il ne reste qu'à montrer que, si V est un sous-k-espace vectoriel gradué de dimension finie de A_+ tel que $V + A_+^2 = A_+$, alors l'application canonique $\pi : S(V) \to A$ est surjective. On va montrer par récurrence sur r que $A_r \subset \operatorname{Im}\pi$. C'est clair lorsque $r = 0$. Supposons maintenant $r \geqslant 1$. Soit $a \in A_r$. On a $V_r + (A_+^2)_r = A_r$ par hypothèse. Donc $a = v + a'$, où $v \in V_r$ et $a' \in (A_+^2)_r$. On écrit $a' = \sum_{i\in I} x_i y_i$ avec x_i, y_i homogènes dans A_+. Alors, $\deg x_i < r$ et $\deg y_i < r$. On conclut alors grâce à l'hypothèse de récurrence. ■

Corollaire 2.12. *Le nombre $\dim_k(A_+/A_+^2)$ est le nombre minimal de générateurs de la k-algèbre A. C'est aussi le nombre minimal de générateurs homogènes de A.*

Notons $n = \dim_k(A_+/A_+^2)$. Si $x_1, \ldots, x_n$ est une famille d'eléments homogènes de A engendrant A telle que $\deg x_1 \leqslant \deg x_2 \leqslant \ldots \leqslant \deg x_n$, alors

$$(\deg x_1, \deg x_2, \ldots, \deg x_n) = \operatorname{Deg}_k(A_+/A_+^2) = \operatorname{Deg}_A(A_+).$$

On appellera *suite des degrés de A* (ou plus simplement *degrés de A*), et on notera $\operatorname{Deg}(A)$, la suite $\operatorname{Deg}_k(A_+/A_+^2)$. Fixons maintenant jusqu'à la fin de cette partie un sous-k-espace vectoriel gradué V de A_+ tel que $A_+^2 \oplus V = A_+$. On notera $\pi : S(V) \to A$ le morphisme canonique d'algèbres graduées :

$$0 \longrightarrow \operatorname{Ker}\pi \longrightarrow S(V) \xrightarrow{\pi} A \longrightarrow 0.$$

On appelle *suite des degrés des relations* de A (ou *degrés des relations* de A), et on note $\operatorname{Rel}(A)$ la suite des degrés du $S(V)$-module gradué de type fini $\operatorname{Ker}\pi$:

$$\operatorname{Rel}(A) = \operatorname{Deg}_{S(V)}(\operatorname{Ker}\pi).$$

On dit que A est une *k-algèbre de polynômes*, ou que A est *régulière*, si $\operatorname{Ker}\pi = 0$ (c'est-à-dire si $\operatorname{Rel}(A) = \varnothing$).

EXEMPLE 2.13 - Soit $V = V_1 \oplus \cdots \oplus V_d$ un k-espace vectoriel gradué de dimension finie. Alors $\operatorname{Deg}(S(V)) = \operatorname{Deg}_k(V)$ et $\operatorname{Rel}(S(V)) = \varnothing$. □

EXEMPLE 2.14 - Soit V un k-espace vectoriel. Supposons k de caractéristique différente de 2 et soit $G = \{\mathrm{Id}_V, -\mathrm{Id}_V\}$. Alors $S(V)_+^G/(S(V)_+^G)^2 \simeq S^2(V)$. Donc $\operatorname{Deg}(S(V)^G) = (2, 2, \ldots, 2)$, le nombre 2 apparaissant $n(n+1)/2$ fois (voir exercice I.2 (b)). Si $\dim V = 2$, alors $\operatorname{Rel}(S(V)^G) = 4$ (voir exercice I.2 (d)). □

REMARQUE 2.15 - Soit V' un autre supplémentaire gradué de $(A_+)^2$ dans A_+. Notons $\pi' : S(V') \to A$ le morphisme surjectif canonique correspondant. Alors il existe un isomorphisme d'algèbres graduées $\psi : S(V) \to S(V')$ tel que $\pi = \pi' \circ \psi$. En particulier, ψ induit un isomorphisme $\operatorname{Ker}\pi \simeq \operatorname{Ker}\pi'$ qui montre que $\operatorname{Rel}(A)$ ne dépend pas du choix de V. □

3. Liberté

Nous allons ici nous intéresser à plusieurs questions concernant les modules libres (caractérisation, résolutions libres, complexes de Koszul).

3.A. Injection directe. Soient M et N deux A-modules gradués et soit $f : M \to N$ un morphisme de A-modules gradués. On dit que f est une *injection directe* si f est injective et s'il existe un sous-A-module gradué N' de N tel que $N = f(M) \oplus N'$.

Proposition 3.1. *Soient M et N deux A-modules libres de type fini gradués et soit $f : M \to N$ un morphisme de A-modules gradués. Alors f est une injection directe (respectivement un isomorphisme) si et seulement si $\bar{f} : M/A_+M \to N/A_+N$ est injective (respectivement un isomorphisme).*

Preuve - Il est clair que, si f est une injection directe (respectivement un isomorphisme), alors $\bar{f} : M/A_+M \to N/A_+N$ est injective (respectivement un isomorphisme). Il suffit donc de montrer que, si $\bar{f}$ est injective, alors f est une injection directe (en effet, pour l'assertion concernant les isomorphismes, la surjectivité découle du lemme de Nakayama gradué).

Supposons donc que $\bar{f}$ soit injective. Soit $\bar{g} : N/A_+N \to M/A_+M$ tel que $\bar{g} \circ \bar{f} = \mathrm{Id}_{m/A_+M}$ ($\bar{g}$ existe car on travaille ici avec des k-espaces vectoriels). Par composition avec la projection $N \to N/A_+N$, on obtient un morphisme de A-modules $\tilde{g} : N \to M/A_+M$ tel que $\tilde{g} \circ f$ soit la projection de M sur M/A_+M. Puisque N est libre, il existe un morphisme de A-modules $g : N \to M$ relevant $\tilde{g}$. Alors, d'après le lemme de Nakayama gradué, $g \circ f$ est surjectif. Or, un endomorphisme surjectif d'un A-module libre est un automorphisme (en effet, $\det(g \circ f) : \wedge^n M \simeq A \to \wedge^n M \simeq A$ est surjectif, où $n = \mathrm{rang}_A(M)$, ce qui montre que $\det(g \circ f)$ est inversible dans A). ■

3.B. Modules libres. Nous commençons par une caractérisation des modules libres. Nous aurons besoin pour cela de la notation suivante. Si M est un A-module gradué, nous noterons $\mathrm{Tor}_A(M)$ le noyau du morphisme de A-modules $\mu_M : A_+ \otimes_A M \to M$, $a \otimes_A m \mapsto am$. C'est un sous-A-module gradué de $A_+ \otimes_A M$.

Remarque - Le morphisme $A \otimes_A M \to M$, $a \otimes_A m \mapsto am$ est injectif. Cependant, en général, $A_+ \otimes_A M$ n'est pas un sous-A-module de $A \otimes_A M$. Il y a bien sûr un morphisme canonique $A_+ \otimes_A M \to A \otimes_A M$, mais il n'est pas injectif. □

Si $f : M \to N$ est une application A-linéaire de degré $d \in \mathbb{Z}$, alors f induit une application A-linéaire de degré d (par produit tensoriel) $\mathrm{Id}_{A_+} \otimes_A f : A_+ \otimes_A M \to A_+ \otimes_A N$. La restriction de ce morphisme à $\mathrm{Tor}_A(M)$ induit une application $\mathrm{Tor}_A(f) : \mathrm{Tor}_A(M) \to \mathrm{Tor}_A(N)$ qui est A-linéaire de degré d.

Proposition 3.2. *Soit $0 \longrightarrow M \xrightarrow{f} M' \xrightarrow{g} M'' \longrightarrow 0$ une suite exacte de A-modules gradués. Alors il existe un unique morphisme de A-modules gradués $\partial : \mathrm{Tor}_A(M'') \to M/A_+M$ tel que la suite*

$$\mathrm{Tor}_A(M) \xrightarrow{\mathrm{Tor}_A(f)} \mathrm{Tor}_A(M') \xrightarrow{\mathrm{Tor}_A(g)} \mathrm{Tor}_A(M'')$$

$$\xrightarrow{\partial} M/A_+M \xrightarrow{\bar{f}} M'/A_+M' \xrightarrow{\bar{g}} M''/A_+M'' \longrightarrow 0$$

est exacte.

Preuve - Commençons par définir l'application ∂. Pour simplifier les notations, on supposera que $M \subset M'$ et que $f : M \to M'$ est l'injection canonique. Notons $\mu_M : A_+ \otimes_A M \to M$,

$a \otimes m \mapsto am$. Soit $x \in A_+ \otimes_A M''$ tel que $\mu_{M''}(x) = 0$. Écrivons $x = \sum_{i\in I} a_i \otimes_A m_i''$, où I est fini, $a_i \in A_+$ et $m_i'' \in M''$. Soient m_i' des éléments de M' tels que $g(m_i') = m_i''$. Alors $\sum_{i\in I} a_i m_i' \in \operatorname{Ker} g = M$ par hypothèse. On note alors $\partial(x)$ l'image de $\sum_{i\in I} a_i m_i'$ dans M/A_+M.

Montrons que ∂ ne dépend pas des différents choix qui ont été faits. Tout d'abord, si $(n_i')_{i\in I}$ est un autre famille d'éléments de M' telle que $g(n_i') = m_i''$, alors $n_i' - m_i' \in M$ pour tout i et donc $\sum_{i\in I} a_i m_i' - \sum_{i\in I} a_i n_i' \in A_+M$, ce qui montre que ∂ ne dépend pas du choix des m_i'. Le fait que ça ne dépend pas du choix des a_i et m_i'' est alors évident. D'autre part il est clair que $\bar{f} \circ \partial = 0$.

• $\operatorname{Ker} \bar{g} = \operatorname{Im} \bar{f}$: soit $x \in M'$ tel que $\bar{x} \in \operatorname{Ker} \bar{g}$, où $\bar{x}$ désigne l'image de x dans M'. Cela signifie que $g(x) \in A_+M''$. Donc il existe $y \in A_+M'$ tel que $g(y) = g(x)$. Donc $x - y \in M$ et $\bar{f}(\overline{x-y}) = \bar{x} - \bar{y} = \bar{x}$ car $\bar{y} = 0$.

• $\operatorname{Ker} \bar{f} = \operatorname{Im} \partial$: soit $x \in M$ tel que $\bar{x} \in \operatorname{Ker} \bar{f}$. Alors $x \in A_+M'$. Écrivons $x = \sum_{i\in I} a_i m_i'$ avec $a_i \in A_+$ et $m_i' \in M'$. Posons $z = \sum_{i\in I} a_i \otimes g(m_i') \in A_+ \otimes_A M''$. Alors, puisque $x \in M$, on a $\mu_{M''}(z) = g(x) = 0$, donc $z \in \operatorname{Tor}_A(M'')$. Il est de plus clair, par construction de ∂, que $\partial(z) = \bar{x}$.

• $\operatorname{Ker} \partial = \operatorname{Im} \operatorname{Tor}_A(g)$: montrons tout d'abord que $\partial \circ \operatorname{Tor}_A(g) = 0$. Soit $x \in \operatorname{Tor}_A(M')$. On écrit $x = \sum_{i\in I} a_i \otimes_A m_i'$, avec $a_i \in A_+$, $m_i' \in M'$ et $\sum_{i\in I} a_i m_i' = 0$. Alors, $\partial(\operatorname{Tor}_A(g)(x)) = \partial(\sum_{i\in I} a_i \otimes_A g(m_i')) = \sum_{i\in I} a_i m_i' + A_+M = 0$ dans M/A_+M. Donc $\operatorname{Im} \operatorname{Tor}_A(g) \subset \operatorname{Ker} \partial$.

Réciproquement, soit $x \in \operatorname{Ker} \partial$. On écrit $x = \sum_{i\in I} a_i \otimes_A m_i''$, avec $a_i \in A_+$, $m_i'' \in M''$ et $\sum_{i\in I} a_i m_i'' = 0$. Soit $(m_i')_{i\in I}$ une famille d'él'ements de M' telle que $g(m_i') = m_i''$. Par construction, on a $\partial(x) = \sum_{i\in I} a_i m_i' + A_+M$. Puisque $x \in \operatorname{Ker} \partial$, on a $\sum_{i\in I} a_i m_i' \in A_+M$. Écrivons $\sum_{i\in I} a_i m_i' = \sum_{j\in J} b_j m_j$, avec $b_j \in A_+$ et $m_j \in M$. Posons

$$z = \sum_{i\in I} a_i \otimes_A m_i' - \sum_{j\in J} b_j \otimes_A m_j \in A_+ \otimes_A M'.$$

Alors $z \in \operatorname{Tor}_A(M')$ et

$$\operatorname{Tor}_A(g)(z) \sum_{i\in I} a_i \otimes_A g(m_i') - \sum_{j\in J} b_j \otimes_A g(m_j) = x$$

car $g(m_j) = 0$.

• $\operatorname{Ker} \operatorname{Tor}_A(g) = \operatorname{Im} \operatorname{Tor}_A(f)$: cela résulte immédiatement de l'exactitude à droite du produit tensoriel. ■

Corollaire 3.3. *Un A-module gradué M est libre si et seulement si* $\operatorname{Tor}_A(M) = 0$.

Preuve - L'application $\mu_A : A_+ \otimes A \simeq A_+ \to A$ est clairement injective. Donc, si M est un A-module libre, alors l'application μ_M est injective.

Réciproquement, supposons que $\operatorname{Tor}_A(M) = 0$. Soit E un sous-k-espace vectoriel gradué de M tel que $M = E \oplus A_+M$. Soit $L = A \otimes_k E$. C'est un A-module libre et l'application $g : L \to M$, $a \otimes_k v \mapsto av$ est un morphisme surjectif de A-modules gradués. Posons $K = \operatorname{Ker} g$. On a donc, d'après la proposition 3.2 et puisque $\operatorname{Tor}_A(M) = 0$,

$$0 \longrightarrow K/A_+K \longrightarrow L/A_+L \longrightarrow M/A_+M \longrightarrow 0.$$

Mais, $M/A_+M \simeq E \simeq L/A_+L$ et l'application $L/A_+L \to M/A_+M$ s'identifie, via les isomorphismes précédents, à Id_E. Donc $K/A_+K = 0$, ce qui implique que $K = 0$ d'après le lemme de Nakayama gradué. Donc $L \simeq M$ et M est libre. ■

Corollaire 3.4. *Soient M et N deux A-modules gradués tels que $M \oplus N$ est un A-module libre. Alors M et N sont libres.*

PREUVE - On a $\mathrm{Tor}_A(M \oplus N) = \mathrm{Tor}_A(M) \oplus \mathrm{Tor}_A(N)$. D'où le résultat d'après le corollaire 3.3. ■

3.C. Couverture libre, résolutions libres. Soit M un A-module gradué. Soit V_M un supplémentaire gradué de A_+M dans M. Alors l'application $\tau_M : A \otimes_k V_M \to M$, $a \otimes_k v \mapsto av$ est un morphisme surjectif de A-modules gradués d'après le lemme de Nakayama gradué. De plus, $A \otimes_k V_M$ est libre. Nous noterons ce A-module L_M. On dit que (L_M, τ_M) (ou que L_M lorsque le morphisme τ_M sera implicite) est une *couverture libre* de M.

REMARQUE 3.5 - Le couple (L_M, τ_M) ne dépend pas, à isomorphisme près, du choix du supplémentaire V_M. En d'autres termes, si V'_M est un autre supplémentaire gradué de A_+M dans M et si $\tau'_M : A \otimes_k V'_M \to M$, $a \otimes_k v \mapsto av$, alors il existe un isomorphisme de A-modules gradués $\psi : A \otimes_k V_M \to A \otimes_k V'_M$ tel que $\tau_M = \tau'_M \circ \psi$. □

Remarquons que τ_M induit le morphisme identité $L_M/A_+L_M \simeq V \to M/A_+M \simeq V$. Cela montre entre autres que que

$$\tau_M^{-1}(A_+M) = A_+L_M. \tag{3.6}$$

En particulier,

$$\mathrm{Ker}\,\tau_M \subset A_+L_M. \tag{3.7}$$

Proposition 3.8. *Soit L un A-module libre gradué et soit $\tau : L \to M$ un morphisme surjectif de A-modules gradués. Alors $(L, \tau) \simeq (L_M \oplus L', \tau_M \oplus 0)$, où L' est un A-module gradué.*

PREUVE - Il existe un morphisme $\psi : L \to L_M$ de A-modules gradués tel que $\tau = \tau_M \circ \psi$. La surjectivité de ψ implique alors que $L_M = \mathrm{Im}\,\psi + \mathrm{Ker}\,\tau_M$. Donc, d'après 3.7 et le lemme de nakayama gradué, on obtient que ψ est surjectif. Le A-module L_M étant lui aussi libre, il existe un morphisme de A-modules gradués $\theta : L_M \to L$ tel que $\psi \circ \theta = \mathrm{Id}_{L_M}$. Donc $L = \mathrm{Im}\,th \oplus \mathrm{Ker}\,\psi$. Or, $\mathrm{Im}\,\theta \simeq L_M$ et $\mathrm{Ker}\,\psi$ est libre d'après le corollaire 3.4. La preuve de la proposition est alors essentiellement complète. ■

Corollaire 3.9. *Soit L un A-module libre gradué et soit $\tau : L \to M$ un morphisme surjectif de A-modules gradués. Alors (L, τ) est une couverture libre de M si et seulement si* $\mathrm{Ker}\,\tau \subset A_+L$.

On appelle *résolution libre* de M toute suite exacte (éventuellement infinie) de A-modules gradués de la forme

$$\cdots \longrightarrow L_2 \longrightarrow L_1 \longrightarrow L_0 \longrightarrow M \longrightarrow 0,$$

où les L_i sont des A-modules gradués libres.

EXEMPLE 3.10 - Posons $L_M^{(0)} = L_M$ et $\tau_M^{(0)} = \tau_M$ et, pour $i \geqslant 0$, posons $L_M^{(i+1)} = L_{\mathrm{Ker}\,\tau_M^{(i)}}$ et $\tau_{M^{(i+1)}} = \tau_{\mathrm{Ker}\,\tau_M^{(i)}}$. Alors la suite

$$\cdots \longrightarrow L_M^{(2)} \xrightarrow{\tau_M^{(2)}} L_M^{(1)} \xrightarrow{\tau_M^{(1)}} L_M^{(0)} \xrightarrow{\tau_M^{(0)}} M \longrightarrow 0$$

est exacte : c'est une résolution libre de M. Nous l'appellerons *résolution libre minimale* de M. □

EXEMPLE 3.11 - Le k-espace vectoriel k est muni d'une structure naturelle de A-module via l'isomorphisme $k \simeq A/A_+$. Nous appellerons ce A-module de A-module *trivial*.

Supposons maintenant que $A = k[X, Y]$ où X et Y sont deux indéterminées. Posons

$$(\mathcal{K}) \qquad 0 \longrightarrow A[-2] \xrightarrow{\alpha} A[-1] \oplus A[-1] \xrightarrow{\beta} A \xrightarrow{\tau} k \longrightarrow 0,$$

où $\alpha(a) = aX \oplus (-aY)$, $\beta(a \oplus b) = aX + bY$ et $\tau : A \to k$ est la projection canonique. Alors $(\mathcal{K})$ est une résolution libre du A-module k : c'en est même une résolution minimale. □

3.D. Complexe de Koszul. Notons $\mathcal{K}_1(A) = A \otimes_k V$. C'est un A-module libre de rang $n = \dim_k V$. On a une application naturelle $d_1 : A \otimes_k V \to A$, $a \otimes_k v \mapsto av$. L'image de d_1 est A_+. Si $0 \leqslant i \leqslant n$, on note $\mathcal{K}_i(A) = \wedge^i \mathcal{K}_1(A)$. C'est un A-module gradué libre de rang $\begin{pmatrix} n \\ i \end{pmatrix}$. Notons que $\mathcal{K}_0(A) = A$.

On considère le complexe, noté $\mathcal{K}(A)$ et appelé *complexe de Koszul de A*,

$$0 \longrightarrow \mathcal{K}_n(A) \xrightarrow{d_n} \mathcal{K}_{n-1}(A) \xrightarrow{d_{n-1}} \cdots \xrightarrow{d_2} \mathcal{K}_1(A) \xrightarrow{d_1} A \xrightarrow{d_0} k \longrightarrow 0,$$

où

$$d_i(v_1 \wedge \cdots \wedge v_i) = \sum_{j=1}^{i} (-1)^{j+1} d_1(v_j)(v_1 \wedge \cdots \wedge v_{j-1} \wedge v_{j+1} \wedge \cdots \wedge v_i)$$

lorsque $i \geqslant 1$ et d_0 est l'application naturelle.

Proposition 3.12. *Avec les notations précédentes, on a :*

(a) *Si $0 \leqslant i \leqslant n-1$, alors $d_i \circ d_{i+1} = 0$.*
(b) $\operatorname{Im} d_i \subset A_+ \mathcal{K}_{i-1}(A)$.
(c) *Si $i \geqslant 2$ et si $v \in \mathcal{K}_1(A)$ et $x \in \mathcal{K}_{i-1}(A)$, alors $d_i(v \wedge x) = d_1(v)x - v \wedge d_{i-1}(x)$.*
(d) *L'application $\mathcal{K}_i(A)/A_+\mathcal{K}_i(A) \to A_+\mathcal{K}_{i-1}(A)/(A_+)^2\mathcal{K}_{i-1}(A)$ induite par d_i est injective.*

Preuve - (a) Soient $v_1, \ldots, v_{i+1}$ des éléments de $\mathcal{K}_1(A)$. Si j et j' sont deux éléments de $\{1, 2, \ldots, i+1\}$ tels que $j \neq j'$, on note $f_{j,j'}(v_1, \ldots, v_{i+1}) = v_{a_1} \wedge v_{a_2} \wedge \cdots \wedge v_{a_{i-1}}$, où $\{1, 2, \ldots, i+1\} \backslash \{j, j'\} = \{a_1, a_2, \ldots, a_{i-1}\}$ avec $a_1 \leqslant \ldots \leqslant a_{i-1}$. On a, pour $i \geqslant 1$,

$$\begin{aligned}
(d_i \circ d_{i+1})(v_1 \wedge \cdots \wedge v_{i+1}) &= \sum_{j=1}^{i+1} (-1)^{j+1} d_1(v_j) d_i(v_1 \wedge \cdots \wedge v_{j-1} \wedge v_{j+1} \wedge \cdots \wedge v_{i+1}) \\
&= \sum_{1 \leqslant j' < j \leqslant i+1} (-1)^{j+j'+2} d_1(v_j) d_1(v_{j'}) f_{j,j'}(v_1, \ldots, v_{i+1}) \\
&\quad + \sum_{1 \leqslant j < j' \leqslant i+1} (-1)^{j+j'+1} d_1(v_j) d_1(v_{j'}) f_{j,j'}(v_1, \ldots, v_{i+1}) \\
&= 0.
\end{aligned}$$

Cela montre la première assertion pour $i \geqslant 1$. Cette assertion est évidente lorsque $i = 0$.

(b) et (c) sont clairs.

(d) On a $\mathcal{K}_i(A)/A_+\mathcal{K}_i(A) \simeq \wedge^i V$ et $A_+\mathcal{K}_{i-1}(A)/(A_+)^2\mathcal{K}_{i-1}(A) \simeq V \otimes_k \wedge^{i-1} V$. À travers ces isomorphismes, l'application de l'assertion (d) s'identifie à l'application k-linéaire $\bar{d}_i : \wedge^i V \to V \otimes_k \wedge^{i-1} V$ définie par

$$\bar{d}_i(v_1 \wedge \cdots \wedge v_i) = \sum_{j=1}^{i} (-1)^{j+1} v_j \otimes (v_1 \wedge \cdots \wedge v_{j-1} \wedge v_{j+1} \wedge \cdots \wedge v_i)$$

pour tous $v_1, \ldots, v_i$ dans V. L'injectivité de $\bar{d}_i$ est alors immédiate. ■

Théorème 3.13. *Si A est régulière, alors le complexe de Koszul de A est exact.*

PREUVE - Si $v \in V$, nous noterons $\tilde{v} = 1 \otimes_k v \in \mathcal{K}_1(A)$. Tout d'abord, il est clair que, quelle que soit l'algèbre A, on a $\operatorname{Im} d_1 = \operatorname{Ker} d_0$. Fixons une base $(v_1, \dots, v_n)$ de V. Alors $(\tilde{v}_1, \dots, \tilde{v}_n)$ est une A-base de $K_1(A)$.

Pour montrer l'exactitude de $\mathcal{K}(A)$, nous raisonnerons par récurrence sur $n = \dim V$, le résultat étant évident lorsque $n = 0$ ou 1. Montrons pour commencer que $\operatorname{Im} d_2 = \operatorname{Ker} d_1$, c'est-à-dire que, si $x \in \operatorname{Ker} d_1$, alors il existe une famille $(a_{ij})_{1 \leqslant i<j \leqslant n}$ d'él'ements de A telle que $x = \sum_{1 \leqslant i<j \leqslant n} a_{ij}(v_i\tilde{v}_j - v_j\tilde{v}_i)$. Écrivons $x = \sum_{i=1}^{n} \alpha_i \tilde{v}_i$, avec $\alpha_i \in A$. On a alors

$$(*) \qquad \sum_{i=1}^{n} \alpha_i v_i = 0.$$

Regardons cette égalité dans l'algèbre $A/(Av_1 + \cdots + Av_{n-1})$. Cette dernière algèbre étant intègre, on a que $\alpha_n \in Av_1 + \cdots + Av_{n-1}$. Écrivons donc $\alpha_n = \sum_{i=1}^{n-1} a_{in}v_i$ et posons $y = x - \sum_{i=1}^{n-1} a_{in}(v_i\tilde{v}_n - v_n\tilde{v}_i)$. Alors $y = \sum_{i=1}^{n-1} \beta_i\tilde{v}_i$, avec $\beta_i \in A$ et $d_1(y) = 0$. On voit alors immédiatement qu'un raisonnement par récurrence permet de conclure que $y \in \operatorname{Im} d_2$ et donc que $x \in \operatorname{Im} d_2$.

