GIT

1 Introduction

Cours 1

Commençons par un cadre simple dans lequel on se donne un $\mathbb{C}$-espace vectoriel de dimension finie V sur lequel agit linéairement un groupe G. Autrement dit, on a un morphisme de groupes $\rho : G \to \mathrm{GL}(V)$ mais on notera pour simplifier $g.v = \rho(g)(v)$ pour $g \in G$ et $v \in V$.

Le groupe agit alors sur l'espace des fonctions polynomiales sur V, noté $\mathbb{C}[V]$. Une telle action est donnée par la formule

$$(g.P)(v) = P(g^{-1}v).$$

On considère l'algèbre des fonctions polynomiales invariantes par G et on la note:

$$\mathbb{C}[V]^G = \{P \in \mathbb{C}[V], g.P = P\}.$$

Supposons que cette algèbre est de type fini (ce n'est pas nécessairement vrai), c'est-à-dire qu'elle est engendrée par un nombre fini de polynômes $P_1, \ldots, P_N$. On considère alors l'application

$$\Phi : \begin{cases} V \to \mathbb{C}^N \\ v \mapsto (P_1(v), \ldots, P_N(v)) \end{cases}$$

et on note $V//G$ son image. En un sens que l'on précisera plus tard, cette image ne dépend pas du choix des générateurs, et on l'appellera le quotient algébrique de V par G. L'application surjective $\Phi : V \to V//G$ passe alors au quotient en une surjection

$$\Psi : V/G \to V//G$$

qui n'a pas lieu d'être injective, on verra des exemples.

1.1 Decomposition en composantes homogènes

Pour $d \geq 0$, on définit alors $\mathbb{C}[V]_d$ comme l'ensemble des polynômes homogènes de degré d, i.e. vérifiant $P(\lambda v) = \lambda^d P(v)$. On a par exemple $\mathbb{C}[V]_0 = \mathbb{C}$, $\mathbb{C}[V]_1 = V^*$ puis $\mathbb{C}[V]_d = S^d V^*$. Ces sous-espaces sont de dimension finie et stables par l'action de G. Ils donnent lieu à une décomposition

$$\mathbb{C}[V] = \bigoplus_{d \in \mathbb{N}} \mathbb{C}[V]_d.$$

Pour être concret, choisissons un isomorphisme $V = \mathbb{C}^n$ et notons $(x_1, \ldots, x_n)$ les coordonnées associées. On notera alors $X_1, \ldots, X_n$ à la fois les formes linéaires duales de la base canonique et les variables associées à l'isomorphisme

$$\mathbb{C}[V] \simeq \mathbb{C}[X_1, \ldots, X_n]$$

Les polynômes homogènes de degré d sont alors les combinaisons de monômes $X_1^{a_1} \cdots X_n^{a_n}$ vérifiant $a_1 + \cdots + a_n = d$.

La décomposition ci-dessus induit une décomposition en morceaux de dimension finie:

$$\mathbb{C}[V]^G = \bigoplus_{d \in \mathbb{N}} \mathbb{C}[V]_d^G.$$

Enfin, on définit la série de Hilbert

$$P = \sum_{d \in \mathbb{N}} t^d \dim \mathbb{C}[V]_d^G$$

qui se trouvera être rationnelle dans tous les cas intéressant pour nous. Elle sera en pratique plus facile à calculer que l'algèbre complète des invariants.

1.2 Exemples où G est fini

1.2.1 Un exemple avec S_n

Notons $e_1, \ldots, e_n$ la base canonique de $\mathbb{C}^n$ et S_n le groupe symétrique, que l'on fait agir sur $\mathbb{C}^n$ par la formule $\sigma e_i = e_{\sigma(i)}$. L'action induite sur $\mathbb{C}[X_1, \ldots, X_n]$ est alors

$$(\sigma.P)(X_1, \ldots, X_n) = P(X_{\sigma^{-1}(1)}, \ldots, X_{\sigma^{-1}(n)}).$$

Écrivons

$$(T - X_1) \cdots (T - X_n) = T^n - \sigma_1 T^{n-1} + \sigma_2 T^{n-2} + \cdots + (-1)^n \sigma_n$$

où $\sigma_k = \sum_{i_1 < \cdots < i_k} X_{i_1} \cdots X_{i_k}$ est le k-ième polynôme symétrique élémentaire (qui est de degré k). Il est bien connu qu'on a l'isomorphisme

$$\mathbb{C}[X_1, \ldots, X_n]^{S_n} = \mathbb{C}[\sigma_1, \ldots, \sigma_n]$$

En particulier, cela nous donne

$$P_{S_n} = \frac{1}{(1-t)(1-t^2)\cdots(1-t^n)} \text{ et } \mathbb{C}/\!/S_n = \mathbb{C}^n.$$

1.2.2 Un exemple avec A_n

La situation est déjà plus compliquée avec le groupe alterné, noté A_n et son action induite sur $\mathbb{C}^n$. En effet, on sait bien que le polynôme $\Delta = \prod_{i<j}(X_i - X_j)$ vérifie $\sigma.\Delta = \epsilon(\sigma)\Delta$ où $\epsilon : S_n \to \mathbb{Z}/2\mathbb{Z}$ désigne la signature. Il est donc invariant par A_n.

Tout polynôme invariant sous A_n peut s'écrire de manière unique sous la forme $P = P^+ + P^-$ où $\sigma.P^+ = P^+$ et $\sigma P^- = \epsilon(\sigma)P^-$ pour tout $\sigma \in S_n$ (écrire $P = \frac{1}{2}(P + \tau.P) + \frac{1}{2}(P - \tau.P)$ pour une transposition τ).

Un polynôme de la forme P^- doit s'annuler quand $X_i = X_j$ et donc est divisible par $(X_i - X_j)$ pour tout $i \neq j$. Ainsi $P^- = \