Posons maintenant $A' = k[v_1, \dots, v_{n-1}] \subset A$. Alors A' est une k-algèbre régulière et A est un A'-module libre (de base $(1, v_n, v_n^2, v_n^3, \dots)$). Par suite, le complexe $A \otimes_{A'} \mathcal{K}(A')$ est exact par hypothèse de récurrence. Supposons $i \geqslant 2$ et soit $x \in \operatorname{Ker} d_i$. Écrivons $x = x_0 + \tilde{v}_n \wedge x_1$ avec $x_0 \in A \otimes_{A'} \mathcal{K}_i(A')$ et $x_1 \in A \otimes_{A'} \mathcal{K}_{i-1}(A')$. On a alors, d'après la proposition 3.12 (c), $d_i(x) = d_i(x_0) + v_n x_1 + \tilde{v}_n \wedge d_{i-1}(x_1)$. Puisque

$$\mathcal{K}_{i-1}(A) = \Big(A \otimes_{A'} \mathcal{K}_{i-1}(A')\Big) \oplus \Big(\tilde{v}_n \wedge (A \otimes_{A'} \mathcal{K}_{i-2}(A'))\Big)$$

et que l'application

$$A \otimes_{A'} \mathcal{K}_{i-2}(A') \longrightarrow \tilde{v}_n \wedge (A \otimes_{A'} \mathcal{K}_{i-2}(A'))$$

qui à z associe $\tilde{v}_n \wedge z$ est injective, on en déduit que $d_{i-1}(x_1) = 0$. Par l'exactitude du complexe $A \otimes_{A'} \mathcal{K}(A')$, on obtient qu'il existe $y_1 \in A \otimes_{A'} \mathcal{K}_i(A')$ tel que $x_1 = d_i(y_1)$. Par suite, $0 = d_i(x) = d_i(x_0 + v_n y_1)$ et donc, toujours par l'exactitude du complexe $A \otimes_{A'} \mathcal{K}(A')$, il existe $y_0 \in A \otimes_{A'} \mathcal{K}_{i+1}(A')$ tel que $x_0 + v_n y_1 = d_{i+1}(y_0)$. Il est alors facile de vérifier, en utilisant la proposition 3.12 (c), que $x = d_{i+1}(y_0 - \tilde{v}_n y_1)$. D'où $x \in \operatorname{Im} d_{i+1}$. ■

REMARQUE 3.14 - Il est possible de montrer que A est régulière si et seulement si le complexe de Koszul de A est exact, mais cela demande nettement plus de travail. Pour un exemple de complexe de Koszul non exact, voir l'exercice II.1. □

Nous concluons cette partie avec un théorème crucial donnant une borne sur la longueur d'une résolution libre du A-module trivial.

Théorème 3.15. *Soit*

$$\dots \xrightarrow{\tau_3} L_2 \xrightarrow{\tau_2} L_1 \xrightarrow{\tau_1} L_0 \xrightarrow{\tau_0} k$$

une résolution libre du A-module k. Alors il existe une famille de morphismes de A-modules gradués $f_i : \mathcal{K}_i(A) \to L_i$ telle que le diagramme

$$\begin{array}{ccccccccccc}
\cdots & \xrightarrow{d_3} & \mathcal{K}_2(A) & \xrightarrow{d_2} & \mathcal{K}_1(A) & \xrightarrow{d_1} & \mathcal{K}_0(A) & \xrightarrow{d_0} & k & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle \mathrm{Id}_k} & & \\
\cdots & \xrightarrow{\tau_3} & L_2 & \xrightarrow{\tau_2} & L_1 & \xrightarrow{\tau_1} & L_0 & \xrightarrow{\tau_0} & k & \longrightarrow & 0
\end{array}$$

soit commutatif. De plus, f_i est une injection directe pour tout $i \geqslant 0$.

PREUVE - L'existence des applications f_i est immédiate par récurrence sur i. Nous allons montrer, toujours par récurrence sur i, que f_i est une injection directe. Le fait que f_0 est une injection directe, c'est-à-dire que l'application $A/A_+ \simeq k \to L_0/A_+L_0$ est injective (voir proposition 3.1), est immédiat.

Soit maintenant que $i \geqslant 0$ et supposons que f_i est une injection directe. Considérons le diagramme

$$\begin{array}{ccc}
\mathcal{K}_{i+1}(A)/A_+\mathcal{K}_{i+1}(A) & \xrightarrow{\alpha} & A_+\mathcal{K}_i(A)/(A_+)^2\mathcal{K}_i(A) \\
\downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\
L_{i+1}/A_+L_{i+1} & \xrightarrow{\delta} & A_+L_i/(A_+)^2L_i,
\end{array}$$

où α est induit par d_{i+1}, β est induit par f_{i+1}, γ est induit par f_i et δ est induit par τ_{i+1}. Par hypothèse de récurrence, on a que γ est injective. De plus, α est injective d'après la proposition 3.12 (d). Par suite, β est injective, et donc f_{i+1} est une injection directe (voir lemme 3.1). ■

Corollaire 3.16. *Soit*

$$\ldots \xrightarrow{\tau_3} L_2 \xrightarrow{\tau_2} L_1 \xrightarrow{\tau_1} L_0 \xrightarrow{\tau_0} k$$

une résolution libre du A-module k. Alors $L_i \neq 0$ si $0 \leqslant i \leqslant \dim V$.

Exercices de la partie II

Exercice II.1. Soit $A = k[X, Y]/(XY)$.

(a) Calculer les degrés de A et la suite des degrés des relations de A.

(b) Montrer qu'il existe une sous-algèbre de polynômes A' de A et un élément homogène $a \in A$ tels que $A = A' \oplus A'a$.

(c) Montrer que le complexe de Koszul de l'algèbre $k[X, Y]/(XY)$ n'est pas exact.

Partie III. Série de Poincaré

4. Série de Poincaré

Notons $\mathbb{Z}((T))$ l'algèbre des séries formelles de Laurent $\mathbb{Z}[[T]][T^{-1}]$. Soit M un k-espace vectoriel gradué. On appelle *série de Poincaré* de M, et on note $P_M(T) \in \mathbb{Z}((T))$, la série formelle

$$P_M(T) = \sum_{r\in\mathbb{Z}} (\dim M_r).T^r.$$

Les premières propriétés de cette série sont immédiates :

- $P_{M\oplus N}(T) = P_M(T) + P_N(T)$.
- $P_{M\otimes N}(T) = P_M(T).P_N(T)$.
- Si $f : M \to N$ est un morphisme de k-espaces vectoriels gradués, alors $P_M(T) = P_{\operatorname{Ker} f}(T) + P_{\operatorname{Im} f}(T)$.
- $P_{M[d]}(T) = T^{-d}P_M(T)$.
- Soit

$$0 \longrightarrow M^{(1)} \xrightarrow{f_1} M^{(2)} \xrightarrow{f_2} \dots \xrightarrow{f_{e-1}} M^{(e)} \longrightarrow 0$$

une suite exacte, où les $M^{(i)}$ sont des k-espaces vectoriels gradués et où f_i est une application k-linéaire de degré $d_i \in \mathbb{Z}$. Alors

$$\sum_{i=1}^{e} (-1)^i T^{d_i+\dots+d_{e-1}} P_{M^{(i)}}(T) = 0. \tag{4.1}$$

En effet, on a une suite exacte de morphismes de k-espaces vectoriels gradués

$$0 \longrightarrow M^{(1)} \xrightarrow{f_1} M^{(2)}[d_1] \xrightarrow{f_2} M^{(3)}[d_1+d_2] \xrightarrow{f_3} \dots \xrightarrow{f_{e-1}} M^{(e)}[d_1+\dots+d_{e-1}] \longrightarrow 0,$$

d'où on déduit que

$$\sum_{i=1}^{e} (-1)^i P_{M^{(i)}[d_1+\dots+d_{i-1}]}(T) = 0.$$

Il suffit alors d'appliquer le résultat précédent et de multiplier par $T^{d_1+\dots+d_{e-1}}$.

Exemples 4.2 - (a) $P_{k[X]}(T) = 1 + T + T^2 + \dots = \dfrac{1}{1-T}$.

(b) Si $V = V_1 \oplus \dots \oplus V_N$ est un k-espace vectoriel gradué de dimension finie et si $\operatorname{Deg}_k(V) = (d_1, \dots, d_n)$, alors

$$P_{S(V)}(T) = \prod_{i=1}^{n} \frac{1}{1-T^{d_i}}. \ \square$$

5. Taux de croissance

5.A. Définition. Nous allons ici associer à tout module gradué de type fini sur une k-algèbre graduée un nombre entier naturel appelé son *taux de croissance*. Sa définition est justifiée par le théorème suivant :

Théorème de Hilbert-Serre. *Soit A une k-algèbre graduée. Soit M un A-module gradué de type fini. Soient $x_1, \dots, x_n$ des générateurs homogènes de degré > 0 de A. Alors*

$$P_M(T) = \frac{f(T)}{\prod_{i=1}^{n}(1-T^{d_i})},$$

où $f(T) \in \mathbb{Z}[T, T^{-1}]$.

PREUVE - Raisonnons par récurrence sur n, le résultat étant trivial lorsque $n = 0$. Supposons maintenant $n \geqslant 1$. On note $A' = A/x_n A$ et on note x'_i l'image de x_i dans A' $(1 \leqslant i \leqslant n-1)$. Alors $A' = k[x'_1, \ldots, x'_{n-1}]$. Notons $\mu : M \to M$, $m \mapsto x_n m$. On a alors une suite exacte

$$0 \longrightarrow \operatorname{Ker} \mu \longrightarrow M \xrightarrow{\mu} M \longrightarrow \operatorname{Coker} \mu \longrightarrow 0.$$

L'application linéire μ est de degré d_n. Par suite, on a

$$T^{d_n} P_{\operatorname{Ker}\mu}(T) - T^{d_n} P_M(T) + P_M(T) - P_{\operatorname{Coker}\mu}(T) = 0.$$

De plus, $\operatorname{Ker} \mu$ et $\operatorname{Coker} \mu$ sont des A'-modules de type fini. L'hypothèse de récurrence s'applique donc à eux. Il existe deux polynômes f_1 et f_2 dans $\mathbb{Z}[T, T^{-1}]$ tels que

$$P_{\operatorname{Ker}\mu}(T) = \frac{f_1(T)}{\prod_{i=1}^{n-1}(1 - T^{d_i})} \quad \text{et} \quad P_{\operatorname{Coker}\mu}(T) = \frac{f_2(T)}{\prod_{i=1}^{n-1}(1 - T^{d_i})}.$$

Donc

$$P_M(T) = \frac{P_{\operatorname{Coker}\mu}(T) - T^{d_n} P_{\operatorname{Ker}\mu}(T)}{\prod_{i=1}^{n}(1 - T^{d_i})}. \blacksquare$$

Le théorème de Hilbert-Serre donne un sens à la définition suivante : si A est une k-algèbre graduée et si M est un A-module gradué de type fini, on appelle *taux de croissance* de M, et on note $\delta(M)$, l'ordre de $T = 1$ comme pôle de $P_M(T)$.

REMARQUE - On peut montrer (voir partie **??**) que $\delta(M)$ est la dimension de Krull de M telle qu'elle est définie algébriquement. Si A est intègre, alors $\delta(A)$ est le *degré de transcendance* de du corps des fractions de A. □

Lemme technique. *Soit* $f(T) \in \mathbb{Z}[T, T^{-1}]$ *et soit* $(a_r)_{r \geqslant r_0}$ *(avec* $r_0 \in \mathbb{Z}$*) une suite d'entiers positifs ou nuls. Supposons que*

$$P(T) = \frac{f(T)}{\prod_{i=1}^{n}(1 - T^{d_i})} = \sum_{r \geqslant r_0} a_r T^r,$$

avec $d_i \geqslant 1$*. Notons* δ *l'ordre de* $q = 1$ *comme pôle de* $P(T)$*. Alors :*

(a) *Il existe* $C > 0$ *tel que* $a_r \leqslant C r^{\delta - 1}$ *pour tout* $r \geqslant r_0$*.*
(b) *Il n'existe pas de* $D > 0$ *tel que* $a_r \leqslant D r^{\delta - 2}$ *pour tout* $r \geqslant r_0$*.*

PREUVE - Quitte à multiplier par T^{r_0}, on peut supposer que $r_0 = 0$. Posons

$$g(T) = \prod_{i=1}^{n}(1 + T + T^2 + \cdots + T^{d_i - 1}) = \sum_{j=0}^{d} \alpha_j T^j,$$

où $d = d_1 + d_2 + \cdots + d_n - n$ et $\alpha_j \in \mathbb{N}^*$. On a

$$P(T)g(T) = \frac{f(T)g(T)}{(1-T)^n} = \sum_{r \geqslant 0} b_r T^r,$$

avec $b_r = \sum_{j=0}^{d} \alpha_j a_{m-j} \geqslant 0$. Cela montre que, si le résultat est vrai pour $P(T)g(T)$, alors il est vrai pour $P(T)$. Cela signifie que l'on peut supposer que $d_1 = d_2 = \cdots = d_n = 1$. On peut même

supposer, quitte à simplifier la fraction rationnelle $P(T)$, que $n = \delta$. On écrit $f(T) = \sum_{j=0}^{e} \beta_j T^j$, avec $\beta_j \in \mathbb{Z}$ et $\beta_0 + \beta_1 + \cdots + \beta_e \neq 0$. On a

$$\frac{1}{(1-T)^n} = \sum_{r \geqslant 0} \left(\begin{array}{c} r+n-1 \\ n-1 \end{array} \right) T^r.$$

Donc

$$a_r = \sum_{j=0}^{e} \beta_j \left(\begin{array}{c} r-j+n-1 \\ n-1 \end{array} \right).$$

Le coefficient de r^{n-1} dans a_r est $\beta_0 + \beta_1 + \cdots + \beta_e \neq 0$. D'où le résultat. ■

EXEMPLE 5.1 - Si V est un k-espace vectoriel gradué de dimension finie, alors $\delta(S(V)) = \dim V$. □

5.B. Propriétés. Commençons par une première liste de propriétés du taux de croissance.

Proposition 5.2. *Avec les notations ci-dessus, on a :*

(a) *Si $M \subset N$, alors $\delta(M) \leqslant \delta(N)$ et $\delta(N/M) \leqslant \delta(N)$.*
(b) *Si $A \subset B$ et B est un A-module de type fini, alors $\delta(A) = \delta(B)$.*
(c) *$\delta(M) = 0$ si et seulement si $\dim_k M < \infty$.*
(d) *Si $a \in A_+$ est homogène, alors $\delta(M/aM) \geqslant \delta(M) - 1$.*
(e) *Si $a \in A_+$ est homogène et ne divise pas 0 dans M, alors $\delta(M/aM) = \delta(M) - 1$.*
(f) *Si $a \in A_+$ est homogène et est tel que $a^e \in \mathrm{Ann}_A(M)$ (pour un $e \geqslant 1$), alors $\delta(M/aM) = \delta(M)$.*

PREUVE - (a) découle facilement du lemme technique. Pour (b), remarquons que $\delta(A) \leqslant \delta(B)$ d'après (a). D'autre part, il existe une famille finie $(b_i)_{1 \leqslant i \leqslant n}$ d'éléments homogènes de B telle que $B = \sum_{i=1}^{n} Ab_i$. On a donc un morphisme surjectif de A-modules gradués de type fini $\oplus_{i=1}^{n} A[-\deg b_i] \to B$. Donc, d'après (a), $\delta(B) \leqslant \delta(\oplus_{i=1}^{n} A[-\deg b_i])$. Mais, d'après le lemme technique, $\delta(\oplus_{i=1}^{n} A[-\deg b_i]) = \delta(A)$.

(c) Il est clair que si $\dim_k M \leqslant \infty$, alors $\delta(M) = 0$. Réciproquement, supposons que $\delta(M) = 0$. Alors, d'après le lemme technique, on a $\lim_{r \to +\infty} \dim M_r = 0$. Donc $\dim_k M < \infty$.

(d) Notons $\mu : M \to M$, $a \mapsto aM$. On a $M/aM = \mathrm{Coker}\, \mu$. Notons d le degré de a. D'après la preuve du théorème de Hilbert-Serre, on a

$$P_{\mathrm{Coker}\, \mu}(T) = (1 - T^d) P_M(T) + T^d P_{\mathrm{Ker}\, \mu}(T).$$

Donc $\delta(M/aM) = \delta(\mathrm{Coker}\, \mu) \geqslant \delta(M) - 1$.

(e) Si a ne divise pas 0, alors, dans la preuve ci-dessus, on a $\mathrm{Ker}\, \mu = 0$. Donc $P_{\mathrm{Coker}\, \mu}(T) = (1 - T^d) P_M(T)$ et donc $\delta(M/aM) = \delta(M) - 1$.

(f) Quitte à raisonner par récurrence sur e, on peut supposer que $a^2 = 0$. Avec les notations de la preuve de (d), on a une suite exacte

$$0 \longrightarrow \mathrm{Ker}\, \mu \longrightarrow M \longrightarrow \mathrm{Im}\, \mu \longrightarrow 0.$$

De plus, $\mathrm{Im}\, \mu \subset \mathrm{Ker}\, \mu$ car $a^2 = 0$. Notons c, c' et c'' les nombres rationnels positifs ou nuls tels que

$$P_M(T) = \frac{c}{(1-T)^\delta} + ...,$$

$$P_{\operatorname{Ker}\mu/\operatorname{Im}\mu}(T) = \frac{c'}{(1-T)^\delta} + ...,$$

et

$$P_{\operatorname{Im}\mu}(T) = \frac{c''}{(1-T)^\delta} + ...,$$

où $\delta = \delta(M)$. Alors

$$T^d P_{\operatorname{Ker}\mu}(T) - T^d P_M(T) + P_{\operatorname{Im}\mu}(T) = 0.$$

Par suite,

$$T^d P_{\operatorname{Ker}\mu/\operatorname{Im}\mu}(T) + (1+T^d) P_{\operatorname{Im}\mu}(T) = T^d P_M(T).$$

Donc $c = 2c' + c''$, ce qui montre que c' ou c'' est strictement positif. Donc $c - c' > 0$, ce qui montre que $\delta(M/\operatorname{Im}\mu) = \delta = \delta(M)$. ■

Corollaire 5.3. *Soit A une k-algèbre graduée et soient $x_1,\ldots, x_n$ des éléments de A_+ homogènes tels que $A = k[x_1,\ldots,x_n]$. Alors les assertions suivantes sont équivalentes :*

(1) *$x_1,\ldots, x_n$ sont algébriquement indépendants.*
(2) *$\delta(A) = n$.*

Preuve - (1) ⇒ (2) résulte de l'exemple 5.1. Réciproquement, supposons que $x_1,\ldots, x_n$ ne soient pas algébriquement indépendants. Soit $B = A[X_1,\ldots,X_n]$ où on décrète que $\deg X_i = \deg x_i$. Notons $\pi : B \to A$ le morphisme surjectif d'algèbres graduées tel que $\pi(X_i) = x_i$. Puisque $x_1, \ldots, x_n$ ne sont pas algébriquement indépendants, il existe un polynôme non nul $F \in B$, homogène, tel que $\pi(F) = 0$. On a donc un morphisme surjectif $B/FB \to A$, ce qui montre que $\delta(A) \leqslant \delta(B/FB)$. Mais, puisque B est intègre, F n'est pas un diviseur de 0 dans B. Donc, d'après la proposition 5.2 (e), on a $\delta(B/FB) = \delta(B) - 1 = n - 1$. ■

Exemple 5.4 - Soit V un k-espace vectoriel de dimension finie et soit G un sous-groupe fini de $\mathbf{GL}_k(V)$. Alors $\delta(S(V)^G) = \dim V$. En effet, cela résulte de l'exemple 5.1, du théorème 0 (f) et de la proposition 5.2 (b). □

Corollaire 5.5. *On a $\delta(A_{\text{réd}}) = \delta(A)$.*

Corollaire 5.6. *Les assertions suivantes sont équivalentes :*

(1) *$\delta(A) = 0$;*
(2) *$\dim_k A < \infty$;*
(3) *$\operatorname{Max}(A) = \{A_+\}$;*
(4) *$\operatorname{Spec}(A) = \{A_+\}$.*

Preuve - L'équivalence entre (1) et (2) découle de la Proposition 5.2 (c). Si $\dim_k A < \infty$, alors tout élément de A_+ est nilpotent. Donc (2) ⇒ (4). Il est clair que (4) ⇒ (3). Il ne nous reste qu'à montrer que (3) ⇒ (1). D'après le corollaire 5.5, on a $\delta(A_{\text{réd}}) = \delta(A)$. Donc on peut supposer que A est réduit. Mais alors $\bar{k} \otimes_k A$ s'identifie à l'algèbre de fonctions sur $\operatorname{Max}(\bar{k} \otimes A)$. Or, puisque $\operatorname{Max}(A)$ est fini, $\operatorname{Max}(\bar{k} \otimes A)$ est fini. Donc $\dim_{\bar{k}} \bar{k} \otimes_k A < \infty$. ■

Corollaire 5.7. *Si $\mathfrak{p}$ est un idéal premier homogène de A distinct de A_+, alors $\delta(A/\mathfrak{p}) \geqslant 1$.*

5.C. Caractérisation des k-algèbres régulières. Le théorème suivant fournit une caractérisation des k-algèbres régulières en termes de leur catégorie de modules.

Théorème 5.8. *Les assertions suivantes sont équivalentes :*

(1) *A est régulière ;*

(2) $\delta(A) = \dim_k V$;
(3) *Il existe une résolution libre de k de longueur inférieure ou égale à $\delta(A)$.*

PREUVE - L'équivalence entre (1) et (2) découle du corollaire 5.3. D'après la proposition 3.12, on a que (1) $\Rightarrow$ (2). L'implication (2) $\Rightarrow$ (1) découle du théorème 3.15. ■

Corollaire 5.9. *Soit S une k-algèbre graduée régulière et soit R une sous-k-algèbre graduée. On suppose que S est un R-module libre de type fini. Alors R est régulière.*

PREUVE - Remarquons pour commencer que $\delta(S) = \delta(R)$ d'après la proposition 5.2 (b). Si S est un R-module libre, alors $\mathcal{K}(S)$ est une résolution libre du R-module k. Donc, le R-module k admet une résolution libre de longueur $\delta(S) = \delta(R)$. Donc R est régulière en vertu du théorème 5.8. ■

6. Indépendance algébrique

Nous allons maintenant donner plusieurs moyens de montrer qu'une famille de polynômes polynômes est algébriquement indépendante. La démonstration du théorème suivant utilise le Nullstellensatz.

Théorème 6.1. *Soient $P_1,\dots, P_n$ des polynômes homogènes appartenant à $S = k[X_1,\dots,X_n]$, avec $\deg X_i = d_i$. Notons R la sous-k-algèbre (graduée) de $k[X_1,\dots,X_n]$ engendrée par $P_1, \dots, P_n$. Alors les assertions suivantes sont équivalentes :*

(1) *S est un R-module de type fini ;*
(2) *$\dim_k S/R_+S < \infty$;*
(3) *$(0,\dots,0) \in \bar{k}^n$ est l'unique solution du sytème d'équations $P_1(x) = \cdots = P_n(x) = 0$ avec $x \in \bar{k}^n$.*

Si ces conditions sont vérifiées, alors $P_1, \dots, P_n$ sont algébriquement indépendants.

PREUVE - L'équivalence entre (1) et (2) découle du corollaire 2.9 (a). Pour montrer l'équivalence entre (2) et (3), nous pouvons supposer que k est algébriquement clos. Dans ce cas, cela résulte facilement du Nullstellensatz de Hilbert en remarquant que $\dim_k S/R_+S < \infty$ si et seulement si tous les éléments de S_+/R_+S sont nilpotents.

Supposons maintenant les conditions (1), (2) et (3) satisfaites. Puisque S est un R-module de type fini, on a $\delta(S) = \delta(R)$ d'après la proposition 5.2 (b). Donc, d'après le corollaire 5.3, $P_1,\dots, P_n$ sont algébriquement indépendants. ■

EXEMPLE 6.2 - Soit $\sigma_1,\dots, \sigma_n$ les polynômes symétriques élémentaires dans $k[X_1,\dots,X_n]$. Soit $x = (x_1,\dots,x_n) \in \bar{k}^n$ tel que $\sigma_1(x) = \cdots = \sigma_n(x) = 0$. Alors

$$(T - x_1)(T - x_2)\dots(T - x_n) = T^n,$$

ce qui montre que $x = (0,\dots,0)$. Donc, d'après le théorème 6.1, $\sigma_1, \dots, \sigma_n$ sont algébriquement indépendants. □

Théorème 6.3. *Soient $P_1,\dots, P_n$ des polynômes homogènes appartenant à $S = k[X_1,\dots,X_n]$, avec $\deg X_i = d_i$. Posons $J = \left(\dfrac{\partial P_i}{\partial X_j}\right)_{1 \leqslant i,j \leqslant n}$.*

Si $\det J \neq 0$, alors $P_1,\dots, P_n$ sont algébriquement indépendants. Si k est de caractéristique 0 et si $P_1,\dots, P_n$ sont algébriquement indépendants, alors $\det J \neq 0$.

PREUVE - On peut supposer, et nous le ferons, que k est algébriquement clos. Notons p la caractéristique de k.

Supposons que $P_1,\dots,\ P_n$ ne sont pas algébriquement indépendants. Il existe un polynôme $F \in k[T_1,\dots,T_n]$, non nul, de degré minimal, tel que $F(P_1,\dots,P_n)=0$. Notons D la matrice ligne $\Big(\dfrac{\partial F}{\partial T_1},\dfrac{\partial F}{\partial T_2},\dots,\dfrac{\partial F}{\partial T_n}\Big)$. Alors $D(P_1,\dots,P_r)J=0$. Si $D(P_1,\dots,P_n)=0$ cela signifie, par minimalité du degré polynôme F, que $\dfrac{\partial F}{\partial T_i}=0$ pour tout i. C'est impossible si $p=0$. Si $p>0$, alors il existe $G\in k[T_1,\dots,T_n]$ tel que $F=G^p$, ce qui est encore impossible par minimalité du degré de F. Donc $D(P_1,\dots,P_n)\neq 0$ et donc $\det J=0$.

Réciproquement, supposons que $p=0$ et que $P_1,\dots,\ P_n$ sont algébriquement indépendants. Alors, pour tout $i\in\{1,2,\dots,n\}$, il existe un polynôme $F_i\in k[T_0,T_1,\dots,T_n]$ de degré minimal tel que $F_i(X_i,P_1,\dots,P_n)=0$. Soit $M=\Big(\dfrac{\partial F_i}{\partial T_j}(X_i,P_1,\dots,P_n)\Big)_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant n+1}}$. Alors

$$MJ=-\operatorname{diag}\Big(\frac{\partial F_i}{\partial T_0}(X_i,P_1,\dots,P_n)\Big)_{1\leqslant i\leqslant n}.$$

Mais, puisque $p=0$, on a $\dfrac{\partial F_i}{\partial T_0}\neq 0$ donc $\dfrac{\partial F_i}{\partial T_0}(X_i,P_1,\dots,P_n)\neq 0$ par minimalité du degré de F_i. Donc $\det J\neq 0$. ■

Exercices de la partie III

Exercice III.1. Calculer la série de Poincaré de $k[X,Y]/(XY)$.

Exercice III.2. On suppose k de caractéristique différente de 2. Soit $\mathfrak{A}_n\subset\mathfrak{S}_n$ le groupe alterné de degré n. On note $\varepsilon:\mathfrak{S}_n\to k^\times$ le morphisme signature. Notons que $\mathfrak{A}_n=\operatorname{Ker}\varepsilon$.

Soit $A=k[X_1,\dots,X_n]$. On fait agir $\mathfrak{S}_n$ par permutations des indéterminées. Posons

$$\Delta=\prod_{1\leqslant i<j\leqslant n}(X_i-X_j).$$

(a) Montrer que, pour tout $\sigma\in\mathfrak{S}_n$, on a ${}^\sigma\Delta=\varepsilon(\sigma)\Delta$.
(b) Montrer que, si $P\in k[X_1,\dots,X_n]$ vérifie ${}^\sigma P=\varepsilon(\sigma)P$ pour tout $\sigma\in\mathfrak{S}_n$, alors Δ divise P.
(c) Montrer que $k[X_1,\dots,X_n]^{\mathfrak{A}_n}=k[\sigma_1,\dots,\sigma_n,\Delta]$.
(d) Montrer que $\Delta^2\in k[X_1,\dots,X_n]^{\mathfrak{S}_n}$. Notons P ce polynôme symétrique.
(e) Montrer que $k[X_1,\dots,X_n]^{\mathfrak{A}_n}\simeq k[\sigma_1,\dots,\sigma_n][T]/(T^2-P)$.
(f) Déterminer la série de Poincaré de $k[X_1,\dots,X_n]^{\mathfrak{A}_n}$.

Exercice III.3 (suite de l'exercice I.11). Reprenons les notations de l'exercice I.11. Notons V' le sous-espace vectoriel de V engendré par $X_1,\ \dots,\ X_{n-1}$. On note $\varphi:S(V)\to S(V')$ le morphisme d'agèbres graduées tel que $X_i\mapsto X_i$ si $i\leqslant n-1$ et $X_n\mapsto 0$.

Notons T' (respectivement $Y'_1,\ \dots,\ Y'_{n-2}$) les éléments de $S(V')$ définis comme T, $Y_1,\ \dots,\ Y_{n-1}$ mais mais en remplaçant V par V'.

(a) Montrer que $\pi(T)=0$, $\pi(Y_1)=T'^{q(q-1)}$ et $\pi(Y_i)=Y'^q_{i-1}$ si $2\leqslant i\leqslant n-1$.

(b) Soit $\bar{k}$ une clôture algébrique de k et soit $x = (x_1, \ldots, x_n) \in \bar{k}^n$ tel que $T(x) = Y_1(x) = \cdots = Y_{n-1}(x) = 0$. Montrer que $x = 0$.
(c) En déduire que T, Y_1, …, Y_{n-1} sont algébriquement indépendants.
(d) Montrer que $(\deg T)(\deg Y_1)\ldots(\deg Y_{n-1}) = |G_1|$ et $(\deg T^{q-1})(\deg Y_1)\ldots(\deg Y_{n-1}) = |G|$.

Partie IV. Récolte

Dans cette partie, nous supposerons que k est *de caractéristique nulle*. Nous fixons un k-espace vectoriel de dimension finie V (que nous verrrons comme un k-espace vectoriel gradué concentré en degré 1). Posons $n = \dim V$. Nous nous fixons aussi un sous-groupe fini G de $\mathbf{GL}_k(V)$. Pour finir, soit $S = S(V)$ et $R = S(V)^G = S^G$.

7. Formule de Molien

La série de Poincaré de l'algèbre $S(V)^G$ peut être calculée très facilement en utilisant les polynômes caractéristiques des éléments de G :

Formule de Molien. *Avec les hypothèses ci-dessus, on a*

$$P_R(T) = \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\det(1 - T\sigma)}.$$

Preuve - On a $R = e_G S$. Par suite,

$$\begin{aligned} P_R(T) &= \sum_{r \geqslant 0} \dim(e_G S^r(V))\ T^r \\ &= \sum_{r \geqslant 0} \mathrm{Tr}(e_G, S^r(V))\ T^r \\ &= \frac{1}{|G|} \sum_{\sigma \in G} \Big(\sum_{r \geqslant 0} \mathrm{Tr}(\sigma, S^r(V))\ T^r \Big) \end{aligned}$$

Ici, la deuxième égalité découle du fait que k est de caractéristique nulle et que e_G est un projecteur. Pour montrer la formule de Molien, il suffit de montrer que, pour tout $\sigma \in \mathbf{GL}_k(V)$, on a

$$(*) \qquad \sum_{r \geqslant 0} \mathrm{Tr}(\sigma, S^r(V))\ T^r = \frac{1}{\det(1 - T\sigma)}.$$

Pour cela, on peut supposer que k est algébriquement clos. Soit $(e_1, \ldots, e_n)$ une base de V dans laquelle σ est représenté par une matrice triangulaire supérieure. Soient $(\lambda_1, \ldots, \lambda_n)$ les termes diagonaux de σ. Alors, en ordonnant les monômes de degré r en $e_1, \ldots, e_n$ lexicographiquement, l'action de σ sur $S^r(V)$ est représenté par une matrice triangulaire supérieure sont les termes

diagonaux sont $\lambda_1^{i_1}\dots\lambda_n^{i_n}$ avec $i_1+\dots+i_n=r$. Par suite,

$$\begin{aligned}\sum_{r\geqslant 0}\mathrm{Tr}(\sigma,S^r(V))\,T^r &= \sum_{r\geqslant 0}\Big(\sum_{i_1+\dots+i_n=r}\lambda_1^{i_1}\dots\lambda_n^{i_n}T^r\Big)\\ &= \Big(\sum_{i_1=0}^{\infty}\lambda_1^{i_1}T^{i_1}\Big)\dots\Big(\sum_{i_n=0}^{\infty}\lambda_n^{i_n}T^{i_n}\Big)\\ &= \Big(\frac{1}{1-\lambda_1 T}\Big)\dots\Big(\frac{1}{1-\lambda_n T}\Big)\\ &= \frac{1}{\det(1-T\sigma)}.\ \blacksquare\end{aligned}$$

Exemple 7.1 - Supposons que $\dim V=2$ et que $G=\{\mathrm{Id}_V,-\mathrm{Id}_V\}$. On a vu dans l'exercice I.2 que $R\simeq k[U,V,W]/(V^2-UW)$, avec $\deg U=\deg V=\deg W=2$. Par suite,

$$(*)\qquad P_R(T)=(1-T^4)P_{k[U,V,W]}(T)=\frac{1+T^2}{(1-T^2)^2}.$$

On peut retrouver ce résultat par la formule de Molien. En effet, celle-ci nous dit que

$$P_R(T)=\frac{1}{2}\Big(\frac{1}{(1-T)^2}+\frac{1}{(1+T)^2}\Big),$$

ce qui confirme $(*)$. □

Exemple 7.2 - Soit $V=k^n$, soit $(X_1,\dots,X_n)$ la base canonique de V et supposons que $G\simeq\mathfrak{S}_n$ agisse que V par permutation des vecteurs de la base canonique : ${}^{\sigma}X_i=X_{\sigma(i)}$. Alors il est bien connu que $R=k[X_1,\dots,X_n]^{\mathfrak{S}_n}=k[\Sigma_1,\dots,\Sigma_n]$ où les Σ_i sont les polynômes symétriques élémentaires. Alors $P_R(T)=\prod_{i=1}^n(1/(1-T^i))$. La formule de Molien nous donne alors l'identité remarquable suivante :

$$\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\frac{1}{\det(1-T\sigma)}=\prod_{i=1}^n\frac{1}{1-T^i}.$$

Si $\sigma\in\mathfrak{S}_n$, et si $\lambda=(\lambda_1,\lambda_2,\dots,\lambda_s)$ est la suite des longueurs des cycles de σ (notons que $\lambda_1+\dots+\lambda_s=n$), alors $\det(1-T\sigma)=(1-T^{\lambda_1})(1-T^{\lambda_2})\dots(1-T^{\lambda_s})$. □

Exemple 7.3 - Si χ est un caractère irréductible de G et si k est algébriquement clos, nous noterons, pour $r\geqslant 0$, S^r_χ la somme des composantes isotypiques de S^r associées au caractère χ. On pose aussi $S_\chi=\oplus_{r\geqslant 0}S^r_\chi$. C'est un sous-$R$-module gradué de S (de type fini car R est noethérienne). De plus, si on note

$$e_\chi=\frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g\in k[G]$$

l'idempotent central associé à χ, alors $S_\chi=e_\chi S$. En particulier, il résulte de l'égalité $(*)$ apparaissant dans la preuve de la formule de Molien que

$$P_{S_\chi}(T)=\frac{\chi(1)}{|G|}\sum_{\sigma\in G}\frac{\chi(g^{-1})}{\det(1-T\sigma)}.$$

En particulier, $\delta(S_\chi)=\dim V$. □

Notons $\mu_{|G|}(\bar{k})$ le groupe des racines de l'unités dans un clôture algébrique $\bar{k}$ de k. On décompose la série de Molien en élément simple, le dénominateur étant forcément un produit de polynômes cyclotomiques $\Phi_j(T)$ avec j divisant $|G|$ (voir formule de Molien) :

$$P_R(T) = \sum_{\zeta \in \mu_{|G|}(\bar{k})} \Big(\sum_{r=1}^{n_\zeta} \frac{c_{r,\zeta}(G)}{(\zeta - T)^r} \Big),$$

où n_ζ est tel que $c_{\zeta,n_\zeta}(G) \neq 0$.

Proposition 7.4. *Avec les notations ci-dessus, on a :*

(a) $n_\zeta = \mathrm{Max}\{\dim \mathrm{Ker}(\sigma - \zeta \,\mathrm{Id}_V) \mid \sigma \in G\}$.
(b) $n_1 = n$.
(c) $c_{n,1}(G) = \dfrac{1}{|G|}$.
(d) $c_{n-1,1}(G) = \dfrac{|\mathrm{Réf}(G)|}{2|G|}$.

Preuve - (a) découle de la formule de Molien. (b) découle de (a). Écrivons, grâce à la formule de Molien,

$$P_R(T) = \frac{1}{|G|}\Big(\frac{1}{(1-T)^n} + \sum_{\sigma \in \mathrm{Réf}(G)} \frac{1}{(1-T)^{n-1}(1 - T\det\sigma)} + \sum_{\substack{\sigma \in G \\ \sigma \neq 1 \text{ et } \sigma \notin \mathrm{Réf}(G)}} \frac{1}{\det(1 - T\sigma)} \Big).$$

On en déduit alors que $c_{n,1}(G) = \dfrac{1}{|G|}$ et

$$c_{n-1,1}(G) = \sum_{\sigma \in \mathrm{Réf}(G)} \frac{1}{1 - \det\sigma}.$$

Or, si $\alpha \in \bar{k}^\times$, on a $\dfrac{1}{1-\alpha} + \dfrac{1}{1-\alpha^{-1}} = 1$, donc $c_{n-1,1}(G) = \dfrac{\mathrm{Réf}(G)}{2|G|}$. ■

Corollaire 7.5. *Supposons que R soit une algèbre de polynômes. On note $(d_1, \ldots, d_{n'})$ la suite des degrés de R. Alors*

(a) $n' = n$.
(b) $|G| = d_1 \ldots d_n$.
(c) $|\mathrm{Réf}(G)| = d_1 + \cdots + d_n - n$.

Preuve - Puisque R est une algèbre de polynômes, on a $n' = \delta(R)$. Mais, $\delta(R) = \delta(S) = n$. D'où (a). D'autre part, on a

$$P_R(T) = \frac{1}{(1-T)^n}\Big(\prod_{i=1}^{n} \frac{1}{1 + T + \cdots + T^{d_i - 1}} \Big).$$

Posons

$$g(T) = \prod_{i=1}^{n} \frac{1}{1 + T + \cdots + T^{d_i - 1}}.$$

On a $c_{n,1}(G) = g(1) = \dfrac{1}{d_1 \ldots d_n}$. D'où (b) d'après la proposition 7.4 (c).

D'autre part, on a $c_{n-1,1}(G) = -g'(1)$. Or,

$$-\frac{g'(T)}{g(T)} = \sum_{i=1}^{n} \frac{1 + 2T + \cdots + (d_i - 1)T^{d_i - 2}}{1 + T + \cdots + T^{d_i - 1}}.$$

Par suite,

$$|G| g'(1) = \sum_{i=1}^{n} \frac{d_i(d_i - 1)}{2d_i}.$$

D'où (c) d'après la proposition 7.4 (d). ■

8. Le théorème de Shephard-Todd-Chevalley

Le but de cette section est de démontrer le théorème suivant :

Théorème (Shephard-Todd-Chevalley). *Supposons k de caractéristique nulle. Les assertions suivantes sont équivalentes :*

(1) *G est engendré par des pseudo-réflexions.*
(2) *S est un R-module libre.*
(3) *S est un $R[G]$-module libre (de rang 1).*
(4) *R est une algèbre régulière.*

Supposons ces conditions satisfaites et posons $\mathrm{Deg}(R) = (d_1, \ldots, d_n)$. *Alors* $|G| = d_1 \ldots d_n$ *et* $|\mathrm{Réf}(G)| = d_1 + \cdots + d_n - n$.

Preuve - Montrons dans un premier temps que (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (4). D'après le corollaire 5.9, on a que (2) $\Rightarrow$ (4).

Montrons que (1) $\Rightarrow$ (2). Pour cela, il nous suffit de montrer que $\mathrm{Tor}_R(S) = 0$ (voir le corollaire 3.3). Mais $\mathrm{Tor}_R(S)$ est naturellement un S-module gradué donc, en vertu du lemme de Nakayama gradué, il suffit de montrer que $\mathrm{Tor}_R(S)/R_+ \mathrm{Tor}_R(S) = 0$. Posons $E = \mathrm{Tor}_R(S)/R_+ \mathrm{Tor}_R(S)$. Tout d'abord, remarquons que E^G est l'image de $\mathrm{Tor}_R(S)^G$ car k est de caractéristique 0 (voir corollaire N). Mais, $\mathrm{Tor}_R(S)^G = \mathrm{Tor}_R(S^G)$ (toujours parce que k est de caractéristique 0) et $\mathrm{Tor}_R(S^G) = \mathrm{Tor}_R(R) = 0$ car R est un R-module libre (voir corollaire 3.3). On a donc montré que $E^G = 0$.

Montrons maintenant qu'une pseudo-réflexion de G agit trivialement sur E (cela impliquera que $E = E^G = 0$ car G est engendré par des pseudo-réflexions). Soit donc $\sigma \in \mathrm{Réf}(G)$. Soit $v \in V$ un générateur de $\mathrm{Im}(\sigma - \mathrm{Id}_V)$. Alors, pour tout $f \in S$, on a

$$(\#) \qquad {}^{\sigma}f - f \equiv 0 \bmod vS.$$

Posons $\mu_v : S \to S$, $x \mapsto vx$ et $\theta : S \to S$, $x \mapsto ({}^{\sigma}f - f)/v$. Alors $\sigma - 1 = \mu_v \circ \theta$ donc $\sigma - 1$ agit trivialement sur E car $v \in S_+$. D'où le résultat.

Montrons que (4) $\Rightarrow$ (1). Notons $(d_1, \ldots, d_n) = \mathrm{Deg}(R)$. Soit H le sous-groupe de G engendré par les réflexions appartenant à G. C'est un sous-groupe distingué de G. On a déjà montré que (1) $\Rightarrow$ (4). Donc $S(V)^H$ est une régulière. Notons $(e_1, \ldots, e_n) = \mathrm{Deg}(S(V)^H)$. Remarquons que $S(V)^G \subset S(V)^H$. Ceci implique que :

Fait. *Si $1 \leqslant i \leqslant n$, alors $e_i \leqslant d_i$.*

Soient $x_1, \ldots, x_n$ (respectivement $y_1, \ldots, y_n$) un système minimal de générateurs homogènes de $S(V)^G$ (respectivement $S(V)^H$) tel que $\deg x_i = d_i$ (respectivement $\deg y_i = e_i$). Fixons $i \in \{1, 2, \ldots, n\}$. Alors $(x_1, \ldots, x_i)$ ne peut pas être contenu dans $k[y_1, \ldots, y_{i-1}]$. Par conséquent, il existe $j \in \{1, 2, \ldots, i\}$ et $j' \in \{i, i+1, \ldots, n\}$ tel que, dans l'expression de x_j comme polynômes en les $y_?$, l'élément $y_{j'}$ apparaisse effectivement. Alors $e_{j'} \leqslant d_j$. Donc $e_i \leqslant e_{j'} \leqslant d_j led_i$. □

D'autre part, d'après le corollaire 7.5 (b), on a

$$|\text{Réf}(H)| = e_1 + \cdots + e_n - n \qquad \text{et } |\text{Réf}(H)| = d_1 + \cdots + d_n - n.$$

Or, par construction, on a $\text{Réf}(G) = \text{Réf}(H)$. Donc $e_i = d_i$ pour tout $1 \leqslant i \leqslant n$. Par suite, d'après le corollaire 7.5 (a), on a $|G| = |H|$. Donc $G = H$.

Remarquons que l'on a pour l'instant montré que (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (4). Il est de plus clair que (3) $\Rightarrow$ (2). Il ne reste qu'à montrer que (2) $\Rightarrow$ (3). Soit U un sous-k-espace vectoriel gradué G-stable de S tel que $R_+S \oplus U = S$. Un tel espace existe car k est de caractéristique nulle. Puisque S est libre sur R, l'application canonique $R \otimes_k U \to S$, $a \otimes_k u \mapsto ru$ est un isomorphisme de $R[G]$-modules. Il ne nous reste qu'à montrer que U est un $k[G]$-module libre de rang 1.

Notons K (respectivement L) le corps des fractions de R (respectivement S). Alors $L \simeq K \otimes_k U$ (isomorphisme de $K[G]$-modules). Mais, l'extension L de K est galoisienne de groupe G. Donc, d'après le théorème de la base normale, $L \simeq K[G]$ comme $K[G]$-modules. Il est alors facile de voir que $U \simeq k[G]$ (par exemple en utilisant la théorie des caractères).

Lorsque les conditions (1), (2), (3) ou (4) sont satisfaites, il résulte du corollaire 7.5 (b) et (c) que $|G| = d_1 \ldots d_n$ et $|\text{Réf}(G)| = d_1 + \cdots + d_n - n$. ■

9. Applications

Nous donnerons ici trois applications du théorème de Chevalley. Nous ne donnerons la démonstration que d'une seule.

9.A. Sous-groupes paraboliques. Soit $v \in V$. On note G_v le stabilisateur de v dans G.

Théorème (Steinberg). *Si G est engendré par des pseudo-réflexions et si $v \in V$, alors G_v est engendré par des pseudo-réflexions.*

Commentaires - Ce théorème, démontré initialement par Steinberg par des méthodes originales (équations différentielles !), a depuis reçu une autre preuve plus géométrique, utilisant le *théorème de pureté du lieu de ramification* et le théorème de Chevalley (voir M. Auslander, *On the purity of the branch locus*, Amer. J. of Math. **84** (1962), 116-125 ou encore N. Bourbaki, *Groupes et algèbres de Lie, Chapitre V*, exercices 7 et 8). Il est à noter que, si $k \subset \mathbb{R}$, alors ce théorème se démontre *naturellement*, sans passer par la théorie des invariants ou le théorème de pureté (voir *Groupes et algèbres de Lie, Chapitre V*, §3, théorème 2). □

9.B. Éléments réguliers. Un vecteur v de V est dit *G-régulier* si $G_v = \{1\}$. Un élément $g \in G$ est dit *régulier* s'il admet un vecteur propre G-régulier.

Théorème (Springer). *Supposons que G est engendré par des pseudo-réflexions. Soit g un élément régulier de G. Soit v un vecteur propre G-régulier de g et notons $\zeta \in \boldsymbol{\mu}_\infty(\mathbb{C})$ tel que $g(v) = \zeta v$. Alors $C_G(g)$ est un sous-groupe fini de $\mathbf{GL}_k(\text{Ker}(g - \zeta \,\text{Id}_V))$ engendré par des réflexions.*

COMMENTAIRES - D'après le théorème de Steinberg, un élément $v \in V$ est G-régulier si et seulement si il n'appartient à aucun des hyperplans de réflexion de G, c'est-à-dire qu'il n'est fixé par aucune pseudo-réflexion de G.

Notons aussi que, avec les hypothèses du théorème de Springer, l'ordre de g est égal à l'ordre de ζ car $G_v = \{1\}$. □

9.C. Quotients de groupes de réflexions. On dira que G est un groupe *d'intersection complète* si $\dim V = \mathrm{Long}(\mathrm{Deg}(R)) - \mathrm{Long}(\mathrm{Rel}(R))$.

EXEMPLE 9.1 - Si G est engendré par des pseudo-réflexions, alors G est un groupe d'intersection complète. En effet, d'après le théorème de Shephard-Todd-Chevalley, on a $\mathrm{Long}(\mathrm{Deg}(R)) = \dim V$ et $\mathrm{Long}(\mathrm{Rel}(R)) = 0$. □

EXEMPLE 9.2 - D'après un théorème de Kac-Watanabe, si G est un groupe d'intersection complète, alors G est engendré par des pseudo-réflexions et des produits de deux pseudo-réflexions. De plus, si G est un groupe d'intersection complète et ne contient pas de pseudo-réflexion, alors $G \subset \mathbf{SL}_k(V)$. □

Soit N un sous-groupe distingué de G. Alors le groupe quotient G/N agit sur l'algèbre d'invariants S^N. Notons $\bar{V}$ un supplémentaire gradué G/N-stable de $(S_+^N)^2$ dans S_+^N. Posons $\pi_N : S(\bar{V}) \to S^N$ le morphisme surjectif canonique et I_N le noyau de π_N. Remarquons que G/N agit sur $S(\bar{V})$, que π_N est G/N-équivariant et donc que I_N est G/N-stable.

Théorème (Bessis-Bonnafé-Rouquier). *Supposons que G est engendré par des réflexions. Alors les assertions suivantes sont équivalentes :*

(1) *G/N est un sous-groupe de $\mathbf{GL}_k(\bar{V})$ engendré par des pseudo-réflexions.*
(2) *N est un groupe d'intersection complète et G/N agit trivialement sur $I_N/S(\bar{V})_+ I_N$.*

PREUVE - (2) ⇒ (1) : supposons que N est d'intersection complète et que G/N agit trivialement sur $I_N/S(\bar{V})_+ I_N$. Alors l'idéal I_N de $S(\bar{V})$ peut être engendré par r éléments homogènes invariants sous G/N, où $r = \dim \bar{V} - \dim V$. En appliquant l'idempotent $e_{G/N}$, on obtient que $(I_N)^{G/N}$ est engendré par ces r éléments homogènes. Mais, $S(\bar{V})^{G/N}/(I_N)^{G/N} \simeq R$ et R est une k-algèbre régulière (d'après le théorème de Shephard-Todd-Chevalley). Donc l'algèbre $S(\bar{V})^{G/N}$ est engendré par $r + \dim V$ éléments homogènes. Or $r + \dim V = \dim \bar{V} = \delta(S(\bar{V})^{G/N})$, ce qui montre que $S(\bar{V})^{G/N}$ est régulière (voir corollaire 5.3). Donc, d'après le théorème de Shephard-Todd-Chevalley, on a que G/N est un sous-groupe de $\mathbf{GL}_k(\bar{V})$ engendré par des pseudo-réflexions.

(1) ⇒ (2) : réciproquement, supposons que G/N est un sous-groupe de $\mathbf{GL}_k(\bar{V})$ engendré par des pseudo-réflexions. Alors $S(\bar{V})$ est un $S(\bar{V})^{G/N}$-module de rang $|G/N|$ (voir le théorème de Shephard-Todd-Chevalley). Donc $S(\bar{V})/(I_N)^{G/N} S(\bar{V})$ est un $S(\bar{V})^{G/N}/(I_N)^{G/N}$-module libre de rang $|G/N|$. Mais, $S(\bar{V})^{G/N}/(I_N)^{G/N} \simeq R$. Donc $S(\bar{V})/(I_N)^{G/N} S(\bar{V})$ est un R-module libre de rang $|G/N|$.

Par ailleurs, $S \simeq R[G]$, comme $r[G]$-module. Donc $S^N \simeq R[G/N]$ comme $R[G/N]$-module. Donc $S(\bar{V})/I_N$ est un R-module libre de rang $|G/N|$. Cela implique que la surjection canonique $S(\bar{V})^{G/N}/(I_N)^{G/N} \to S(\bar{V})/I_N$ est un isomorphisme de R-modules. Donc I_N est engendré par des éléments G/N-invariants, donc G/N agit trivialement sur $I_N/S(\bar{V})_+ I_N$. Notons r la dimension de ce dernier k-espace vectoriel. Il nous reste à voir que $r = \dim \bar{V} - \dim V$. Il suffit donc de montrer le lemme suivant :

Lemme. *Soit A une k-algèbre graduée régulière et soit I un idéal homogène de A. On suppose que A/I est régulière. Alors* $\dim I/A_+I = \delta(A) - \delta(A/I)$.

PREUVE DU LEMME - Si $I = A$, alors c'est évident. Supposons donc que $I \neq A$, c'est-à-dire $I \subset A_+$. Posons $n = \delta(A)$, $m = \delta(A/I)$ et $r = \dim I/A_+I$. Il résulte de la proposition 5.2 (d) que $r \geqslant n - m$. D'autre part, $m = \dim A_+/(I + (A_+)^2)$ car A/I est régulière. De même, $n = \dim A_+/(A_+)^2$. Donc $n - m = \dim(I + (A_+)^2)/(A_+)^2$.

Soient maintenant E et F deux sous-k-espaces vectoriels gradués de A_+ tels que $A_+ = E \oplus (I + (A_+)^2)$ et $I = F \oplus (I \cap (A_+)^2)$. On a $I + (A_+)^2 = F \oplus (A_+)^2$ et donc $\dim F = n - m$. Donc, pour montrer que $n - m \geqslant r$, il nous suffit de montrer que F engendre I. Posons $J = AF \subset I$. Alors $A/J \simeq S(E \oplus F)/FS(E \oplus F)$ est régulière. Notons $\pi : A/J \to A/I$ le morphisme surjectif canonique. Alors A/J et A/I sont régulières et $\delta(A/J) = \delta(A/I)$. Supposons trouvé un élément homogène $a \in J$ tel que $a \notin I$. Alors $\delta(A/I) \leqslant \delta(A/(J + aA)) = \delta(A/J) - 1$ car A/J est intègre. C'est impossible. Donc $I = J$. ■

EXEMPLE 9.3 - Avec les notations du théorème précédent, si N est engendré par des pseudo-réflexions, alors N est d'intersection complète (voir exemple 9.1) et G/N agit trivialement sur $I_N/S(\bar{V})_+I_N = 0$... Donc, d'après le théorème précédent, G/N est un sous-groupe de $\mathbf{GL}_k(\bar{V})$ engendré par des réflexions. □

Exercices de la partie IV

Exercice IV.1. On suppose que $k = \mathbb{C}$. On note i une racine carré de -1. Soit $V = k^2$ et soit (X, Y) la base canonique de V. Soit G le sous-groupe de $\mathbf{GL}_2(k)$ engendré par

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad \text{et} \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(a) Montrer que G est fini et que $|G| = 8$ (G est le groupe des quaternions).
(b) Calculer la série de Poincaré de R par la formule de Molien.
(c) Posons $u = X^4 + Y^4$, $v = X^2Y^2$ et $w = XY(X^4 - Y^4)$. Montrer que u, v et w appartiennent à R. Montrer que $w^2 = v(u^2 - 4v^2)$.
(d) Montrer que u et v sont algébriquement indépendants (utiliser le théorème 6.1).
(e) Soit A la sous-algèbre de R engendrée par u et v. Calculer la série de Poincaré de A.
(f) Soit A' la sous-algèbre de R engendrée par u, v et w. Montrer que $A' = A \oplus Aw$. En déduire que $P_{A'}(T) = P_R(T)$.
(g) Montrer que $A' = R$. En déduire que $R \simeq k[U, V, W]/(W^2 - V(U^2 - 4V^2))$. En particulier, $\mathrm{Deg}(R) = (4, 4, 6)$ et $\mathrm{Rel}(R) = 12$.

Exercice IV.2*. Soit k un *corps de nombre*. Soit G un sous-groupe fini de $\mathbf{GL}_k(V)$ engendré par des pseudo-réflexions. Montrer qu'il existe une extension galoisienne finie k' de k telle que $\mathrm{Gal}(k'/k) \simeq G$.

Indication : Il faudra utiliser le théorème suivant dû à Hilbert. Si $P(T) \in k(X_1, \ldots, X_n)[T]$ est un polynôme irréductible (vu comme polynôme à coefficients dans $k(X_1, \ldots, X_n)$), alors il existe

(une infinité) de n-uplets $(x_1, \ldots, x_n) \in k^n$ tels que la spécialisation de P en ces n-uplets est bien définie et est un polynôme irréductible dans $k[T]$ (l'hypothèse *"k est un corps de nombre"* est cruciale pour ce théorème).

Exercice IV.3 (Bourbaki, "Groupes et algèbres de Lie", chapitre V, §5, exercice 4). Soit $H = \mathbf{GL}_3(\mathbb{F}_2)$.

(a) Montrer que H est simple, d'ordre 168, qu'il a 6 classes de conjugaison et qu'il contient 21 éléments d'ordre 2.
(b) Montrer que les degrés des caractères irréductibles de H sont 1, 3, 3, 6, 7 et 8.

Soit $\rho : H \to \mathbf{GL}_3(\mathbb{C})$ une représentation irréductible de H. Posons $V = \mathbb{C}^3$.

(c) Montrer que $-\rho(s)$ est une réflexion pour tout élément $s \in H$ d'ordre 2.
(d) Soit G le sous-groupe de $\mathbf{GL}_3(\mathbb{C})$ engendré par les $-\rho(s)$, pour $s \in H$ d'ordre 2. Montrer que $G = \rho(H) \times \{\mathrm{Id}_V, -\mathrm{Id}_V\}$.
(e) Montrer que les degrés de $S(V)^G$ sont 4, 6 et 14.

Commentaires sur l'exercice IV.3 - Soit P l'unique (à une constante multiplicative près) invariant homogène de G de degré 4. Il définit une courbe fermée $\mathcal{C}$ dans $\mathbf{P}(V^*) \simeq \mathbf{P}^2(\mathbb{C})$. Le groupe H agit fidèlement sur cette courbe. De plus, on peut montrer que cette courbe est lisse, donc de genre 3. Or, un théorème de Hurwitz nous dit que, si C est une courbe de genre g définie sur un corps de caractéristique nulle, alors son groupe d'automorphismes est d'ordre $\leqslant 84(g-1)$. Appliqué à notre cas, $|\operatorname{Aut}(\mathcal{C})| \leqslant 168$. Donc $\operatorname{Aut}(\mathcal{C}) \simeq \mathbf{GL}_3(\mathbb{F}_2)$. On a donc construit ainsi un exemple montrant que la borne peut être atteinte lorsque $g = 3$. □

Exercice IV.4. Soit G un sous-groupe de $\mathbf{GL}_2(k)$ engendré par des pseudo-réflexions et contenant $-\mathrm{Id}_V$, où $V = k^2$. Soit $N = \{\mathrm{Id}_V, -\mathrm{Id}_V\}$ et reprenons les notations du théorème de Bessis-Bonnafé-Rouquier.

(a) Montrer que $\bar{V} = S^2(V)$.
(b) Montrer que G/N est un sous-groupe de $\mathbf{GL}_k(\bar{V})$ engendré par des pseudo-réflexions si et seulement si G est engendré par des réflexions.
(c) Supposons que G est engendré par des réflexions. Montrer que, si $s \in \mathrm{Réf}(G)$, alors l'image $\bar{s}$ de s dans G/N agit comme une réflexion sur $\bar{V}$.

Partie V. Groupes de réflexions, généralités

Soit k un corps de caractéristique nulle. Nous fixons dans cette partie un k-espace vectoriel V de dimension finie. Nous noterons $n = \dim_k V$. Rappelons qu'un sous-groupe Γ de $\mathbf{GL}_k(V)$ est dit *irréductible* s'il n'existe pas de sous-espace G-stable non trivial de V. On dit que G est *absolument irréductible* si $\mathrm{Id}_{\bar{k}} \otimes_k \Gamma$ est un sous-groupe irréductible de $\mathbf{GL}_{\bar{k}}(\bar{k} \otimes_k V)$.

Nous fixons aussi dans cette partie un sous-groupe fini G de $\mathbf{GL}_k(V)$ engendré par des pseudo-réflexions. Par bus de langage, nous appellerons *suite des degrés de* G (et nous noterons $\mathrm{Deg}(G)$) la suite des degrés de l'algèbre d'invariants $S(V)^G$ (qui est régulière d'après le théorème de Shephard-Todd-Chevalley).

10. Irréductibilité

Soit $v \in V$ et $f \in V^*$. On suppose que $v \neq 0$ et $f \neq 0$. On note $s_{v,f}$ l'application linéaire $V \to V$, $x \mapsto x - f(x)v$. Alors $s_{v,f}$ est une pseudo-réflexion de V (on a $\mathrm{Ker}(s - \mathrm{Id}_V) = \mathrm{Ker}\, f$ et $\mathrm{Im}(s - \mathrm{Id}_V) = kv$). D'autre part,

$$(*) \qquad s_{v,f} \circ s_{v,f}(x) = x - f(x)(2 - f(v))v.$$

Donc $s_{v,f}$ est une réflexion si et seulement si $f(v) = 2$.

Il est clair que $s_{v,f} = s_{v',f'}$ si et seulement si il existe $\lambda \in k^\times$ tel que $v' = \lambda v$ et $f' = \lambda^{-1} f$. D'autre part, si $s \in \mathbf{GL}_k(V)$ est une pseudo-réflexion, alors il existe $v \in V$ et $f \in V^*$, tous deux non nuls, tels que $s = s_{v,f}$.

Lemme 10.1. *Soient $v \in V$ et $f \in V^*$, tous deux non nuls. Alors :*

(a) $\det s_{v,f} = 1 - f(v)$.
(b) *$s_{v,f}$ est diagonalisable si et seulement si $f(v) \neq 0$.*

Proposition 10.2. *Soit $V = V^G \oplus V_1 \oplus V_2 \oplus \cdots \oplus V_r$ une décomposition de V en somme de $k[G]$-modules irréductibles. Notons G_i la restriction de G à V_i. Alors :*

(a) *La famille $(V_1, \ldots, V_r)$ est déterminée de façon unique à l'ordre près.*
(b) *L'application canonique $G \to G_1 \times \cdots \times G_r$ est un isomorphisme.*
(c) *G_i est un sous-groupe fini de $\mathbf{GL}_k(V_i)$ engendré par des réflexions.*
(d) *G est irréductible si et seulement si $\mathrm{End}_k(V)^G = k\,\mathrm{Id}_V$. En d'autres termes, G est irréductible si et seulement si il est absolument irréductible.*
(e) *$\bar{k} \otimes_k V_i$ est un $\bar{k}[G]$-module irréductible. En d'autres termes, G_i est absolument irréductible*

Preuve - (c) est évident : en effet, la restriction d'une pseudo-réflexion de G à V_i est une pseudo-réflexion ou l'identité.

(b) L'application $G \to G_1 \times \cdots \times G_r$ est injective. Soit maintenant $s \in \mathrm{Réf}(G)$. Alors s appartient à un et un seul des G_i. On obtient ainsi une partition de $\mathrm{Réf}(G)$ en r parties disctinctes $E_1, \ldots, E_r$, où $E_i = \mathrm{Réf}(G) \cap G_i$. Il est alors clair que E_i engendre G_i, et donc que $G \to G_1 \times \cdots \times G_r$ est surjective.

(a) Les représentations irréductibles V_i de G sont deux à deux non isomorphes, d'où (a).

(d) Si $\mathrm{End}_k(V)^G = k\,\mathrm{Id}_V$, alors V est irréductible. Réciproquement, supposons V est irréductible et soit $\varphi \in \mathrm{End}_k(V)^G$. Pour tout $s \in \mathrm{Réf}(G)$, fixons un générateur v_s de $\mathrm{Im}(s-\mathrm{Id}_V)$. Fixons $s \in \mathrm{Réf}(G)$. Alors $\varphi(v_s)$ est colinéaire à v_s car φ commute avec s. Soit $\lambda \in k$ tel que $s(v_s) = \lambda v_s$. Posons $V' = \ker(\varphi - \lambda\,\mathrm{Id}_V)$. Alors V' est un sous-$k[G]$-module de V contenant v_s. Donc $V' = V$, ce qui montre que $\varphi = \lambda\,\mathrm{Id}_V$.

(e) résulte immédiatement de (d). ■

La proposition 10.2 montre que, pour classifier les groupes de réflexions, il suffit de classifier ceux qui sont irréductibles.

Corollaire 10.3. *Si G est irréductible et si $\mathrm{Deg}(G) = (d_1, d_2, \ldots, d_n)$, alors $Z(G)$ est cyclique d'ordre $\mathrm{pgcd}(d_1, d_2, \ldots, d_n)$.*

Preuve - Si G est irréductible, alors G est absolument irréductible d'après la proposition 10.2 (d). Par conséquent, les seuls endomorphismes de V qui commutent avec l'action de G sont les homothéties. Donc $Z(G)$ consite en les homothéties. En particulier, $Z(G)$ est isomorphe à un sous-groupe fini de $k^\times$, donc il est cyclique. Notons d son ordre. Alors

$$S(V)^{Z(G)} = \bigoplus_{r \geqslant 0} S^{dr}(V).$$

Cela montre que d divise $\delta = \mathrm{pgcd}(d_1, d_2, \ldots, d_n)$.

Soit maintenant ζ une racine primitive δ-ième de l'unité. Posons $\tilde{G} =< G, \zeta\,\mathrm{Id}_V >$. Alors $\tilde{G}$ est un sous-groupe fini de $\mathbf{GL}_k(V)$ contenant G et $S(V)^{\tilde{G}} = S(V)^G$. Cela montre en particulier que, si L désigne le corps des fractions de $S(V)$, alors $L^G = L^{\tilde{G}}$. Donc $|G| = |\tilde{G}|$ et donc $\zeta\,\mathrm{Id}_V \subset Z(G)$. Donc δ divise d. ■

11. Groupe des commutateurs de G

Le but de cette section est d'étudier les groupes $D(G)$ et $G/D(G)$, où $D(G)$ désigne le groupe dérivé de G, en étudiant l'action de G sur l'algèbre symétrique.

11.A. Abélianisé de G. Soit

$$\mathcal{A}_G = \{\mathrm{Ker}(s - \mathrm{Id}_V) \mid s \in \mathrm{Réf}(G)\}.$$

Si $H \in \mathcal{A}_G$, posons

$$G_H = \{\sigma \in G \mid \forall\ v \in H,\ \sigma(v) = v\}.$$

Puisque k est de caractéristique 0 et que G_H est fini, il existe un supplémentaire D_H de H qui est G_H-stable. Ce supplémentaire G_H-stable est unique car, si $H = \mathrm{Ker}(s - \mathrm{Id}_V)$ avec $s \in \mathrm{Réf}(G)$, alors $D_H = \mathrm{Im}(s-\mathrm{Id}_V)$. Fixons un générateur v_H de D_H, posons $e_H = |G_H|$ et $G_H^\# = G_H - \{1\}$. Alors $G_H^\# = G_H \cap \mathrm{Réf}(G)$, G_H est cyclique, engendré par des pseudo-réflexions : nous fixerons un générateur s_H de G_H. Remarquons que

$$\mathrm{Réf}(G) = \coprod_{H \in \mathcal{A}_G} G_H^\#.$$

En particulier, $G =< (s_H)_{H \in \mathcal{A}_G} >$.

Lemme 11.1. *Soit $H \in \mathcal{A}_G$. Alors :*

(a) *Si $H' \in \mathcal{A}_G$ vérifie $D_H = D_{H'}$, alors $H = H'$.*

(b) *Si $s \in \mathrm{Réf}(G)$ vérifie $s(H) = H$ et $H \neq \mathrm{Ker}(s - \mathrm{Id}_V)$, alors $s(v_H) = v_H$.*

PREUVE - (a) Supposons que $D_H = D_{H'}$. Notons $\Gamma =< G_H, G_{H'} >$. Alors Γ stabilise D_H. Donc il existe un supplémentaire Γ-stable X de D_H dans V (car Γ est fini et k est de caractéristique nulle). Puisque $G_H \subset \Gamma$, X est G_H-stable. Par suite, $X = H$. De même, $X = H'$. Donc $H = H'$. assertion.

(b) Posons $H' = \mathrm{Ker}(s - \mathrm{Id}_V)$. Alors s normalise G_H, donc stabilise D_H. Par suite, il existe $\lambda \in k^\times$ tel que $s(v_H) = \lambda v_H$. Si $\lambda \neq 1$, alors $v_H \in D_{H'}$ car s est une pseudo-réflexion. Donc $D_H = D_{H'}$, ce qui contredit (a). Donc $\lambda = 1$, ce qui montre (b). ■

Notons $\mathcal{A}_G/G$ l'ensemble des orbites de G dans $\mathcal{A}_G$. Si $\mathcal{C} \in \mathcal{A}_G/G$, nous posons

$$\Delta_{G,\mathcal{C}} = \prod_{H \in \mathcal{C}} v_H$$

et $e_\mathcal{C} = e_H$, où $H \in \mathcal{C}$. Si $\sigma \in G$, alors ${}^\sigma\Delta_{G,\mathcal{C}}$ est proportionnel à $\Delta_{G,\mathcal{C}}$. Nous noterons $\det_\mathcal{C} \sigma$ l'élément de $k^\times$ tel que

$${}^\sigma\Delta_{G,\mathcal{C}} = (\det_\mathcal{C} \sigma)\Delta_{G,\mathcal{C}}.$$

Lemme 11.2. *Soit $\mathcal{C} \in \mathcal{A}_G$. Alors :*

(a) $\det_\mathcal{C} : G \to k^\times$ *est un caractère linéaire de G.*
(b) *Si $H \notin \mathcal{C}$, alors* $\det_\mathcal{C} s_H = 1$.
(c) *Si $H \in \mathcal{C}$, alors* $\det_\mathcal{C} s_H = \det s_H$.
(d) *L'image de* $\det_\mathcal{C}$ *est* $\boldsymbol{\mu}_{e_\mathcal{C}}(k)$.

PREUVE - (a) est évident. Montrons maintenant (b), (c) et (d). Tout d'abord, $s_H(v_H) = (\det s_H)v_H$. Soit maintenant $H \neq H'$. Notons e le cardinal de l'orbite de H' sous l'action de s_H. Posons $\delta = v_{H'} v_{s_H(H')} \dots v_{s_H^{e-1}(H')}$. On a $s_H^e(H') = H'$ et s_H^e est une pseudo-réflexion d'hyperplan H ou l'identité. Donc, d'après le lemme 11.1 (b), on a $s_H^e(v_H) = v_H$. Pour $0 \leqslant i \leqslant e-1$, notons λ_i l'élément de $k^\times$ tel que ${}^{s_H}v_{s_H^i(H')} = \lambda_i v_{s_H^{i+1}(H')}$. On a alors ${}^{s_H}\delta = \lambda_0\lambda_1 \dots \lambda_{e-1}\delta$ et, puisque $s_H^e(v_H) = v_H$, on a $\lambda_0\lambda_1 \dots \lambda_{e-1} = 1$. Donc ${}^{s_H}\delta = \delta$. Maintenant, (b), (c) et (d) découlent de cette remarque (il faut décomposer les éléments de $\mathcal{C}$ en orbites sous l'action de G_H). ■

Théorème 11.3. *Si $\sigma \in G$, alors*

$$\det \sigma = \prod_{\mathcal{C} \in \mathcal{A}_G/G} \det_\mathcal{C} \sigma.$$

De plus, l'application

$$\prod_{\mathcal{C} \in \mathcal{A}_G/G} \det_\mathcal{C} : G \longrightarrow \prod_{\mathcal{C} \in \mathcal{A}_G/G} \boldsymbol{\mu}_{e_\mathcal{C}}(k)$$

est surjective et son noyau est le groupe dérivé de G.

PREUVE - Montrons la première assertion. Il suffit de la vérifier lorsque $\sigma \in \mathrm{Réf}(G)$. Dans ce cas, cela découle immédiatement du lemme 11.2 (b) et (c).

La surjectivité de $\prod_{\mathcal{C} \in \mathcal{A}_G/G} \det_\mathcal{C}$ découle facilement du lemme 11.2, (b), (c) et (d). Notons N son noyau. Alors N contient le groupe dérivé de G, que nous notons $D(G)$. Fixons, pour tout $\mathcal{C} \in \mathcal{A}_G/G$, un hyperplan $H_\mathcal{C} \in \mathcal{C}$. Posons $s_\mathcal{C} = s_{H_\mathcal{C}}$ et notons $\bar{s}_\mathcal{C}$ la classe de $s_\mathcal{C}$ dans $G/D(G)$. Alors $G/D(G) =< (\bar{s}_\mathcal{C})_{\mathcal{C} \in \mathcal{A}_G/G} >$. Soit maintenant $\sigma \in N$. Notons $\bar{\sigma}$ sa classe dans $G/D(G)$. Écrivons $\bar{\sigma} = \prod_{\mathcal{C} \in \mathcal{A}_G/G} \bar{s}_\mathcal{C}^{d_\mathcal{C}}$ où $d_\mathcal{C} \in \mathbb{Z}$. Alors $1 = \det_\mathcal{C}(\sigma) = (\det s_\mathcal{C})^{d_\mathcal{C}}$. Par suite, $d_\mathcal{C}$ est un multiple de $e_\mathcal{C}$. Donc $\bar{\sigma} = 1$, ce qui montre que $N \subset D(G)$. ■

11.B. Invariants du groupe dérivé. Notons $G^\wedge$ le groupe $\prod_{\mathcal{C}\in\mathcal{A}_G/G} \mathbb{Z}/e_{\mathcal{C}}\mathbb{Z}$. Si $\mathbf{i}=(i_{\mathcal{C}})_{\mathcal{C}\in\mathcal{A}_G/G}$ est un élément de $G^\wedge$, on note

$$\begin{array}{rccc} \zeta_{\mathbf{i}}: & G & \longrightarrow & k^\times \\ & \sigma & \longmapsto & \displaystyle\prod_{\mathcal{C}\in\mathcal{A}_G/G} (\det_{\mathcal{C}}\sigma)^{i_{\mathcal{C}}}. \end{array}$$

Alors $\zeta_{\mathbf{i}}$ est un caractère linéaire de G. Le théorème 11.3 montre que :

Corollaire 11.4. *L'application $\mathbf{i}\mapsto\zeta_{\mathbf{i}}$ définit un isomorphisme entre $G^\wedge$ et le groupe des caractères linéaires de G (à valeurs dans k ou $\bar{k}$).*

Posons maintenant

$$\Delta_{G,\mathbf{i}} = \prod_{\mathcal{C}\in\mathcal{A}_G/G} \Delta_{G,\mathcal{C}}^{i_{\mathcal{C}}^\circ},$$

où $i_{\mathcal{C}}^\circ$ est l'unique représentant de $i_{\mathcal{C}}$ dans $\{0,1,\dots,e_{\mathcal{C}}-1\}$. Posons aussi

$$S(V)_{\mathbf{i}} = \{P\in S(V)\mid \forall\ \sigma\in G,\ {}^\sigma P=\zeta_{\mathbf{i}}(\sigma)P\}.$$

Théorème 11.5. *Si $\mathbf{i}\in G^\wedge$, alors $S(V)_{\mathbf{i}} = S(V)^G\Delta_{G,\mathbf{i}}$.*

Preuve - Tout d'abord, il découle des définitions que $S(V)^G\Delta_{G,\mathbf{i}}\subset S(V)_{\mathbf{i}}$. D'autre part, si $P\in S(V)_{\mathbf{i}}$ est divisible (dans $S(V)$) par $\Delta_{G,\mathbf{i}}$, alors $P/\Delta_{G,\mathbf{i}}\in S(V)^G$. Il nous reste donc à montrer que tout élément de $S(V)_{\mathbf{i}}$ est divisible par $\Delta_{G,\mathbf{i}}$.

Soit donc $P\in S(V)_{\mathbf{i}}$. Pour montrer le résultat, nous devons montrer que, si $H\in\mathcal{A}_G$ et si $\mathcal{C}$ désigne l'orbite de H sous G, alors $v_H^{i_{\mathcal{C}}^\circ}$ divise P. Soit donc $H\in\mathcal{A}_G$ et soit $\mathcal{C}$ l'orbite de H sous G. Alors P s'écrit de façon unique

$$P=\sum_{i=0}^{r}\alpha_i v_H^i \qquad \text{où } \alpha_i\in S(H).$$

On a, par hypothèse et d'après le lemme 11.2, ${}^{s_H}P=(\det s_H)^{i_{\mathcal{C}}^\circ}P$. Mais,

$${}^{s_H}P=\sum_{i=0}^{r}\alpha_i(\det s_H)^i v_H^i.$$

Par suite, pour tout i, on a $\alpha_i((\det s_H)^i-(\det s_H)^{i_{\mathcal{C}}^\circ})=0$. Comme $\det s_H$ est d'ordre $e_{\mathcal{C}}$, cela montre que $\alpha_i=0$ si $i\not\equiv i_{\mathcal{C}}^\circ \bmod e_{\mathcal{C}}$. D'où le résultat. ■

Corollaire 11.6. *Posons $r=|\mathcal{A}_G/G|$ et $\mathcal{A}_G/G=\{\mathcal{C}_1,\dots,\mathcal{C}_r\}$. On a*

$$S(V)^{D(G)}=S(V)^G[(\Delta_{G,\mathcal{C}})_{\mathcal{C}\in\mathcal{A}_G/G}]=S(V)^G[T_1,\dots,T_r]/<T_1^{e_{\mathcal{C}_1}}-\Delta_{G,\mathcal{C}_1}^{e_{\mathcal{C}_1}},\dots,T_r^{e_{\mathcal{C}_r}}-\Delta_{G,\mathcal{C}_r}^{e_{\mathcal{C}_r}}>.$$

11.C. Jacobien. Posons maintenant

$$\Delta_G=\prod_{\mathcal{C}\in\mathcal{A}_G/G}\Delta_{G,\mathcal{C}} \qquad\text{et}\qquad \Delta_G^*=\prod_{\mathcal{C}\in\mathcal{A}_G/G}\Delta_{G,\mathcal{C}}^{e_{\mathcal{C}}-1}.$$

Alors, pour tout $\sigma\in G$, on a

(11.7) $$ {}^\sigma\Delta_G=(\det\sigma)\Delta_G.$$

et

(11.8) $$ {}^\sigma\Delta_G^*=(\det\sigma)^{-1}\Delta_G^*.$$

Remarque - On peut montrer que $S\Delta_G^*$ est la *différente* de S par rapport à R et que $R\Delta_G\Delta_G^* \subset R$ est le *discriminant* de S par rapport à R. □

Proposition 11.9. *Soit $(X_1, \dots, X_n)$ une base de V et soient P_1, …, P_n des générateurs homogènes de $S(V)^G$. Alors*

$$\Delta_G^* = \lambda \det\Big(\frac{\partial P_i}{\partial X_j}\Big)_{1 \leqslant i,j \leqslant n},$$

pour un certain $\lambda \in k^\times$.

Preuve - Posons

$$J = \det\Big(\frac{\partial P_i}{\partial X_j}\Big)_{1 \leqslant i,j \leqslant n}.$$

Notons que

$$\deg \Delta_G^* = \sum_{H \in \mathcal{A}_G} (e_H - 1) = \sum_{H \in \mathcal{A}_G} |G_H^\#| = |\mathrm{Réf}(G)|.$$

et

$$\deg J = \sum_{i=1}^{n} (\deg P_i - 1) = |\mathrm{Réf}(G)|$$

d'après le théorème de Chevalley-Shephard-Todd. Par suite, il suffit de montrer que Δ_G^* divise J et que $J \neq 0$. Le fait que $J \neq 0$ découle du théorème 6.3.

Montrons maintenant que Δ_G^* divise J. D'après le théorème 11.5, il suffit de montrer que ${}^\sigma J = (\det \sigma)^{-1} J$ pour tout $\sigma \in G$. Pour cela, on peut supposer que k est algébriquement clos. Fixons donc $\sigma \in G$. Soit $(Y_1, \dots, Y_n)$ une base de V dans laquelle σ est diagonalisable. Posons

$$J' = \det\Big(\frac{\partial P_i}{\partial Y_j}\Big)_{1 \leqslant i,j \leqslant n}.$$

Alors $J' = \mu J$ où $\mu \in k^\times$. Il suffit donc de montrer que ${}^\sigma J' = (\det \sigma)^{-1} J'$. Or, si $\sigma(Y_j) = \lambda_j Y_j$ avec $\lambda_j \in k^\times$, alors, par inspection monôme par monôme, on obtient

$${}^\sigma\Big(\frac{\partial P_i}{\partial Y_j}\Big) = \lambda_j^{-1}\Big(\frac{\partial P_i}{\partial Y_j}\Big).$$

Donc ${}^\sigma J' = (\lambda_1 \dots \lambda_n)^{-1} J' = (\det \sigma)^{-1} J'$. ■

12. Représentations de Macdonald

Soit X une partie de $\mathrm{Réf}(G)$. Notons G_X le sous-groupe de G engendré par X. Alors G_X est engendré par des réflexions. On peut donc reprendre les construction précédentes. Notons E_X le sous-espace vectoriel de $S(V)$ engendré par les ${}^\sigma\Delta_{G_X}^*$. Rappelons que $\Delta_{G_X}^*$ est homogène de degré $|\mathrm{Réf}(G_X)|$. Alors E_X est un $k[G]$-module.

Théorème 12.1 (Macdonald). *E_X est un $k[G]$-module absolument irréductible.*

Preuve - Il faut montrer que $\mathrm{End}_k(E_X)^G = k\,\mathrm{Id}_V$. Soit donc $\varphi \in \mathrm{End}_k(E_X)^G$. Alors, puisque φ commute à l'action de G_X, on a, pour tout $\sigma \in G_X$,

$${}^\sigma\varphi(\Delta_{G_X}^*) = (\det \sigma)^{-1}\varphi(\Delta_{G_X}^*).$$

Donc, d'après le théorème 11.5, on obtient que $\varphi(\Delta_{G_X}^*)$ est un multiple de $\Delta_{G_X}^*$. Puisqu'ils sont de même degré, il existe $\lambda \in k^\times$ tel que $\varphi(\Delta_{G_X}^*) = \lambda\Delta_{G_X}^*$. Puisque φ commute avec l'action de G, on a, pour tout $\sigma \in G$, $\varphi({}^\sigma\Delta_{G_X}^*) = \lambda\,{}^\sigma\Delta_{G_X}^*$. Donc $\varphi = \lambda\,\mathrm{Id}_V$. ■

13. Groupes de réflexions complexes

Nous allons dans cette section décrire quelques groupes de réflexions complexes. La classification des groupes de réflexions complexes irréductible (Shephard-Todd) fait apparaître une famille infinie et 34 groupes exceptionnels. Il n'est pas possible ici d'expliquer, de démontrer, ni même d'illustrer toute cette classification. Nous nous bornerons à construire la famille infinie ainsi que quelques groupes exceptionnels en rang 2. Dans le chapitre sur les groupes de Coxeter, nous verrons quelques autres groupes exceptionnels réalisables sur le corps des réels.

13.A. Groupes abéliens. Soit Γ un groupe abélien. Alors Γ peut être vu comme un groupe engendré par des pseudo-réflexions de multiple manières. Choisissons une décomposition $\Gamma = \Gamma_1 \times \cdots \times \Gamma_n$ de Γ en produit de groupes cycliques. Posons $d_i = |\Gamma_i|$ et notons x_i un générateur de Γ_i. On suppose que $d_1 \leqslant \ldots \leqslant d_n$.

Soit $V = \mathbb{C}^n$ et notons $(X_1, \ldots, X_n)$ la base canonique de V. Soit

$$\begin{array}{rccc} \rho : & \Gamma & \longrightarrow & \mathbf{GL}_n(\mathbb{C}) \\ & x_1^{e_1} \times x_n^{e_n} & \longmapsto & \mathrm{diag}(e^{2i\pi e_1/d_1}, \ldots, e^{2i\pi e_n/d_n}). \end{array}$$

Alors ρ est un morphisme injectif et l'image de ρ est engendré par des pseudo-réflexions. De plus, $(X_1^{d_1}, \ldots, X_n^{d_n})$ est un système de générateurs homogènes de $S(V)^G$. Par conséquent, $\mathrm{Deg}(S(V)^G) = (d_1, \ldots, d_n)$.

13.B. La famille infinie. Soit n un entier naturel non nul. Notons $V = \mathbb{C}^n$ et soit $(X_1, \ldots, X_n)$ la base canonique de V. Notons $\mathcal{N}_n(\mathbb{C})$ le groupe des matrices monômiales inversibles dans $\mathbf{GL}_n(\mathbb{C})$. Soit $\gamma : \mathcal{N}_n(\mathbb{C}) \to \mathbb{C}^\times$ l'application qui, à un élément de $\mathcal{N}_n(\mathbb{C})$, associe le produit de ses coefficients non nuls. Alors γ est un morphisme de groupes. Si d est un entier naturel non nul, on note $G(d, 1, n)$ le sous-groupe (fini) de $\mathcal{N}_n(\mathbb{C})$ formé des matrices monômiales dont les coefficients non nuls appartiennent à μ_d.

Soit (d, e, n) un triplet d'entiers naturels non nuls. On pose

$$G(de, e, n) = \{\sigma \in G(de, 1, n) \mid \gamma(\sigma) \in \mu_d\}.$$

Notons $\Delta(de, e, n)$ le sous-groupe de $G(de, e, n)$ formé des matrices diagonales. Nous identifions $\mathfrak{S}_n$ au sous-groupe des matrices de permutation. On a $\mathfrak{S}_n \subset G(de, e, n)$ et $\mathfrak{S}_n = G(1, 1, n)$.

Proposition 13.1. *Soit (d, e, n) un triplet d'entiers naturels non nuls. Alors :*

(a) *$G(de, e, n) = \mathfrak{S}_n \ltimes \Delta(de, e, n)$. Donc $|G(de, e, n)| = d^n e^{n-1} n!$*
(b) *$G(de, e, n)$ est un sous-groupe fini de $\mathbf{GL}_n(\mathbb{C})$ engendré par des pseudo-réflexions.*
(c) *Si $(d, e) \neq (1, 1)$ ou $(d, e, n) \neq (1, 2, 2)$, alors $G(de, e, n)$ est irréductible.*
(d) *Le groupe $G(1, 1, n) = \mathfrak{S}_n$ agit de manière irréductible et fidèle sur l'hyperplan d'équation $x_1 + \cdots + x_n = 0$.*
(e) *$\sigma_1(X_1^{de}, \ldots, X_n^{de})$, $\sigma_2(X_1^{de}, \ldots, X_n^{de})$, $\ldots$, $\sigma_{n-1}(X_1^{de}, \ldots, X_n^{de})$, $\sigma_n(X_1^d, \ldots, X_n^d)$ forme un système minimal de générateurs homogènes de l'algèbre $S(V)^{G(de,e,n)}$. En particulier, $\mathrm{Deg}(G(de, e, n)) = (de, 2de, \ldots, (n-1)de, nd)$.*

Preuve - (a) est évident. Montrons (d). Posons

$$H = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid x_1 + \cdots + x_n = 0\}$$

et

$$D = \mathbb{C}.(1, 1, \ldots, 1).$$

Alors $\mathbb{C}^n = H \oplus D$ et H et D sont $\mathfrak{S}_n$-stables. De plus, $\mathfrak{S}_n$ agit trivialement sur D. Donc $\mathfrak{S}_n$ agisse fidèlement sur H. Montrons maintenant que H est une représentation irréductible de $\mathfrak{S}_n$. Soit $\varphi : H \to H$ une application $\mathbb{C}$-linéaire telle que $\varphi(\sigma(x)) = \sigma(\varphi(x))$ pour tous

$\sigma \in \mathfrak{S}_n$ et $x \in H$. Il nous suffit de montrer que φ est une homothétie. Notons $(e_1, \dots, e_n)$ la base canonique de $\mathbb{C}^n$. Si $1 \leqslant i < j \leqslant n$, on note τ_{ij} la transposition $(i,j) \in \mathfrak{S}_n$. Alors $\mathrm{Ker}(\tau_{ij} + \mathrm{Id}_V) = \mathbb{C}(e_i - e_j)$. Par suite, il existe λ_{ij} tel que $\varphi(e_i - e_j) = \lambda_{ij}(e_i - e_j)$. Il nous reste à montrer que $\lambda_{i,i+1} = \lambda_{i+1,i+2}$ car $(e_1 - e_2, e_2 - e_3, \dots, e_{n-1} - e_n)$ est une $\mathbb{C}$-base de H. Il suffit pour cela de calculer $\varphi(e_i - e_{i+2}) = \varphi(e_i - e_{i+1}) + \varphi(e_{i+1} - e_{i+2})$: on trouve alors $\lambda_{i,i+1} = \lambda_{i+1,i+2} = \lambda_{i,i+2}$.

(c) D'après (d), les seuls sous-espaces $\mathfrak{S}_n$-stables non triviaux de $\mathbb{C}^n$ sont D et H. Mais, si $(d,e) \neq (1,1)$ ou $(d,e,n) \neq (1,2,2)$, alors D et H ne sont pas $\Delta(de,e,n)$-stables. Donc $G(de,e,n)$ est irréductible.

(b) Tout d'abord, remarquons que $G(de,e,n)$ est fini. De plus, $\mathfrak{S}_n$ est engendré par des réflexions (les transpositions). Posons $s = \mathrm{diag}(\zeta, 1, \dots, 1)$, où ζ est une racine primitive d-ième de l'unité et $t = \mathrm{diag}(\xi, \xi^{-1}, 1, \dots, 1)\tau_{12}$, où ξ est une racine primitive de-ième de l'unité. Alors il est facile de voir que $G(de,e,n) =< s, t, \mathfrak{S}_n >$, donc est engendré par des pseudo-réflexions.

(e) Posons, pour $1 \leqslant i \leqslant n-1$, $Y_i = \sigma_i(X_1^{de}, \dots, X_n^{de})$ et $Y_n = \sigma_n(x_1^d, \dots, X_n^d)$. Il est clair que $Y_1, \dots, Y_n$ sont dans $S(V)^{G(de,e,n)}$. D'autre part, d'après le théorème 6.1, il sont algébriquement indépendants. De plus, d'après (a), on a $|G(de,e,n)| = \prod_{i=1}^n \deg Y_i$. Notons $\mathrm{Deg}(G) = (d_1, \dots, d_n)$ et posons $\mathrm{Deg}(k[Y_1, \dots, Y_n]) = (e_1, \dots, e_n)$. Alors, d'après le fait démontré au cours de la preuve du théorème de Chevalley, on a $e_i \geqslant d_i$. Comme $e_1 \dots e_n = d_1 \dots d_n$, on en déduit que $e_i = d_i$ et que la série de Poincaré de $S(V)^G$ est égale à celle de $k[Y_1, \dots, Y_n]$. Donc $S(V)^G = k[Y_1, \dots, Y_n]$. ■

13.C. Quelques groupes exceptionnels. Shephard et Todd ont montré que, outre cette famille infinie de groupes de réflexions complexes, il y a 34 groupes de réflexions irréductibles exceptionnels. Nous ne donnerons pas ici la liste, mais nous nous contenterons de quelques exemples.

Exemple 13.2 - Soit ζ une racine de l'unité dans $\mathbb{C}$, $\zeta \neq 1$. Posons

$$s = \begin{pmatrix} \zeta & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad t = \begin{pmatrix} 1 & 0 \\ -\zeta & \zeta \end{pmatrix} \quad \in \mathbf{GL}_2(\mathbb{C}).$$

Alors s et t sont des réflexions d'ordre $o(\zeta)$ et vérifiant $sts = tst$. On note $G =< s, t >$. C'est un groupe engendré par des pseudo-réflexions. Il est irréductible.

On montrera dans l'exercice V.4 les faits suivants. Tout d'abord, G est fini si et seulement si $o(\zeta) \in \{2,3,4,5\}$. Dans ce cas, notons (d_1, d_2) la suite des degrés de $S(\mathbb{C}^2)^G$. Alors :

$o(\zeta)$	$\lvert G\rvert$	d_1, d_2	$\lvert Z(G)\rvert$
2	6	2, 3	1
3	24	4, 6	2
4	96	8, 12	4
5	600	20, 30	10

Exemple 13.3 - Soit ζ et ξ deux racines de l'unité dans $\mathbb{C}$, $\zeta, \xi \neq 1$. Posons

$$s = \begin{pmatrix} \zeta & -1 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad t = \begin{pmatrix} 1 & 0 \\ \zeta + \xi & \xi \end{pmatrix} \quad \in \mathbf{GL}_2(\mathbb{C}).$$

Alors s et t sont des réflexions d'ordre $o(\zeta)$ et $o(\xi)$ respectivement et vérifiant $ststst = tststs$. On note $G =< s, t >$. C'est un groupe engendré par des pseudo-réflexions. Il est irréductible.

On montrera dans l'exercice V.5 les faits suivants. Tout d'abord, G est fini si et seulement si $(o(\zeta), o(\xi)) \in \{(2,2),(3,3),(4,3),(5,3)\}$. Dans ce cas, notons (d_1, d_2) la suite des degrés de $S(\mathbb{C}^2)^G$. Alors :

$o(\zeta), o(\xi)$	$\lvert G\rvert$	d_1, d_2	$\lvert Z(G)\rvert$
$2,2$	8	$2,4$	2
$3,3$	72	$6,12$	6
$4,3$	288	$12,24$	12
$5,3$	1800	$30,60$	30

EXEMPLE 13.4 - Dans l'exercice IV.3, nous avons construit un groupe de réflexions complexe irréductible de rang 3 isomorphe à $\mathbf{GL}_3(\mathbb{F}_2) \times \{1, -1\}$. □

Exercices de la partie V

Exercice V.1. Montrer que le groupe dérivé de G est d'intersection complète (voir §9.C) et que, en reprenant les notations du théorème de Bessis-Bonnafé-Rouquier, G agit trivialement sur $I_{D(G)}/S(V_{D(G)})_+ I_{D(G)}$.

Exercice V.2. Posons $G^+ = G \cap \mathrm{Ker}(\det)$ et $p = |G/G^+|$. Supposons que p est premier.

(a) Montrer que $e_{\mathcal{C}} = p$ pour tout $\mathcal{C} \in \mathcal{A}_G/G$.
(b) Montrer que $S(V)^{G^+} = S(V)^G[\Delta_G] \simeq S(C)^G[T]/(T^p - \Delta_G^p)$.
(c) Montrer que G^+ est d'intersection complète et que, en reprenant les notations du théorème de Bessis-Bonnafé-Rouquier, G agit trivialement sur $I_{G^+)}/S(V_{G^+})_+ I_{G^+}$.

Exercice V.3. Montrer par un exemple que les assertions (a), (b) et (c) de l'exercice précédent peuvent ne pas être satisfaites lorsque $|G/G^+|$ n'est pas premier.

Exercice V.4. Montrer les assertions de l'exemple 13.2.

Exercice V.5. Montrer les assertions de l'exemple 13.3.

Exercice V.6. Soit n un entier naturel non nul. Voyons $\mathfrak{S}_n$ comme un groupe engendré par des réflexions. Si $\lambda = (\lambda_1, \ldots, \lambda_r)$ est une partition de n, c'est-à-dire une suite décroissante d'entiers naturels non nuls telle que $\lambda_1 + \cdots + \lambda_r = n$, notons $\mathfrak{S}_\lambda$ le sous-groupe naturel de $\mathfrak{S}_n$ isomorphe à $\mathfrak{S}_{\lambda_1} \times \cdots \times \mathfrak{S}_{\lambda_r}$.

(a) Montrer que $\mathfrak{S}_\lambda$ est engendré par des réflexions.

Notons E_λ la représentation absolument irréductible de $\mathfrak{S}_n$ associée à $\mathfrak{S}_\lambda$ par le théorème de Macdonald.

(b) Montrer que, si $\lambda \neq \lambda'$, alors E_λ et $E_{\lambda'}$ ne sont pas isomorphes (comme $\mathbb{Q}[\mathfrak{S}_n]$-modules.
(c) Montrer que $(E_\lambda)_{\lambda \vdash n}$ est un ensemble de reprśentants des classes d'isomorphie de $\mathbb{Q}[\mathfrak{S}_n]$-modules irréductibles.
(d) Montrer que $E_{(n-1,1)}$ est la représentation naturelle de $\mathfrak{S}_n$ comme groupe de réflexions irréductible en dimension $n-1$.

Partie VI. Groupes de Coxeter

14. Matrices de Coxeter, diagrammes de Dynkin

Fixons un ensemble fini S. On appelle *matrice de Coxeter* (*de support* S) toute matrice carrée symétrique $(m_{st})_{s,t\in S}$ d'entiers naturels non nuls telle que $m_{ss}=1$ et $m_{st}\geqslant 2$ si $s\neq 2$.

On appelle *diagramme de Dynkin* (*de support* S) tout graphe pondéré (non orienté) d'ensemble de sommets S et dont les arêtes sont pondérées par des entiers naturels $\geqslant 3$. Lorsque l'entier qui pondère une arête est égal à 3, nous ne l'écrirons pas. Lorsqu'il est égal à 4, nous pourrons le remplacer par une double arête. Lorsqu'il est égal à 6, nous pourrons remplacer par une triple arête.

Si $M=(m_{st})_{s,t\in S}$ est une matrice de Coxeter de support S, on notera $\mathbf{\Delta}(M)$ le diagramme de Dynkin de support S où s et t sont reliés par une arête de poids $m_{st}=m_{ts}$ lorsque $m_{st}\geqslant 3$ et ne sont pas reliés si $m_{st}=m_{ts}=2$. Si Δ est un diagramme de Dynkin de support S, nous noterons $\mathbf{M}(\Delta)$ la matrice de Coxeter telle que m_{st} est le poids de l'arête reliant s et t s'il y en a une, ou $m_{st}=2$ s'il n'y en a pas. Il est clair que $\mathbf{M}(\mathbf{\Delta}(M))=M$ et $\mathbf{\Delta}(\mathbf{M}(\Delta))=\Delta$, de sorte que l'on a ainsi construit une bijection entre les matrices de Coxeter de support S et les diagrammes de Dynkin de support S.

15. Groupes de Coxeter

Fixons ici un ensemble fini S et un diagramme de Dynkin Δ de support S. Posons $M=\mathbf{M}(\Delta)=(m_{st})_{s,t\in S}$. Nous noterons $\tilde{W}(\Delta)$ le groupe de présentation

$$\tilde{W}(\Delta)=<S\mid \forall\ s,t\in S,\ (st)^{m_{st}}=1>.$$

Notons que dans $\tilde{W}(\Delta)$, les éléments de S sont d'ordre 1 ou 2 (car $m_{ss}=1$).

Posons $V_\Delta=\oplus_{s\in S}\mathbb{R}e_s$ et posons, pour s, $t\in S$,

$$B_\Delta(e_s,e_t)=-\cos\frac{\pi}{m_{st}}.$$

Prolongeons B_Δ en une forme bilinéaire sur V_Δ. C'est une forme bilinéaire symétrique car M est symétrique. Nous posons, pour tout $x\in V$,

$$\sigma_s(x)=x-2B_\Delta(x,e_s)e_s.$$

Puisque $B_\Delta(e_s,e_s)=1$, on a $\sigma_s(e_s)=-e_s$, si $H_s=e_s^\perp$, alors $\sigma_s(x)=x$ pour tout $x\in H_s$. Donc σ_s est une réflexion orthogonale par rapport à l'hyperplan H_s. On note $W(\Delta)$ le sous-groupe de $\mathbf{GL}_\mathbb{R}(V_\Delta)$ engendré par $(\sigma_s)_{s\in S}$. En fait, $W(\Delta)\subset\mathbf{O}(V_\Delta,B_\Delta)$.

Proposition 15.1. *Il existe un unique morphisme surjectif de groupes $\tilde{W}(\Delta)\to W(\Delta)$ tel que $s\mapsto\sigma_s$.*

Preuve - Il suffit de vérifier que $(\sigma_s\sigma_t)^{m_{st}}=\mathrm{Id}_{V_\Delta}$. C'est facile lorsque $s=t$. On peut donc supposer que $s\neq t$. Notons P le plan engendré par e_s et e_t. Notons V' l'orthogonal de P. On a $P\cap V'=0$ car la restriction de B_Δ à P est définie positive. Donc $V_\Delta=P\oplus V'$. Il est évident que $\sigma_s\sigma_t$ agit trivialement sur V'. Il suffit de déterminer la restriction de $\sigma_s\sigma_t$ à P. C'est une rotation d'angle $2\pi/m_{st}$, d'où le résultat. ■

Proposition 15.2. *Soient $\Delta_1,\ldots,\Delta_r$ les composantes connexes de Δ. Notons S_i l'ensemble des sommets de Δ_i et notons V_i le sous-espace vectoriel de V engendré de base $(e_s)_{s\in S_i}$. Alors*

$V_\Delta = V_1 \oplus \cdots \oplus V_r$ est une décomposition orthogonale de V_Δ en somme directe de $\mathbb{R}[W(\Delta)]$-modules.

PREUVE - Soient s et t deux éléments de S tels que $m_{st} = 2$. Alors $B_\Delta(e_s, e_t) = 0$ et donc $\sigma_s(e_t) = e_t$ et $\sigma_t(e_s) = e_s$. Cela montre donc que, si $s \in S_i$, alors $\sigma_t(e_s) \in V_i$ dans tous les cas. ■

Corollaire 15.3. *Si $W(\Delta)$ est irréductible alors Δ est connexe.*

Proposition 15.4. *Si Δ est connexe, alors les seuls sous-espaces de V_Δ stables sous l'action de $W(\Delta)$ sont V_Δ et les sous-espaces de $V_\Delta^\perp$.*

PREUVE - Tout d'abord, $W(\Delta)$ agit trivialement sur $V_\Delta^\perp$. Donc tout sous-espace de $V_\Delta^\perp$ est stable sous l'action de $W(\Delta)$. Réciproquement, soit V' un sous-espace de V_Δ stable par $W(\Delta)$ qui ne soit pas contenu dans $V_\Delta^\perp$. Soit $x \in V'$ tel que $x \notin V_\Delta^\perp$. Il existe $s \in S$ tel que $B_\Delta(e_s, x) \neq 0$. Par suite, $\sigma_s(x) = x - 2B_\Delta(e_s, x)e_s \in V'$ (car V' est $W(\Delta)$-stable), donc $e_s \in V'$. Soit maintenant $t \in S$. Puisque Δ est connexe, il existe une suite $s = s_1, s_2, \ldots, s_r = t$ d'éléments de S deux à deux distincts tels que $m_{s_i s_{i+1}} \geqslant 3$ pour tout i, c'est-à-dire $B_\Delta(e_{s_i}, e_{s_{i+1}}) \neq 0$. Puisque $\sigma_{s_{i+1}}(e_{s_i}) = e_{s_i} - 2B_\Delta(e_{s_i}, e_{s_{i+1}})e_{s_{i+1}}$, il n'est pas difficile de montrer par récurrence sur i que $e_{s_i} \in V'$. Donc $e_t \in V'$, ce qui montre que $V' = V_\Delta$. ■

Pour montrer le théorème suivant, nous aurons besoin de quelques notations. Si $s \in S$, on pose $H_s = e_s^\perp$ et $H_s^+ = \{x \in V_\Delta \mid B_\Delta(x, e_s) > 0\}$. Soit

$$C_\Delta = \bigcap_{s \in S} H_s^+.$$

Notons que C_Δ est un simplexe ouvert (non vide...) de V_Δ et que l'adhérence de C_Δ est égale à

$$\overline{C}_\Delta = \{x \in V_\Delta \mid \forall\ s \in S,\ B_\Delta(x, e_s) \geqslant 0\}.$$

Si $w \in \tilde{W}(\Delta)$, notons $\ell(w)$ sa *longueur*, c'est-à-dire la longueur minimale d'une décomposition $w = s_1 \ldots s_l$ avec $s_i \in S$. Compte tenu de la présentation de $\tilde{W}(\Delta)$, l'application $\tilde{W}(\Delta) \to \{1, -1\}$, $w \mapsto \varepsilon(w) = (-1)^{\ell(w)}$ est un morphisme de groupes. Par suite, si $w \in \tilde{W}(\Delta)$ et si $s \in S$, alors $\ell(sw)$ et $\ell(ws)$ appartiennent à $\{\ell(w) - 1, \ell(w) + 1\}$.

Théorème (Tits). *Si $w \in \tilde{W}(\Delta)$ vérifie $\sigma(w)(C) \cap C \neq \varnothing$, alors $w = 1$.*

PREUVE - Nous allons montrer par récurrence sur l les assertions suivantes :

> *(P_l) Si $w \in \tilde{W}(\Delta)$ est tel que $\ell(w) = l$ et si $s \in S$, alors $w(C) \subset H_s^+$ ou $w(C) \subset s(H_s^+)$ et $\ell(sw) = \ell(w) - 1$.*
>
> *(Q_l) Si $w \in \tilde{W}(\Delta)$ est tel que $\ell(w) = l$ et si $s, t \in S$, avec $s \neq t$, alors il existe $u \in W_{s,t} =< s, t >$ tel que $w(C) \subset u(H_s^+ \cap H_t^+)$ et $\ell(w) = \ell(u) + \ell(u^{-1}w)$.*

Ces assertions sont triviales pour $l = 0$. Elles sont aussi aisément vérifiables pour l quelconque lorsque $n = \dim V_\Delta = |S| = 2$. Supposons donc que (P_l) et (Q_l) sont vraies. Montrons qu'alors (P_{l+1}) et (Q_{l+1}) le sont.

Tout d'abord, soit $w \in \tilde{W}(\Delta)$ tel que $\ell(w) = l + 1$ et soit $s \in S$. Il existe $t \in S$ tel que $\ell(tw) = \ell(w) - 1 = l$. Posons $w' = tw$. Si $s = t$, alors, d'après (P_l), on a $w'(C) \subset H_s^+$. Donc $w(C) \subset s(H_s^+)$, ce qui montre (P_{l+1}) dans ce cas. Supposons maintenant que $s \neq t$. Alors, d'après (Q_l) appliqué à w', il existe $u' \in W_{s,t}$ tel que $w'(C) \subset u'(H_s^+ \cap H_t^+)$ et $\ell(w') = \ell(u') + \ell(u'^{-1}w')$. On a alors $w(C) \subset tu'(H_s^+ \cap H_t^+)$. En utilisant le fait que les assertions (P_l) et (Q_l) soient vraie en rang 2, on obtient que $tu'(H_s^+ \cap H_t^+) \subset H_s^+$ ou $tu'(H_s^+ \cap H_t^+) \subset s(H_s^+)$ mais alors $\ell(stu') =$

$\ell(tu')-1$. Dans le premier cas, on obtient que $w(C)\subset H_s^+$. Dans le second cas, on obtient que $w(C)\subset s(H_s^+)$ et que $\ell(sw)=\ell(stw')\leqslant \ell(tu')+\ell(w')-1\leqslant \ell(w)$. Donc $\ell(sw)=\ell(w)-1$. Cela termine la preuve de (P_{l+1}).

Montrons maintenant (Q_{l+1}). Soit $w\in\tilde{W}(\Delta)$ tel que $\ell(w)=l+1$ et soient s et t deux éléments distincts de S. Si $w(C)\subset H_s^+\cap H_t^+$, la condition (Q_{l+1}) est vérifiée en prenant $u=1$. Sinon, supposons par exemple que $w(C)\not\subset H_s^+$. Alors, puisque (P_{l+1}) est vraie, on a $w(C)\subset s(H_s^+)$ et $\ell(sw)=\ell(w)-1=l$. Posons $w'=sw$. Puisque (Q_l) est vraie, il existe $u'\in W_{s,t}$ tel que $w'(C)\subset u'(H_s^+\cap H_t^+)$ et $\ell(w')=\ell(u')+\ell(u'^{-1}w')$. Posons $u=su'$. Ona alors $w(C)\subset u(H_s^+\cap H_t^+)$ et il est facile de voir que $\ell(w)=\ell(u)+\ell(u^{-1}w)$. Cela montre (Q_{l+1}).

Revenons à la preuve du théorème de Tits. Soit $w\in\tilde{W}(\Delta)$ tel que $w(C)\cap C\neq\varnothing$. Posons $l=\ell(w)$. Si $l=0$, alors $w=1$. Supposons donc que $l>0$. Il existe alors $s\in S$ tel que $\ell(sw)=\ell(w)-1$. Donc $\ell(ssw)=\ell(sw)+1$ et donc, d'après (P_l), on a $w(C)\subset ssw(C)\subset s(H_s^+)$ ce qui est impossible. ■

Corollaire 15.5. *Le morphisme surjectif $\tilde{W}(\Delta)\to W(\Delta)$ construit dans la proposition 15.1 est un isomorphisme.*

Corollaire 15.6. *Le groupe $W(\Delta)$ est un sous-groupe discret de $\mathbf{O}(V_\Delta,B_\Delta)$.*

Preuve - Soit $x\in C$. Posons $U=\{\sigma\in\mathbf{GL}_{\mathbb{R}}(V_\Delta)\mid\sigma(x)\in C\}$. Alors U est un ouvert de $\mathbf{GL}_{\mathbb{R}}(V_\Delta)$: en effet, c'est l'image inverse de C sous l'application continue $\mathbf{GL}_{\mathbb{R}}(V_\Delta)\to V_\Delta$, $\sigma\mapsto\sigma(x)$. D'autre part, d'après le théorème de Tits, $U\cap W(\Delta)=\{\mathrm{Id}_{V_\Delta}\}$. Donc $W(\Delta)$ est un sous-groupe discret de $\mathbf{O}(V_\Delta,B_\Delta)$. ■

16. Groupes de Coxeter finis

16.A. Classification. Nous utiliserons beaucoup le théorème suivant, dont nous ne donnerons pas non plus de preuve.

Proposition 16.1. *Le groupe $W(\Delta)$ est fini si et seulement si la forme B_Δ est définie positive.*

Preuve - Tout d'abord, si B_Δ est définie positive, alors $W(\Delta)$ est un sous-groupe discret (voir corollaire 15.6) du groupe compact $\mathbf{O}(V_\Delta,B_\Delta)$. Donc il est fini.

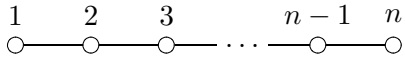
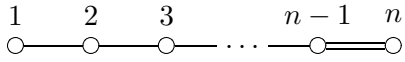
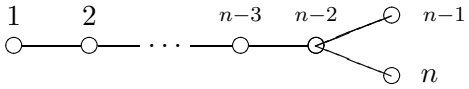
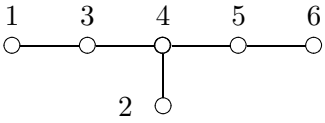
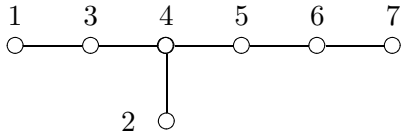
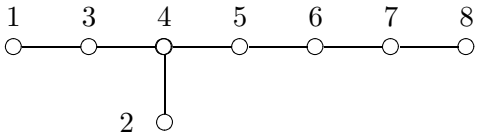
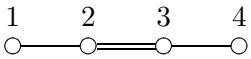
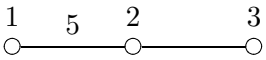
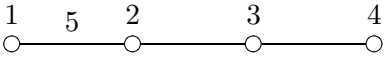
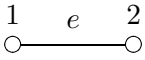
Réciproquement, supposons $W(\Delta)$ fini. Dans ce cas, par la semi-simplicité de l'action de $W(\Delta)$ sur V_Δ et la proposition 15.4, $V_\Delta^\perp=0$ et $W(\Delta)$ est (absolument) irréductible. D'après la proposition 15.2, nous pouvons supposer, et nous le ferons, que Δ est connexe. Soit $\langle,\rangle_0$ une forme bilinéaire symétrique définie positive sur V_Δ. Si x et y sont dans V_Δ, posons

$$\langle x,y\rangle=\sum_{\sigma\in W(\Delta)}\langle\sigma(x),\sigma(y)\rangle_0.$$

Alors $\langle,\rangle$ est une forme bilinéaire symétrique définie positive sur V_Δ invariante par l'action de $W(\Delta)$. Cela induit un isomorphisme $W(\Delta)$-équivariant $V_\Delta\simeq V_\Delta^*$. D'autre part, $\dim_{\mathbb{R}}(V_\Delta\otimes_{\mathbb{R}}V_\Delta^*)^{W(\Delta)}=1$. Donc $\dim_{\mathbb{R}}(V_\Delta^*\otimes_{\mathbb{R}}V_\Delta^*)^{W(\Delta)}=1$. Or, $\langle,\rangle$ et B_Δ peuvent être vus comme des éléments de $V_\Delta^*\otimes_{\mathbb{R}}V_\Delta^*$ stables sous $W(\Delta)$. Donc ils sont proportionnels. Puisque $B_\Delta(e_s,e_s)=1>0$, cela montre que B_Δ est définie positive. ■

Corollaire 16.2. *Supposons $W(\Delta)$ fini et reprenons les notations de la proposition 15.2. Alors $V_\Delta = V_1 \oplus \cdots \oplus V_r$ est une décomposition orthogonale de V_Δ en somme de sous-$\mathbb{R}[W(\Delta)]$-modules (absolument) irréductibles. En particulier, $W(\Delta)$ est irréductible si et seulement si Δ est connexe.*

Corollaire 16.3. *Le groupe $W(\Delta)$ est fini si et seulement si les composantes connexes de Δ sont isomorphes à l'un des diagrammes suivants :*

Type	*Diagramme*	W
A_n		$\mathfrak{S}_{n+1}$
B_n		$\mathfrak{S}_n \ltimes (\mathbb{Z}/2\mathbb{Z})^n$
D_n		$\mathfrak{S}_n \ltimes (\mathbb{Z}/2\mathbb{Z})^{n-1}$
E_6		
E_7		
E_8		
F_4		$\mathfrak{S}_3 \ltimes W(D_4)$
H_3		$\mathfrak{A}_5 \times \{1, -1\}$
H_4		
$I_2(e)$		D_{12}

Preuve - Il est tout d'abord facile, mais fastidieux, de vérifier au cas par cas que, pour tout Δ isomorphe à l'un des diagrammes donnés dans l'énoncé, la forme B_Δ est définie positive.

Pour montrer la réciproque, on peut supposer que Δ est irréductible. Supposons donc B_Δ définie positive. Quelques calculs fastidieux mais sans difficultés montrent les faits suivants (voir [Bbk]) :

1. Δ *ne contient pas de circuit.*

2. Δ *ne contient pas deux arêtes pondérées par un entier* $\geqslant 4$.

3. *Aucun point n'est relié à* 4 *sommets distincts.*

4. *Si un sommet est relié à au moins trois autres sommets, alors il n'y a pas d'arête pondérée par un entier* $\geqslant 4$.

Il ne reste alors qu'à éliminer quelques cas pour conclure. ■

Donnons maintenant la table des degrés des groupes de Coxeter finis.

Type de $\Delta(M)$	$\lvert W(M)\rvert$	$\mathrm{Deg}(S(V_\Delta)^{W(M)})$	$\lvert Z(W(M))\rvert$
A_1	2	2	2
$A_n,\ n \geqslant 2$	$(n+1)!$	$2, 3, 4, \ldots, n+1$	1
$B_n,\ n \geqslant 2$	$2^n.n!$	$2, 4, 6, \ldots, 2n$	2
$D_n,\ n \geqslant 3$	$2^{n-1}.n!$	$2, 4, 6, \ldots, 2(n-1), n$	$\begin{cases} 2 & \text{si } n \text{ est pair,} \\ 1 & \text{si } n \text{ est impair.} \end{cases}$
E_6	$51840 = 2^7.3^4.5$	$2, 5, 6, 8, 9, 12$	1
E_7	$2903040 = 2^{10}.3^4.5.7$	$2, 6, 8, 10, 12, 14, 18$	2
E_8	$696729600 = 2^{14}.3^5.5^2.7$	$2, 8, 12, 14, 18, 24, 30$	2
F_4	$1152 = 2^7.3^2$	$2, 6, 8, 12$	2
H_3	$120 = 2^3.3.5$	$2, 6, 10$	2
H_4	$14400 = 2^6.3^2.5^2$	$2, 12, 20, 30$	2
$I_2(e),\ e \geqslant 3$	$2e$	$2, e$	1

16.B. Rationalité. Nous allons examiner ici sous quelles conditions un groupe de Coxeter fini stabilise un réseau de V_Δ, c'est-à-dire peut-être vu comme un groupe de réflexions d'un $\mathbb{Q}$-espace vectoriel.

Lemme 16.4. *Supposons* $W(\Delta)$ *soit fini. Alors* $W(\Delta)$ *stabilise un réseau de* V_Δ *si et seulement si* $m_{st} \in \{2, 3, 4, 6\}$ *pour tous* $s \neq t \in S$.

Preuve - Supposons tout d'abord que $W(\Delta)$ stabilise un réseau de V_Δ. Alors, pour tout $\sigma \in W(\Delta)$, on a $\mathrm{Tr}(\sigma) \in \mathbb{Z}$. Or, si s et t sont deux éléments distincts de S, et si $n = |S|$, alors

$\mathrm{Tr}(\sigma_s\sigma_t) = n + 4(\cos^2(\pi/m_{st}) - 1)$. En effet,

$$\sigma_s\sigma_t(e_t) = -e_t + 2B_\Delta(e_s, e_t)e_s,$$

$$\sigma_s\sigma_t(e_s) = \sigma_s(e_s + 2\cos(\pi/m_{st})e_t) = (4\cos^2(\pi/m_{st}) - 1)e_s + 2\cos(\pi/m_{st})e_t$$

et

$$\sigma_s\sigma_t(e_u) = e_u - \alpha e_s - \beta e_t$$

si $u \notin \{s, t\}$. Par suite, $4\cos^2(\pi/m_{st}) \in \mathbb{Z}$, ce qui implique que $m_{st} \in \{2, 3, 4, 6\}$.

Réciproquement, supposons que $m_{st} \in \{2, 3, 4, 6\}$ pour tous $s \neq t \in S$. Nous allons montrer par récurrence sur $|S| = n$ qu'il existe une famille de nombres réels $(\lambda_s)_{s\in S}$ tel que $W(\Delta)$ stabilise le réseau $\oplus_{s\in S}\mathbb{Z}(\lambda_s e_s)$. On peut supposer pour cela que Δ est connexe.

Par examen de la liste des diagrammes de Dynkin possibles, on remarque qu'il existe toujours un élément s_0 de S qui n'est relié quà un seul autre élément de S. Notons $S' = S - \{s_0\}$ et s_1 l'élément de S' relié à s_0. Par hypothèse de récurrence, il existe une famille de nombres réels $(\lambda_s)_{s\in S'}$ telle que $\Gamma' = \oplus_{s\in S'}\mathbb{Z}(\lambda_s e_s)$ soit stable par $W(\Delta')$, où Δ' est le diagramme de Dynkin obtenu en enlevant le sommet s_0.

Si $m_{s_0s_1} = 3$, on pose $\lambda_{s_0} = \lambda_{s_1}$. Si $m_{s_0s_1} = 4$, on pose $\lambda_{s_0} = \sqrt{2}\lambda_{s_1}$. Si $m_{s_0s_1} = 6$, on pose $\lambda_{s_0} = \sqrt{3}\lambda_{s_1}$. Il est alors facile de vérifier que $\Gamma' \oplus \mathbb{Z}(\lambda_{s_0}e_{s_0})$ est stable par l'action de $W(\Delta)$. ■

Si $m_{st} \in \{2, 3, 4, 6\}$ pour tous $s \neq t \in S$, on dit que $W(\Delta)$ est un *groupe de Weyl*. D'après la proposition 16.3, $W(\Delta)$ est un groupe de Weyl si et seulement si toutes les composantes irréductibles de Δ sont de type A_n, B_n, D_n, E_6, E_7, E_8, F_4 ou $I_2(6)$ (ce dernier étant traditionnellement noté G_2). Un groupe de Weyl est donc un groupe de réflexion fini d'un $\mathbb{Q}$-espace vectoriel de dimension finie.

Remarque 16.5 - D'après l'exercice IV.2, si $W(\Delta)$ est un groupe de Weyl, il existe une extension galoisienne K de $\mathbb{Q}$ de groupe de Galois $W(\Delta)$.

Il n'est pas très difficile de montrer que, si Δ est de type H_3 ou H_4, alors $W(\Delta)$ est un groupe de réflexion d'un $\mathbb{Q}(\sqrt{5})$-espace vectoriel. Dans ce cas, toujours d'après l'exercice IV.2, il existe une extension galoisienne K de $\mathbb{Q}(\sqrt{5})$ de groupe de Galois $W(\Delta)$.

Pour finir, si Δ est de type $I_2(e)$, alors $W(\Delta)$ est un groupe de réflexion d'un $\mathbb{Q}(\cos 2\pi/e)$-espace vectoriel de dimension finie. Dans ce cas, toujours d'après l'exercice IV.2, il existe une extension galoisienne K de $\mathbb{Q}(\cos 2\pi/e)$ de groupe de Galois $W(\Delta)$. □

17. Élément de Coxeter

On supposer maintenant que $W(\Delta)$ est fini. Nous noterons $n = |S| = \dim_{\mathbb{R}} V_\Delta$ et nous noterons $(d_1, \ldots, d_n)$ la suite des degrés de $W(\Delta)$. Grâce au corollaire 15.5, nous pouvons identifier les éléments de s avec leurs images par le morphisme de la proposition 15.1. En d'autres termes, $\sigma_s = s$. Numérotons les éléments de S : $S = \{s_1, \ldots, s_n\}$, où $n = |S|$. Posons $c = s_1 \ldots s_n$. Cet élément est appelé élément de Coxeter standard de $W(\Delta)$. Il dépend de l'ordre choisi pour numéroter les éléments de S. Cependant, sa classe de conjugaison n'en dépend pas :

Proposition 17.1. *Soit $\tau \in \mathfrak{S}_n$. Alors $s_1 \ldots s_n$ est conjugué à $s_{\tau(1)} \ldots s_{\tau(n)}$.*

Preuve - Compte tenu du corollaire 16.3, il nous suffit de montrer le lemme suivant :

Lemme 17.2. *Soit Γ un groupe et soit $f : S \to \Gamma$ une application telle que que $f(s)$ et $f(t)$ commutent chaque fois que s et t ne sont pas liés. Soit $\tau \in \mathfrak{S}_n$. Alors $f(s_1)\dots f(s_n)$ et $f(s_{\tau(1)})\dots f(s_{\tau(n)})$ sont conjugués dans Γ.*

PREUVE - On raisonne par récurrence sur $|S|$, le résultat étant trivial pour $n = 1$ et évident pour $n = 2$. Soit $i \in \{1, 2, \dots, n\}$ tel que s_i ne soit lié quà au plus un sommet de Δ, sommet que nous noterons s_j. Quitte à faire agir le groupe symétrique, on peut supposer que $i = n$ et $j = n - 1$.

Comme $f(s_{\tau(1)})\dots f(s_{\tau(n)})$ est conjugué à $f(s_{\tau(2)})\dots f(s_{\tau(n)})f(s_{\tau(1)})$ (et ainsi de suite), on peut supposer que $\tau(n) = n$. Posons $j = \tau^{-1}(n-1)$. Comme s_n n'est lié quà s_{n-1}, on a

$$f(s_{\tau(1)})\dots f(s_{\tau(n)}) = f(s_{\tau(1)})\dots f(s_{\tau(n-1)})f(s_n)$$
$$= f(s_{\tau(1)})\dots f(s_{\tau(j-1)})f(s_{\tau(j+1)})\dots f(s_{\tau(n-2)})f(s_{n-1})f(s_{n-2}),$$

ce qui montre que l'on peut supposer que $\tau(n-1) = n-1$.

Posons $S' = \{s_1, \dots, s_{n-1}\}$ et notons τ' la restriction de τ à $\{1, 2, \dots, n-1\}$. Soit $f' : S' \to \Gamma$ l'application définie par $f'(s_l) = f(s_l)$ si $1 \leqslant l \leqslant n-2$ et $f'(s_{n-1}) = f(s_{n-1})f(s_n)$. Alors, par hypothèse de récurrence, l'élément $a = f'(s_1)\dots f'(s_{n-1})$ de Γ est conjugué à $b = f'(s_{\tau'(1)})\dots f'(s_{\tau'(n-1)})$. Mais, $a = f(s_1)\dots f(s_n)$ et $b = f(s_{\tau(1)})\dots f(s_{\tau(n)})$. ■

On appelle élément de Coxeter de $W(\Delta)$ tout élément de $W(\Delta)$ conjugué à un élément de Coxeter standard. Notons h l'ordre de c. Notons que h (ou h_Δ) est bien un invariant de Δ en vertu de la proposition précédente. Notons m_1,..., m_n les entiers naturels appartenant à $\{0, 1, 2, \dots, h-1\}$ tels que $m_1 \leqslant \dots \leqslant m_n$ et

$$\det(T\,\mathrm{Id}_{V_\Delta} - c) = \prod_{j=1}^{n}(T - e^{2i\pi m_j/h}).$$

Puisque $\det(T\,\mathrm{Id}_{V_\Delta} - c)$ est un polynôme à coefficients réels, on a $m_j + m_{n-j} = h$ pour tout $1 \leqslant j \leqslant n$. En particulier,

$$\sum_{j=1}^{n} m_j = \frac{hn}{2}. \tag{17.3}$$

Les entiers naturels m_1, ..., m_n sont appelés les exposants de Δ (ou de $W(\Delta)$).

Nous allons maintenant nous fixer un ordre sur S qui nous permettra de décomposer c en un produit de deux éléments d'ordre 2 particulièrement sympathique.

Compte tenu du corollaire 16.3, il existe une partition $S = S' \coprod S''$ de S telle que, si s, $t \in S'$ (res[. s, $t \in S''$), alors s et t ne sont pas liés dans Δ (c'est-à-dire $m_{st} = 2$ ou encore $B_\Delta(e_s, e_t) = 0$. Écrivons $S' = \{s_1, \dots, s_l\}$ et $S'' = \{s_{l+1}, \dots, s_n\}$, avec $0 \leqslant l \leqslant n$. Posons $s' = s_1 \dots s_l$, $s'' = s_{l+1} \dots s_n$ et $c = s's''$. Alors c est un élément de Coxeter et s' et s'' sont d'ordre 2. Pour simplifier les notations, nous poserons $e_{s_i} = e_i$, $H_i = e_i^\perp$, $V' = H_1 \cap \dots \cap H_l$ et $V'' = H_{l+1} \cap \dots \cap H_n$. Alors $V_\Delta = V' \oplus V''$ (attention, ce n'est pas forcément une décomposition orthogonale) et s' (resp. s'') est la symétrie orthogonale par rapport à V' (resp. V'").

Lemme 17.4. 1 *n'est pas valeur propre de c. En d'autres termes, $m_1 \geqslant 1$ et $m_n \leqslant h - 1$.*

PREUVE - Soit $x \in V_\Delta$ tel que $c(x) = x$. Alors $s'(x) = s''(x)$, c'est-à-dire $s'(x) - x = s''(x) - x$. Mais, $s'(x) - x \in V'^\perp$ et $s''(x) - x \in V''^\perp$. D'où $s'(x) = s''(x) = x$. Cela montre que $x \in V' \cap V'' = 0$. ■

À partir de maintenant, nous supposerons que $W(\Delta)$ est irréductible (c'est-à-dire que Δ est connexe). Posons

$$C = \{x \in V_\Delta \mid \forall\ 1 \leqslant i \leqslant n,\ B_\Delta(x, e_i) > 0\}.$$

Notons $(e^1, \dots, e^n)$ la base duale de $(e_1, \dots, e_n)$ par rapport à la forme bilináire B_Δ. On note $\rho : V_\Delta \to V_\Delta$ l'endomorphisme tel que $\rho(e^i) = e_i$. La matrice de ρ par rapport à la base $(e^1, \dots, e^l)$ est

$$\mathrm{Mat}(\rho) = (B_\Delta(e_i, e_j))_{1 \leqslant i,j \leqslant n}.$$

Cette matrice, sym'etrique, définie et positive, est diagonalisable et ses valeurs propres sont toutes strictement positives. Notons λ sa plus petite valeur propre, et soit $v = a_1 e^1 + \cdots + a_n e^n$ tel que $\rho(v) = \lambda v$ et $a_1 \geqslant 0$. Posons

$$v'' = a_1 e^1 + \cdots + a_l e^l \qquad \text{et} \qquad v' = a_{l+1} e^{l+1} + \cdots + a_n e^n.$$

On note P le plan engendré par v' et v''.

Lemme 17.5. *Supposons $W(\Delta)$ irréductible. Avec les notations précédentes, on a :*

(a) $\dim_{\mathbb{R}} \mathrm{Ker}(\rho - \lambda\, \mathrm{Id}_{V_\Delta}) = 1$.
(b) $a_i > 0$ *pour tout* i.
(c) P *est stable par* s' *et* s'' *(donc en particulier par* c*).*
(d) $s'|_P$ *(resp.* $s''|_P$*) est la réflexion orthogonale sur* P *par rapport à* $\mathbb{R}v'$ *(resp.* $\mathbb{R}v''$*).*
(e) v', $v'' \in \overline{C}$ *et* $P \cap C = \{\alpha v' + \beta v'' \mid \alpha, \beta > 0\}$.

Preuve - Notons $<,>$ le produit scalaire sur V_Δ tel que $(e^1, \dots, e^n)$ soit une base orthonormale. On a, pour tous x, $y \in V_\Delta$,

$$< x, y >= B_\Delta(\rho(x), y).$$

Posons $\rho' = \rho - \lambda\, \mathrm{Id}_{V_\Delta}$ et notons $(\rho'_{ij})_{1 \leqslant i,j \leqslant n}$ la matrice de ρ' dans la base $(e^1, \dots, e^n)$. On a

$$\rho'_{ij} \leqslant 0 \tag{1}$$

si $i \neq j$ et

$$B_\Delta(x, \rho'(x)) \geqslant 0 \tag{2}$$

pour tout $x \in V_\Delta$.

Soit $x = b_1 e^1 + \cdots + b_n e^n$ tel que $\rho'(x) = 0$ et $x \neq 0$. Posons $x^+ = |b_1| e^1 + \cdots + |b_n| e^n$. Alors, d'après (1), on a $< x^+, \rho'(x^+) > \leqslant < x, \rho'(x) >= 0$. Mais, par définition et d'après (2),

$$< x^+, \rho'(x^+) >= B_\Delta(\rho(x^+), \rho'(x^+)) = B_\Delta(\rho'(x^+), \rho'(x^+)) + \lambda B_\Delta(x^+, \rho'(x^+)) \geqslant 0.$$

Donc $\rho'(x^+) = 0$. Notons I_x l'ensemble des $i \in \{1, 2, \dots, n\}$ tels que $b_i = 0$. Puisque $\sum_{i=1}^n \rho'_{ij} |b_i| = 0$ pour tout j, on a que $\rho'_{ij} = 0$ si $i \notin I_x$ et $i \in I_x$. La connexité de Δ implique alors que $I_x = \varnothing$ ou $I_x = \{1, 2, \dots, n\}$. Comme $x \neq 0$, on a $I_x = \varnothing$. Cela montre que, si $x = b_1 e^1 + \cdots + b_n e^n \in \mathrm{Ker}\, \rho'$, alors $b_i \neq 0$ pour tout i.

En particulier, $\dim_{\mathbb{R}} \mathrm{Ker}\, \rho' \leqslant 1$ car sinon $\dim_{\mathbb{R}}(H_1 \cap \mathrm{Ker}\, \rho') \geqslant 1$ ce qui est impossible d'après ce que l'on vient de voir. D'où (a). De plus, v est proportionnel à x^+, donc $a_i > 0$ pour tout i. D'où (b). Cela montre aussi que v' et v'' appartiennent à $\overline{C}$. D'autre part, soient α et β deux nombres réels. Alors $\alpha v' + \beta v'' \in C$ si et seulement si α et β sont strictement positifs. D'où (e).

Il nous reste à montrer (c) et (d). On a $s'(v') = v'$ et $s''(v'') = v''$. De plus, si $1 \leqslant i \leqslant l$, on a $\lambda B_\Delta(e_i, v) = B_\Delta(e_i, \rho(v))$, ce qui montre que $\lambda a_i = a_i + \sum_{j=l+1}^n a_j B_\Delta(e_i, e_j)$. Donc

$$(\lambda - 1) a_i = \sum_{j=l+1}^{n} a_j B_\Delta(e_i, e_j). \tag{\#}$$

Donc

$$\begin{aligned}(\lambda-1)v'' &= \sum_{i=1}^{l}\sum_{j=l+1}^{n} a_j B_\Delta(e_i,e_j)e^i \\ &= \sum_{j=l+1}^{n} a_j(-e^j+e_j) \\ &= -v'+\sum_{j=l+1}^{n} a_j e_j.\end{aligned}$$

Cela montre que $(\lambda-1)v''+v'$ est orthogonal à e^i pour $1\leqslant i\leqslant l$, donc est orthogonal à V''. Par suite, s'' stabilise le $\mathbb{R}$-sous-espace vectoriel de V_Δ engendré par v'' et $(\lambda-1)v''+v'$, c'est-à-dire P. De même, s' stabilise P. Cela montre (c). (d) est alors immédiat. ■

Théorème 17.6. *Supposons Δ connexe. Alors :*

(a) $m_1=1$ *et* $m_n=h-1$. *De plus,* $1<m_j<h-2$ *si* $2\leqslant j\leqslant n-2$.

(b) $|\text{Réf}(G)|=\dfrac{hn}{2}$.

(c) $d_j=m_j+1$.

Preuve - Notons D le sous-groupe de $W(\Delta)$ engendré par s' et s''. On a $|D|=2h$ et

$$D=\{1,c,c^2,\dots,c^{h-1},s',s'c,\dots,s'c^{h-1}\}.$$

Notons m l'ordre de la restriction de c à P. Alors m divise h et la restriction de D à P (que nous notons D_m) est un groupe diédral d'ordre $2m$. Puisque $P\cap C\neq\varnothing$, il résulte du théorème de Tits que l'application de restriction $D\to D_m$ est un ismorphisme. Par suite, $m=h$.

D'autre part, toujours d'après le théorème de Tits, puisque $\sigma(P\cap C)\cap(P\cap C)\neq\varnothing$ avec $\sigma\in D$ implique que $\sigma=\mathrm{Id}_{V_\Delta}$, et vu la description de $P\cap C$ donnée dans le lemme 17.5 (e), on a que l'angle entre v' et v'' est égal à π/h. Donc la restriction de c à P est une rotation d'angle $2\pi/h$. Le polynôme caractéristique de cette rotation étant $(T-e^{2i\pi/h})(T-e^{-2i\pi/h})$, on en déduit (puisque $m_1\geqslant 1$) que $m_1=1$ et $m_n=h-1$. Cela montre une partie de l'énoncé (a).

Les transformés de $\mathbb{R}v'$ et $\mathbb{R}v''$ par l'action de D_m froment un ensemble de h droites que nous noterons $\mathcal{D}=\{D_1,\dots,D_h\}$. Soit maintenant $H\in\mathcal{A}_{W(\Delta)}$. Notons s_H la réflexion orthogonale par rapport à H. On a $s_H\in W(\Delta)$. Alors P n'est pas contenu dans H car sinon $s_H(P\cap C)=P\cap C$, ce qui contredit le théorème de Tits. Donc $P\cap H$ est une droite de P. On veut montrer que $P\cap H\in\mathcal{D}$. Quitte à conjuguer par un élément de D, on peut supposer que $P\cap H$ rencontre $\overline{P\cap C}$. Mais, d'après le théorème de Tits, on a que H ne rencontre pas $P\cap C$, donc $P\cap H$ est l'une des droites $\mathbb{R}v'$ ou $\mathbb{R}v''$. Donc $P\cap H\in\mathcal{D}$.

Pour montrer (b), c'est-à-dire pour montrer que $|\mathcal{A}_{W(\Delta)}|=\dfrac{hn}{2}$, il suffit de montrer que l'ensemble des hyperplans $H\in\mathcal{A}_{W(\Delta)}$ tels que $H\cap P=\mathbb{R}v'$ ou $\mathbb{R}v''$ est de cardinal n. Soit $\mathcal{H}$ cet ensemble d'hyperplans. On veut montrer que $\mathcal{H}=\{H_{s_1},\dots,H_{s_n}\}$. Il est tout d'abord clair que $H_{s_i}\cap P=\mathbb{R}v'$ si $1\leqslant i\leqslant l$ et $H_{s_i}\cap P=\mathbb{R}v''$ si $l+1\leqslant i\leqslant n$. Réciproquement, soit $H\in\mathcal{A}_{W(\Delta)}$ tel que $H\cap P\in\{\mathbb{R}v',\mathbb{R}v'\}$. Supposons par exemple que $H\cap P=\mathbb{R}v'$. Notons e_H le vecteur unitaire orthogonal à H et situé du même côté de H que C. Écrivons $e_H=\lambda_1e_1+\cdots+\lambda_ne_n$.

Lemme. *On a $\lambda_i\geqslant 0$ pour tout i.*

Preuve - Puisque e_H est du même côté de H que C, et puisque $e^i\in\overline{C}$, on a $B_\Delta(e_H,e^i)\geqslant 0$, c'est-à-dire $\lambda_i\geqslant 0$. □

Puisque $B_\Delta(e_H, v') = 0$, on déduit du lemme précédent que $\lambda_{l+1} = \cdots = \lambda_n = 0$ et donc que $e_H = \lambda_1 e_1 + \cdots + \lambda_l e_l$. Par suite, $s_i(e_H) = (\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_l e_l) - 2\lambda_i e_i$ si $1 \leqslant i \leqslant l$. Donc, d'après le lemme précédent, on obtient que e_H est proportionnel à l'un des e_i, ce qui montre que $H \in \mathcal{H}$. Cela termine la preuve de (b).

Montrons maintenant (c). Travaillons dans $V = \mathbb{C} \otimes_{\mathbb{R}} V_\Delta$ et fixons une base $(X_1, \ldots, X_n)$ de V telle que $c(X_j) = e^{2i\pi m_j/h} X_j$. Soit $P_1, \ldots, P_n$ un système de générateurs homogènes de $S(V)^{W(\Delta)}$ tel que $\deg P_j = d_j$. Considérons la matrice jacobienne

$$J(X_1, \ldots, X_n) = \Big(\frac{\partial P_j}{\partial X_k}\Big)_{1 \leqslant j,k \leqslant n}.$$

On peut de plus supposer que $X_1 \in \mathbb{C} \otimes_{\mathbb{R}} P$, et il est facile de vérifier que $X_1 \notin \mathbb{C} \otimes_{\mathbb{R}} H$ pour tout $H \in \mathcal{A}_{W(\Delta)}$. Par suite, d'après la proposition 11.9, on a $J(1, 0, \ldots, 0) \neq 0$. Il existe donc une permutation $\sigma \in \mathfrak{S}_n$ telle que $\dfrac{\partial P_j}{\partial X_{\sigma(j)}}(1, 0, \ldots, 0) \neq 0$. Comme $\dfrac{\partial P_j}{\partial X_{\sigma(j)}}$ est homogène de degré $d_j - 1$, le coefficient de $X_1^{d_j - 1} X_{\sigma(j)}$ dans P_j est non nul. L'invariance de P_j sous l'action de c montre alors que $d_j - 1 + m_{\sigma(j)} \equiv 0 \bmod h$.

Il existe donc une suite r_j d'entiers naturels telle que $h - m_{\sigma(j)} = m_{n-\sigma(j)} = d_j - 1 + hr_j$. Par suite, d'après (b) et le théorème de Chevalley-Shephard-Todd, on a

$$|\mathcal{A}_{W(\Delta)}| = \sum_{j=1}^{n} m_{n-\sigma(j)}) = \sum_{j=1}^{n} (d_j - 1).$$

Cela montre que $r_j = 0$ pour tout j. En particulier, $m_{n-\sigma(j)} = d_j - 1$. D'où (c).

Il nous reste à montrer la dernière assertion de (a). Compte tenu de (c), si on avait $m_2 = 1$, alors il y aurait deux invariants de degrés 2 de $W(\Delta)$ non proportionnels, ce qui contredit la connexité de Δ (c'est-à-dire l'irréductibilité de $W(\Delta)$). ■

Corollaire 17.7. *On a* $|W(\Delta)| = (m_1 + 1) \ldots (m_n + 1)$.

Exemple 17.8 - Supposons que Δ soit de type A_n. Alors $W(\Delta) \simeq \mathfrak{S}_{n+1}$ et il est facile de voir que $(1, 2, \ldots, n+1)$ est un élément de Coxeter de $W(\Delta)$. Son polynôme caractéristique dans V_Δ est $T^n + T^{n-1} + \cdots + T + 1$, donc les exposants de $W(\Delta)$ sont $(1, 2, \ldots, n)$. D'après le théorème 17.6 (c), on retrouve que les degrés de $W(\Delta)$ sont $(2, 3, \ldots, n+1)$. □

Exemple 17.9 - Supposons que Δ soit de type E_8. Nous allons calculer les matrices de $s_1, \ldots, s_8$. En utilisant par exemple `MAPLE` ou `GAP`, nous pouvons calculer la matrice de $c = s_1 \ldots s_8$ ainsi que son polynôme caractéristique : ce dernier est égal au polynôme cyclotomique $\Phi_{30}(T)$. Cela montre que $h = 30$, $(m_1, \ldots, m_8) = (1, 7, 11, 13, 17, 19, 23, 29)$, $(d_1, \ldots, d_8) = (2, 8, 12, 14, 18, 20, 24, 30)$ et

$$|W(E_8)| = 696729600 = 2^{14}.3^5.5^2.7,$$

ce qui n'était pas évident... □

Exercices de la partie VI

Exercice VI.1. Montrer les assertions de la remarque 16.5 concernant les corps de définition de $W(H_3)$, $W(H_4)$ et $W(I_2(e))$.

Exercice VI.2. Montrer que $W(A_n) \simeq G(1,1,n+1)$, $W(B_n) \simeq G(2,1,n)$, $W(D_n) \simeq G(2,2,n)$ et $W(I_2(e)) \simeq G(e,e,2)$.

Partie VII. Solution des exercices

Solutions des exercices de la partie 0

Exercice X - D'après la théorie de Galois, on a $[K : K^G] = |G|$. Donc $K_0 = K^G$ car $K_0 \subset K^G$. Par suite, A^G et A_0 ont même corps des fractions et sont intégralement clos. De plus, A^G est entier sur A_0. Donc $A_0 = A^G$. □

Solutions des exercices de la partie I

Exercice I.1 - Soit L le corps des fractions de $S(V)$ et K le corps des fractions de $S(V)^G$. Alors, d'après la proposition K (b), on a $K = L^G$. D'après la théorème de la base normale, il existe $l \in L$ tel que $({}^\sigma l)_{\sigma\in G}$ soit une K-base de L. On peut même supposer que $l \in S(V)$ d'après la proposition K (a). Alors la famille $({}^\sigma l)_{\sigma\in G}$ est k-libre. Posons $M = \oplus_{\sigma\in G} k\ {}^\sigma l$. Alors M est G-stable et $M \simeq k[G]$, comme $k[G]$-modules. ■

Exercice I.2 - (a) Si $P \in S(V)$ est homogène de degré d, alors ${}^\sigma P = (-1)^d P$. D'où le résultat.

(b) découle immédiatement du fait qu'un polynôme homogène de degré pair est produit de polynômes homogènes de degré 2.

(c) Soit X un générateur du k-espace vectoriel V. Alors, d'après (b), X^2 est un générateur de la k-algèbre $S(V)^G$. Donc $S(V)^G = k[X^2]$.

(d) Soit (X, Y) une base de V. Alors (X^2, XY, Y^2) est une base de $S^2(V)$. Alors, d'après (b), $S(V)^G = k[X^2, Y^2, XY]$. Notons $\pi : k[T_1, T_2, T] \to S(V)^G$ l'unique morphisme de k-algèbres tel que $T_1 \mapsto X^2$, $T_2 \mapsto Y^2$ et $T \mapsto XY$. Alors π est surjectif et $T^2 - T_1T_2 \in \operatorname{Ker}\pi$. Pour montrer la première assertion de (d), il nous suffit de montrer que $T^2 - T_1T_2$ engendre π.

Soit $P(T_1, T_2, T) \in \operatorname{Ker}\pi$. Voyons P comme un élément de $k[T_1, T_2][T]$ et effectuons la division euclidienne de P par $T^2 - T_1T_2$ (c'est possible car, comme élément de $k[T_1, T_2][T]$, $T^2 - T_1T_2$ est unitaire). On écrit donc

$$P = A.(T^2 - T_1T_2) + B,$$

avec A, $B \in k[T_1, T_2]$ et $\deg_V(B) \leqslant 1$. On écrit $B = \alpha T + \beta$, où α, $\beta \in k[T_1, T_2]$. Puisque $P \in \operatorname{Ker}\pi$, on a $\alpha(X^2, Y^2)XY = -\beta(X^2, Y^2)$. En regardant la parité des degrés en la variable X, on en déduit que $\alpha = \beta = 0$ et donc que P est un multiple de $T^2 - T_1T_2$.

Montrons maintenant la deuxième assertion. Posons $A = k[X^2, Y^2]$ et $v = XY$. Alors on a $S(V)^G = A \oplus Av$. En particulier, $S(V)^G$ est un A-module libre de rang 2. □

EXERCICE I.3 - Avant de commencer, remarquons que l'action de G sur A et bien définie. Reprenons les notations de l'exercice I.2, notamment de la question (d). On a alors un morphisme G-équivariant $S(V) \to A$, $X \mapsto x$ et $Y \mapsto y$. Puisque $|G|$ est inversible dans k, il résulte de la proposition 0 que l'application $S(V)^G \to A^G$ est surjective. Compte tenu du (d), on a donc

$$A^G \simeq k[T_1, T_2, T]/(T^2 - T_1T_2, T_1 + T_2 - 1) \simeq k[T, U]/(T^2 - U(1 - U)). \square$$

EXERCICE I.4 - Purement formel... $\square$

EXERCICE I.5 - Purement formel... $\square$

EXERCICE I.6 - Il est immédiat que $A^G = k \oplus (\oplus_{r \geqslant 1} k.(X^r + X^{-r})$. Il suffit alors de remarquer que, pour tout $r \geqslant 1$, $X^r + X^{-r} \in k[X + X^{-1}]$, ce qui est immédiat par récurrence sur r (par exemple, $X^2 + X^{-2} = (X + X^{-1})^2 - 2$. $\square$

EXERCICE I.7 - (a) Le groupe G contient r rotations (d'angle $2j\pi/r$, $0 \leqslant j \leqslant r - 1$) et r symétries orthogonales (par rapports aux droites passant par les sommets et celles passant par les milieux des côtés). Soit v un sommet du polygone régulier Γ et soit v' le milieu d'un des deux côtés de Γ contenant v. Notons Δ (respectivement Δ') la droite passant par v (respectivement v'). Notons s (respectivement t) la symétrie orthogonale par rapport à Δ (respectivement Δ'). Alors $G =< s, t >$ et $(st)^r = 1$.

(b) Puisque G stabilise Γ, il stabilise l'ensemble $\{v_1, \ldots, v_r\}$ de ses sommets. Donc $P \in S(V)^G$. Il nous reste à montrer que P est non nul. Soit $f : V \to \mathbb{R}$ une forme linéaire telle que $f(v_1) \neq 0$. Alors f s'étend en un morphisme de $\mathbb{R}$-algèbres $\tilde{f} : S(V) \to \mathbb{R}$. On a $\tilde{f}(P) = f(v_1)^2 + \cdots + f(v_r)^2 > 0$. Donc $\tilde{f}(P) \neq 0$.

(c) Puisque G stabilise Γ, il stabilise l'ensemble $\{v_1, \ldots, v_r\}$ de ses sommets. Donc $v_1 \ldots v_r \in S(V)^G$. De plus, $v_1 \ldots v_r$ est homogène de degré r.

(d) Raisonnons par l'absurde. Soit $P \in \mathbb{R}[T_1, T_2]$ de degré minimal tel que $P(T, U) = 0$. Alors P est irréductible car $S(V)$ est intègre. Écrivons

$$P = \sum_{i=0}^{n} a_i T_2^i$$

avec $a_i \in \mathbb{R}[T_1]$ et $a_n \neq 0$. Alors, puisque P est irréductible, on a $a_0 \neq 0$. De plus,

$$-a_0(T) = \sum_{i=1}^{n} a_i U^i$$

et donc U divise $a_0(T)$. En particulier, v_1 divise $a_0(T)$. Supposons v_2 choisi de sorte que (v_1, v_2) soit une base de V. Alors $T = \alpha v_1^2 + \beta v_1 v_2 + \gamma v_2^2$ avec α, $\gamma > 0$. On obtient bien une contradiction.

(e) Reprenons les notations du (d). Soit $P \in S^r(V)^G$, $r \geqslant 0$. Montrons par récurrence sur r que $P \in \mathbb{R}[T,U]$. Si $n = 0$, c'est évident. Supposons donc $n \geqslant 1$. On écrit

$$P = \sum_{i=0}^{n} a_i v_1^i v_2^{n-i}$$

avec $a_i \in \mathbb{R}$. Supposons $a_n \neq 0$. Notons $\sigma : V \to V$ la symétrie orthogonale par rapport à la droite $\mathbb{R}v_1$. Alors $\sigma(v_2) = -v_2 + \lambda v_1$ avec $\lambda \in \mathbb{R}$. Le coefficient de v_2^n dans l'expression de ${}^\sigma P = P$ est égal à $(-1)^n a_n$. Par suite, n est pair. On a alors $Q = P - (a_n/\gamma^{n/2})T \in \mathbb{R}[T,U]$ et l'expression de Q dans la base $(v_1^n, v_1^{n-1}v_2, \ldots, v_2^n)$ fait apparaître un coefficient nul sur v_2^n. Cela montre que l'on peut supposer que $a_n = 0$, ce qui sera fait par la suite.

Dans ce cas, v_1 divise P. Puisque P est invariant et que G agit transitivement sur $\{v_1, \ldots, v_r\}$, on obtient que v_i divise P pour tout i. Deux cas se présentent :

• Si r est impair, alors v_1, …, v_r sont deux à deux linéairement indépendants, donc sont deux à deux premiers entre eux comme éléments de $S(V)$. Par suite, $U = v_1 \ldots v_r$ divise P. Donc $P/U \in S(V)^G$ et l'hypothèse de récurrence montre alors que $P/U \in \mathbb{R}[T,U]$. Par suite, $P \in \mathbb{R}[T,U]$.

• Supposons r pair. En appliquant le même raisonnement que pour le cas impair, on est ramené à montrer que v_1^2 divise P. On sait déjà que $a_n = 0$. D'autre part, puisque r est pair, la symétrie orthogonale τ par rapport à la droite orthogonale à v_1 appartient à G. On a $\tau(v_1) = -v_1$ et $\tau(v_2) = v_2 - \mu v_1$ avec $\mu \in \mathbb{R}$. Par suite, le coefficient de $v_1^{n-1}v_2$ dans ${}^\tau P = P$ est égal à $-a_{n-1}$, ce qui montre que $a_{n-1} = 0$. Donc v_1^2 divise P. □

Exercice I.8 - On a $W = V^G$ et il est immédiat que G agit trivialement sur V/W. Donc l'application $V^G = W \to (V/W)^G = V/W$ est nulle et n'est donc pas surjective. □

Exercice I.9 - Si $a \in k$, alors $a^q = a$. Par suite, $(X+a)^q - (X+a) = X^q + a^q - X - a = X^q - X$. Donc $X^q - X \in k[X]^{(k,+)}$. Soit maintenant $P(X) \in k[X]^{(k,+)}$. On va montrer par récurrence sur $\deg P$ que $P \in k[X^q - X]$ (ce fait étant évident lorsque $\deg P = 0$). Tout d'abord, $P(X) - P(0) \in k[X]^{(k,+)}$, donc on peut supposer que $P(0) = 0$. En d'autres termes, X divise $P(X)$. Puisque P est invariant sous l'action de $(k,+)$, ${}^a X$ divise $P(X)$ pour tout $a \in k$. Donc $\prod_{a\in k}(X+a)$ divise $P(X)$. Mais, $\prod_{a\in k}(X+a) = X^q - X$. Donc $X^q - X$ divise $P(X)$. Soit $Q(X) \in k[X]$ tel que $P(X) = (X^q - X)P(X)$. Alors $Q(X) \in k[X]^{(k,+)}$ et $\deg Q = \deg P - q$. On conclut alors grâce à l'hypothèse de récurrence. □

Exercice I.10 - (a) On a $\prod_{\lambda\in k}(Y/X + \lambda) = (Y/X)^q - Y/X$, d'où le résultat en multipliant par X^q.

(b) Soit T_1 et T_2 deux indéterminées et soit $P \in k[T_1, T_2]$ tel que $P(T', X) = 0$. On écrit

$$P = \sum_{i=0}^{n} a_i T_1^i,$$

où $a_i \in k[T_2]$. Raisonnons par l'absurde et supposons $a_i \neq 0$. Écrivons alors

$$P(T', U) = \sum_{i=0}^{nq} b_i Y^i,$$

où $b_i \in k[X]$. On a $0 = b_{nq} = a_n$, ce qui contredit l'hypothèse. Donc X et T' sont algébriquement indépendants.

Introduisons la notation suivante : si $\lambda \in k$, on pose $\sigma_\lambda = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \in H$. Alors l'application $(k,+) \to H$, $\lambda \mapsto \sigma_\lambda$ est un isomorphisme de groupes. Alors ${}^{\sigma_\lambda}X = X$ et ${}^{\sigma_\lambda}Y = Y + \lambda X$. Donc, d'après (a),

$$T' = \prod_{\lambda \in k} {}^{\sigma_\lambda}Y.$$

On en déduit que X et T' appartiennent à $S(V)^H$.

Soit maintenant $P \in S^r(V)^H$, avec $r \geqslant 1$. Montrons par récurrence sur r que $P \in k[X, T']$. Si $r = 0$, c'est évident. Supposons maintenant que $r \geqslant 1$. On écrit

$$P = a_0 X^r + a_1 X^{r-1} Y + \cdots + a_r X Y^{r-1} + a_{r+1} Y^r.$$

Puisque $X \in S(V)^H$, on a $P - a_0 X^r \in S(V)^H$. De plus, Y divise $P^r - a_0 X^r$. Par suite, $T' = \prod_{\lambda \in k} {}^{\sigma_\lambda}Y$ divise $P - a_0 X^r$. Posons $Q = (P - a_0 X^r)/T'$. Alors $Q \in S(V)^H$ et $\deg Q = r - q$. Donc, par hypothèse de récurrence, $Q \in k[X, T']$. Par suite, $P = a_0 X^r + T' F(X, T') \in k[X, T']$.

(c) découle de calculs élémentaires.

(d) Soit $P \in k[T_1, T_2]$ de degré minimal tel que $P(T, U) = 0$ et $P \neq 0$. Puisque $S(V)$ est intègre, P est irréductible. Écrivons

$$P = \sum_{i=0}^{n} a_i T_1^i$$

avec $a_i \in k[T_2]$ et $a_n \neq 0$. Notons que $a_0 \neq 0$ car P est irréductible. On a alors

$$-a_0(U) = \sum_{i=1}^{n} s_i T^i.$$

Donc T divise $a_0(U) \neq 0$. En particulier, X divise $a_0(U)$, ce qui n'est possible que si $a_0 = 0$. Donc T et U sont algébriquement indépendants.

Soit maintenant $P \in S^r(V)^{G_1}$, avec $r \geqslant 1$. Montrons par récurrence sur r que $P \in k[X, T']$. Si $r = 0$, c'est évident. Supposons donc que $r \geqslant 1$. On écrit

$$P = a_0 X^r + a_1 X^{r-1} Y + \cdots + a_r X Y^{r-1} + a_{r+1} Y^r.$$

Si $a_{r+1} = 0$, alors X divise P. Par suite, ${}^{\sigma}X$ divise P pour tout $\sigma \in G_1$. Donc T divise P. Par hypothèse de récurrence, $P/T \in k[T, U]$ et donc $P \in k[T, U]$. Supposons donc maintenant que $a_{r+1} \neq 0$. Puisque $P \in S(V)^H$, il résulte du (b) que $P \in k[X, T']$. En particulier, en regardant le coefficient de Y^r, on obtient que r est un multiple de q.

Si $a \in k^\times$, on note $\tau_a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \in G_1$. Le coefficient de Y^r de ${}^{\tau_a}P = P$ est $a_{r+1} a^r$. Donc, pour tout $a \in k^\times$, on a $a_{r+1} a^r = a_{r+1}$ et donc $a^r = 1$ car $a_{r+1} \neq 0$. Puisque $k^\times$ est cyclique d'ordre $q - 1$, on obtient que $q - 1$ divise r. Par suite, $q(q-1)$ divise r. Écrivons $r = q(q-1)d$, avec $d \in \mathbb{N}^*$. Alors $P - a_{r+1} U^d \in S^r(V)^{G_1}$. D'autre part, le coefficient de Y^r dans $P - a_{r+1} U^d$ est nul et donc, par le raisonnement précédent, on obtient que $P - a_{r+1} U^d \in k[T, U]$. Par suite, $P \in k[T, U]$.

(e) Soit $P \in S(V)^G$. D'après (d), on a $S(V) \in k[T, U]$. On écrit

$$P = \sum_{i=0}^{n} a_i T^i$$

avec $a_i \in k[U] \subset S(V)^G$. D'après (b), on a alors, pour tout $\sigma \in G$,

$$^\sigma P = \sum_{i=0}^{n} (\det \sigma)^i a_i T^i.$$

Donc, $(\det \sigma)^i a_i = a_i$ pour tout $0 \leqslant i \leqslant r$ et $\sigma \in G$. Cela montre que $a_i = 0$ si i n'est pas un multiple de $q-1$. Donc $P \in k[T^{q-1}, U]$. □

Exercice I.11 - (a) Notons $M_{\mathbf{e}}$ la matrice $(X_i^{q^{e_j}})_{1 \leqslant i,j \leqslant n}$. Un calcul facile montre que $^\sigma M_{\mathbf{e}} = \sigma . M_{\mathbf{e}}$ pour tout $\sigma \in G$. Donc $^\sigma L_{\mathbf{e}} = (\det \sigma) L_{\mathbf{e}}$.

(b) IL est clair que X_1 divise $L_{\mathbf{e}}$. Donc, d'après (a), $^\sigma X_1$ divise $L_{\mathbf{e}}$ pour tout $\sigma \in G$. Par conséquent, T divise $L_{\mathbf{e}}$.

(c) D'après (b), T divise $L_{(0,1,\dots,n-1)}$. De plus, T est homogène et $\deg T = 1+q+\cdots+q^{n-1} = \deg L_{(0,1,\dots,n-1)}$. Il suffit de regarder un coefficient pour en déduire que $T = L_{(0,1,\dots,n-1)}$.

(d) D'après (c), $^\sigma T = (\det \sigma) T$ pour tout $\sigma \in G$. Donc $Y_i \in S(V)^G$. □

Solutions des exercices de la partie II

Exercice II.1 - Soit donc $A = k[X,Y]/(XY)$. Notons x (respectivement y) l'image de X (respectivement Y) dans A. Alors $V = kx \oplus ky$.

(a) On a $\mathrm{Deg}(A) = (1,1)$, $\mathrm{Rel}(A) = (2)$.

(b) Posons $A' = k[x+y]$. Alors A' est une algèbre de polynômes et $A = A' \oplus A'x$.

(c) Posons $\tilde{x} = 1 \otimes_k x \in \mathcal{K}_1(A)$ et $\tilde{y} = 1 \otimes_k y \in \mathcal{K}_1(A)$. Alors le complexe de Koszul de A s'écrit

$$0 \longrightarrow \mathcal{K}_2(A) \xrightarrow{d_2} \mathcal{K}_1(A) \xrightarrow{d_1} \mathcal{K}_0(A) \xrightarrow{d_0} k,$$

où $\tilde{x} \wedge \tilde{y}$ est une A-base de $\mathcal{K}_2(A)$, $(\tilde{x}, \tilde{y})$ est une A-base de $\mathcal{K}_1(A)$, $d_2(\tilde{x} \wedge \tilde{y}) = x\tilde{y} - y\tilde{x}$, $d_1(\tilde{x}) = x$ et $d_1(\tilde{y}) = y$. Alors $x\tilde{y} \in \mathrm{Ker}\, d_1$ (car $xy = 0$). Mais il est facile de vérifier que $x\tilde{y} \notin \mathrm{Im}\, d_2$. □

Solutions des exercices de la partie III

Exercice III.1 - Notons x et y les images respectives de X et Y dans l'algèbre $A = k[X,Y]/(XY)$. Alors $(1, x, x^2, x^3, x^4, \dots, y, y^2, y^3, y^4, \dots)$ est une k-base de A. Par suite,

$$P_A(T) = 1 + 2 \sum_{r \geqslant 1} T^r = \frac{1+T}{1-T}. \; \square$$

EXERCICE III.2 - (a) est clair.

(b) Notons σ_{ij} la transposition (i,j), $1 \leqslant i < j \leqslant n$. Alors, si $X \in \{X_1, \ldots, X_n\}$, on a

$$^{\sigma_{ij}}X \equiv X \bmod (X_i - X_j).$$

Par produit, on obtient que,

$$^{\sigma_{ij}}P \equiv P \bmod (X_i - X_j).$$

Mais, $^{\sigma_{ij}}P = -P$. Donc $2P \equiv 0 \bmod (X_i - X_j)$. Par suite, puisque k est de caractéristique différente de 2, P est divisible par $X_i - X_j$. Ceci étant vrai pour tout couple (i,j), on obtient que Δ divise P.

(c) Soit $P \in k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$. Soit τ une transposition quelconque. On pose $P_1 = P + {}^{\tau}P$ et $P_2 = P - {}^{\tau}P$. Alors $P = (P_1 + P_2)/2$. Alors P_1 et P_2 appartiennent à $k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$. D'autre part, ${}^{\tau}P_1 = P_1$ et ${}^{\tau}P_2 = -P_2$. Cela montre que $P_1 \in k[X_1, \ldots, X_n]^{\mathfrak{S}_n}$, que P_2 est divisible par Δ (voir (b)) et que $P_2/\Delta \in k[X_1, \ldots, X_n]^{\mathfrak{S}_n}$. D'où le résultat.

(d) résulte facilement de (a).

(e) Soit $\pi : k[\sigma_1, \ldots, \sigma_n][T] \to k[X_1, \ldots, X_n]^{\mathfrak{A}_n}$, $T \mapsto \Delta$. Alors π est surjectif d'après (c). Il suffit de montrer que $\operatorname{Ker}\pi$ est engendré par $T^2 - P$. Par division euclidienne, on est ramené 'a montrer que, si $a\Delta + b = 0$, avec a, $b \in k[\sigma_1, \ldots, \sigma_n]$, alors $a = b = 0$. Mais, en appliquant une transposition σ à cette égalité, on obtient que $-a\Delta + b = 0$, ce qui permet de conclure car k est de caractéristique différente de 2.

(f) On a $k[X_1, \ldots, X_n]^{\mathfrak{A}_n} = k[\sigma_1, \ldots, \sigma_n] \oplus k[\sigma_1, \ldots, \sigma_n]\Delta$. Donc

$$P_{k[X_1,\ldots,X_n]^{\mathfrak{A}_n}}(T) = \frac{1 + T^{n(n-1)/2}}{\prod_{i=1}^{n}(1 - T^i)}. \ \square$$

EXERCICE III.3 - (a) découle d'un calcul fastidieux mais facile.

(b) Soit $x = (x_1, \ldots, x_n) \in V = k^n$ tel que $T(x) = Y_1(x) = \cdots = Y_{n-1}(x) = 0$. Puisque $T(x) = 0$, il existe $j \in \{1, 2, \ldots, n\}$ et $a_{j+1}, \ldots, a_n$ dans k tels que $x_j + a_{j+1}x_{j+1} + \cdots + a_n x_n = 0$. Par suite, il existe $\sigma \in G$ tel que $^{\sigma}x = (u_1, \ldots, u_{n-1}, 0)$. Donc, d'après (a), on a $T'(u) = Y_1'(u) = \cdots = Y_{n-2}(u) = 0$, où $u = (u_1, \ldots, u_{n-1})$. Un raisonnement par récurrence per met de conclure que $u = 0$ et donc que $x = 0$.

(c) découle de (b) et du théorème 6.1.

(d) est facile (remarque que $|G_1| = |G|/(q-1)$). $\square$

Solutions des exercices de la partie IV

EXERCICE IV.1 - (a) Soit $K = IJ$. Il est facile de voir que $G = \{1, -1, I, -I, J, -J, K, -K\}$ car $IJI^{-1} = -J$ et $I^2 = J^2 = -1$. Donc $|G| = 8$.

(b) Par la formule de Molien, on a

$$P_R(T) = \frac{1}{8}\Big(\frac{1}{(1-T)^2} + \frac{1}{(1+T)^2} + \frac{6}{1+T^2}\Big) = \frac{1-T^2+T^4}{(1-T^2)(1-T^4)}.$$

(c) Il suffit de montrer que u, v et w sont invariants par I et J, ce qui est évident. Il est tout aussi clair que $w^2 = v(u^2 - 4v^2)$.

(d) Soient x et y dans $\mathbb{C}$ tels que $x^2y^2 = 0$ et $x^4 + y^4 = 0$. La première équation nous donne que $x = 0$ OU $y = 0$. De la deuxième, on déduit que $x = 0$ ET $y = 0$. Donc, d'après le théorème 6.1, u et v sont algébriquement indépendants.

(e) D'après (d) et l'exemple 4.2 (b), on a $P_A(T) = 1/(1-T^4)^2$ car $\deg u = \deg v = 4$.

(f) On a un morphisme surjectif $\pi : A[W] \to A'$, $W \mapsto w$. Pour montrer que $A' = A \oplus Aw$, il suffit de montrer que $\operatorname{Ker}\pi$ est engendré par $W^2 - v^2(u^2 - 4v^2)$. Soit $f \in A[W]$ tel que $\pi(f) = 0$. On effectue la division euclidienne de f par $W^2 - v^2(u^2 - 4v^2)$:

$$f = (W^2 - v^2(u^2 - 4v^2)).g + h \quad \text{avec} \deg_W h \leqslant 1.$$

On a alors $\pi(h) = 0$. On écrit $h = aW + b$, avec a, $b \in A$. On a donc $aw = -b$. En regardant les degrés modulo 4, on obtient que $a = b = 0$.

On déduit de ceci que $P_{A'}(T) = P_A(T) + P_{Aw}(T) = P_A(T)(1 + T^{\deg w})$. Donc

$$P_{A'}(T) = \frac{1+T^6}{(1-T^4)^2} = P_R(T).$$

(g) Puisque $A' \subset R$, on a $\dim A'_r \leqslant \dim R_r$ pour tout $r \geqslant 0$. Le fait que $P_{A'}(T) = P_R(T)$ permet de conclure que $A' = R$. Les dernières assertions proviennent du travail effectué dans le (f). □

EXERCICE IV.2 - D'après le théorème de Shephard-Todd-Chevalley, il existe des éléments algébriquement indépendants $X_1, \ldots, X_n$ de $R = S(V)^G$ tels que $R = k[X_1, \ldots, X_n]$. Notons L (respectivement K) le corps des fractions de S (respectivement R). Soit $\alpha \in S$ tel que $L = K(\alpha)$. Notons P le polynôme minimal de α. Alors $P \in R[T]$ est de degré $|G|$ car $[L : K] = |G|$ (le fait que $P \in R[T]$) découle de la factorialité de R). Soit Δ le discriminant de P ($\Delta \in R$). Posons $R' = R[1/\Delta]$ et $S' = S[1/\Delta]$. Alors $S'[\alpha]$ est la clôture intégrale de R' dans L. En d'autres termes, $S'[\alpha] \simeq R'[T]/(P(T))$ et G agit sur $S'[\alpha]$.

D'après le théorème de Hilbert, il existe $x = (x_1, \ldots, x_n) \in k^n$ tel que $P_x(T)$ soit un polynôme irréductible de $k[T]$ (ici, $P_x(T)$ désigne la spécialisation de P en x) et tel que $\Delta(x_1, \ldots .x_n) \neq 0$. Alors G agit sur $k' = k[T]/(P_x(T))$, k' est un corps et $k'^G = k$ d'après la proposition 0. □

EXERCICE IV.3 - (a) On a $|H| = (2^3-1)(2^3-2)(2^3-4) = 168 = 2^3 \times 3 \times 7$. Un élément $\sigma \in H$ est d'ordre 2 si et seulement si $(\sigma - 1)^2 = 0$ et $\sigma \neq 1$. La décomposition de Jordan nous dit alors que σ est conjugué à $v = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Or,

$$C_H(v) = \{ \begin{pmatrix} a & b & c \\ 0 & a & 0 \\ 0 & d & e \end{pmatrix} \mid a, b, c, d, e \in \mathbb{F}_2 \text{ et } a^2 e \neq 0\}.$$

Donc

$$C_H(v) = \{ \begin{pmatrix} 1 & b & c \\ 0 & 1 & 0 \\ 0 & d & 1 \end{pmatrix} \mid b, c, d \in \mathbb{F}_2 \}.$$

En particulier, $|C_H(v)| = 8$ et il y a donc 21 éléments d'ordre 2 dans H : ils sont tous conjugués.

Pour finir, les classes de conjugaison de $\mathbf{GL}_3(\mathbb{F}_2)$ sont en bijections avec les $\mathbb{F}_2[T]$-module de dimension 3. En voici la liste (nous introduisons la notation de l'élément correspondant) :

$\mathbb{F}_2[T]$-module	σ	$o(\sigma)$	$\lvert C_H(\sigma)\rvert$
$\Big(\mathbb{F}_2[T]/(T-1)\Big)^3$	$1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	1	168
$\mathbb{F}_2[T]/(T-1) \oplus \mathbb{F}_2[T]/(T-1)^2$	$v = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	2	8
$\mathbb{F}_2[T]/(T-1)^3$	$u = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	4	4
$\mathbb{F}_2[T]/(T^2+T+1) \oplus \mathbb{F}_2[T]/(T-1)$	$x = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	3	3
$\mathbb{F}_2[T]/(T^3+T^2+1)$	$y = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$	7	7
$\mathbb{F}_2[T]/(T^3+T+1)$	$y' = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$	7	7

En particulier, il y a 6 classes de conjugaison. Montrons pour finir que H est simple. Soit N un sous-groupe distingué non réduit à l'élément neutre. Le groupe H opère transitivement sur l'ensemble à 7 éléments $E = (\mathbb{F}^2)^3 - \{(0,0,0)\}$. Soit Ω une orbite de N dans E. Puisque N est distingué dans G, alors ${}^\sigma\Omega$ est une orbite pour l'action de N. Cela montre que toutes les orbites de N ont même cardinal. Donc, puique $N \neq \{1\}$, on a $|\Omega| = 7$. En particulier, N contient un élément d'ordre 7. Puisqu'il est distingué et que y' est conjugué à y^3, N contient y et y'. Comme il est distingué, il contient donc 48 éléments d'ordre 7. Soit P un 7-sous-groupe de Sylow de N et soit Q son normalisateur dans N. Alors Q est d'indice 8 dans N, ce qui montre que $7 \times 8 = 56$ divise l'ordre de N. Donc N contient un élément d'ordre 2, donc il contient v et

$$v' = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Or, $v'v = x$, donc N contient un élément d'ordre 3. Par suite, 3×56 divise l'ordre de N. Donc $N = G$ et G est simple.

(b) H a six caractères irréductibles $\{\chi_1 = 1, \chi_2, \chi_3, \chi_4, \chi_5, \chi_6\}$. On pose $n_i = \chi_i(1)$ et on suppose que $n_1 = 1 \leqslant n_2 \leqslant n_3 \leqslant n_4 \leqslant n_5 \leqslant n_6$. Alors

$$\sum_{i=2}^{6} n_i^2 = 167 \qquad \text{et} \qquad n_i \text{ divise } 168.$$

Remarquons que $n_2 \geqslant 2$ car il n'existe pas de morphisme non trivial $H \to \mathbb{C}^\times$. Par suite,

$$(n_2, n_3, n_4, n_5, n_6) = (2, 4, 7, 7, 7) \text{ ou } (3, 3, 6, 7, 8).$$

Pour s'en tirer, on aura besoin du lemme suivant :

> **Lemme.** *Soit* Γ *un groupe fini simple. Alors* Γ *n'a pas de caractère irréductible de degré* 2.
>
> Preuve - Supposons que Γ est simple et que Γ admet un caractère irréductible de degré 2. Alors $|\Gamma|$ est pair et Γ n'est pas abélien. Donc Γ contient une involution σ. Soit $\rho : \Gamma \to \mathbf{GL}_2(\mathbb{C})$ une représentation irréductible de Γ. Puisque Γ est simple, $\operatorname{Ker}\rho = \{1\}$. Trois cas se présentent :
>
> • Si $\rho(\sigma) = 1$, alors $\sigma \in \operatorname{Ker}\rho$ ce qui est impossible.
> • Si $\rho(\sigma) = -1$, alors $\rho(\sigma)$ commute avec $\rho(H)$, donc σ est central dans H car $\operatorname{Ker}\rho = \{1\}$. Donc le centre de H est non trivial, ce qui est impossible.
> • Si $\det(\rho(\sigma)) = -1$, alors l'application $\Gamma \to \mathbb{C}^\times$, $g \mapsto \det(\rho(g))$ n'est pas triviale, donc Γ admet un quotient abélien, ce qui est impossible. ■

(c) Par le même argument que dans la preuve du lemme ci-dessus, on a $\det\rho(\sigma) = 1$ pour tout $\sigma \in H$. En particulier, si $s^2 = 1$, alors $\rho(s) \sim \operatorname{diag}(1, -1, -1)$. Donc $-\rho(s)$ est une réflexion.

(d) Il est clair que $G \subset \Gamma = \rho(H) \times \{\mathrm{Id}_V, -\mathrm{Id}_V\}$. D'autre part, G est distingué dans Γ. Donc $G \cap \rho(H)$ est distingué dans $\rho(H)$. Mais $G \cap \rho(H) \neq 1$ car $G \cap \rho(H)$ contient $\rho(ss')$ pour toutes involutions σ, σ' dans H. Donc $G \cap \rho(H) = \rho(H)$ car $H \simeq \rho(H)$ est simple (voir (a)). Donc G contient $\rho(H)$ et $-\rho(v)$, donc il contient $\rho(H)$ et $-\mathrm{Id}_V$. Donc $G = \Gamma$.

(e) D'après (a), (c) et (d), G est un groupe engendré par des réflexions, $|G| = 336$ et G contient 21 pseudo-réflexions. En effet, puisque $\det(G) = \{1, -1\}$, les pseudo-réflexions de G sont des réflexions.

Par suite, $S(V)^G$ est une $\mathbb{C}$-algèbre de polynômes : notons (d_1, d_2, d_3) la suite de ses degrés. Alors, d'après le théorème de Shephard-Todd-Chevalley, on a

$$d_1 d_2 d_3 = 336 \quad \text{et} \quad d_1 + d_2 + d_3 = 24.$$

D'autre part, puisque $-\mathrm{Id}_V \in G$, d_1, d_2 et d_3 sont divisibles par 2. On en déduit facilement que $(d_1, d_2, d_3) = (4, 6, 14)$. ■

Exercice IV.4 - (a) a déjà été montré dans l'exercice I.2.

(b) Un élément $\sigma \in \mathbf{GL}_k(V)$ agit sur $I_N/S(\bar{V})_+ I_N$ par multiplication par $(\det\sigma)^2$. Donc il n'agit trivialement que lorsque l'élément est de déterminant 1 ou -1. Le (b) découle alors de cette observation et du théorème de Bessis-Bonnafé-Rouquier.

(c) Si $\det(T\,\mathrm{Id}_V - \sigma) = (T - \lambda_1)(T - \lambda_2)$, alors $\det(T\,\mathrm{Id}_{\bar{V}} - \sigma) = (T - \lambda_1^2)(T - \lambda_1\lambda_2)(T - \lambda_2^2)$. Si de plus σ est diagonalisable dans V, alors il est diagonalisable dans $\bar{V} = S^2(V)$. Le (c) découle alors facilement de ces observations. □

Solutions des exercices de la partie V

EXERCICE V.4 - Par action du groupe de Galois, le résultat ne doit dépendre que de l'ordre de ζ et non du choix de la racine primitive d-ième de l'unité. Notons d l'ordre de ζ et supposons donc que $\zeta = e^{2i\pi/d}$. Notons (e_1, e_2) la base canonique de $\mathbb{C}^2$.

Fait 1. *G est irréductible.*

PREUVE - Soit V un sous-$\mathbb{C}$-espace vectoriel non trivial de $\mathbb{C}^2$ stable par G. Alors il est stable par s, donc est égal à $\mathbb{C}e_1$ ou $\mathbb{C}(e_1 + (1-\zeta)e_2)$. De plus il est stable par t, donc est égal à $\mathbb{C}e_2$ ou $\mathbb{C}(e_1 - \zeta(1-\zeta)^{-1}e_2)$. Ceci est impossible car $\zeta(1-\zeta)^{-1} \neq 1-\zeta$. □

Posons $\rho = s^{-1}t$ et $\rho' = st^{-1}$ et $H =< \rho, \rho' >$. Notons que

$$\rho = \begin{pmatrix} 1+\zeta^{-1} & -1 \\ -\zeta & \zeta \end{pmatrix} \qquad \text{et} \qquad \rho' = \begin{pmatrix} ??? \end{pmatrix}.$$

Fait 2. *$H = G \cap \mathbf{SL}_2(\mathbb{C})$ et H est un sous-groupe distingué de G d'indice d. Donc G est fini si et seulement si H est fini.*

PREUVE - On a bien sûr $H \subset \mathbf{SL}_2(\mathbb{C})$. De plus, $G =< s, \rho >$. Comme $s\rho s^{-1} = ts^{-1} = \rho'^{-1}$, on obtient que G normalise H. Par suite, H est un sous-groupe distingué de G d'indice divisant d car $s^d = 1$. Mais $G \cap \mathbf{SL}_2(\mathbb{C})$ est un sous-groupe distingué de G d'indice d, contenant H. Donc $H = G \cap \mathbf{SL}_2(\mathbb{C})$ et $|G/H| = d$. □

Fait 3. *Si G est fini, alors $d \leqslant 5$.*

PREUVE - Supposons G fini. Alors ρ est d'ordre fini. Or, le polynôme caractéristique de ρ est égal à

$$P(T) = T^2 - (1 + \zeta + \zeta^{-1})T + 1.$$

Notons α et β les racines de P. Ce sont des racines de l'unité. On a $\alpha\beta = 1$, donc $\alpha = \beta^{-1}$ et $\alpha + \alpha^{-1} = 1 + 2\cos(2\pi/d)$. Par suite, $1 + 2\cos(2\pi/d) \leqslant 2$, ce qui montre que $d \leqslant 6$. D'autre part, si $d = 6$, alors $P(T) = (T-1)^2$ et $\rho \neq \mathrm{Id}$, donc ρ est d'ordre infini, ce qui est impossible. □

Fait 4. *Si $d = 2$, alors $G \simeq \mathfrak{S}_3$. En particulier, $|Z(G)| = 1$ et $d_1 = 2$ et $d_2 = 3$.*

PREUVE - On a $s^2 = t^2 = 1$. Il suffit donc de voir que st est d'ordre 3, ce qui est évident (cela découle par exemple de la relation $sts = tst$). □

Fait 5. *Si $d = 3$, alors ρ et ρ' sont d'ordre 4. On a $\rho^2 = \rho'^2 = -\mathrm{Id}_V$ et $\rho\rho'\rho^{-1} = \rho'^{-1}$. Par conséquent, $|H| = 8$ et donc $|G| = 24$. De plus, $\mathrm{Deg}(G) = (4, 6)$.*

PREUVE - Toutes les assertions sauf la dernière découle de calculs élémentaires. D'après le théorème de Shephard-Todd-Chevalley, on a $d_1 d_2 = 24$. D'autre part, puisque $-\mathrm{Id}_V \in G$, d_1 et d_2 sont pairs. Il y a donc deux possibilités : $(d_1, d_2) = (2, 12)$ ou $(4, 6)$. Mais il est facile de voir que H est le groupe quaternionique de l'exercice IV.1, donc H n'a pas d'invariants de degré 2. Donc G non plus. Par conséquent, $(d_1, d_2) = (4, 6)$. □

Fait 6. *Si $d = 4$, alors ρ et ρ' sont d'ordre 6. On a $|H| = 24$, $H \simeq \tilde{\mathfrak{A}}_4$, $|G| = 96$ et $(d_1, d_2) = (8, 12)$.*

PREUVE - .... □

Fait 7. *Si $d = 5$, alors ρ et ρ' sont d'ordre 10. On a $|H| = 120$, $H \simeq \tilde{\mathfrak{A}}_5$, $|G| = 600$ et $(d_1, d_2) = (20, 30)$.*

Preuve - ... □

Exercice V.5 -

Références

[Be] D. Bessis, *Sur le corps de définition d'un groupe de réflexions complexe*, Comm. Algebra **25** (1997), 2703–2716.

[BBR] D. Bessis, C. Bonnafé & R. Rouquier, *Quotients et extensions de groupes de réflexions*, Math. Ann. **323** (2002), 405–436.

[Bbk] N. Bourbaki, *Groupes et algèbres de Lie, chapitres IV, V et VI.*

[Br] M. Broué, *Invariants polynômiaux de groupes finis*, Cours de DEA donné à l'Université Paris VII, disponible sur `http://www.math.jussieu.fr/~broue/`

[BMR] M. Broué, G. Malle & R. Rouquier, *Complex reflection groups, braid groups, Hecke algebras*, J. reine angew. Math. **500** (1998), 127–190.

[C] C. Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. **77** (1955), 778–782.

[ST] G.C. Shephard & J.A. Todd, *Finite unitary reflection groups*, Canadian J. Math. **6** (1954), 274–304.

[Sp] T.A Springer, *Regular elements of finite reflection groups*, Invent. Math. **25** (1974), 159–198.

[St] R. Steinberg, *Differential equations invariant under finite reflection groups*, Trans. Amer. Math. Soc. **112** (1964), 392–400.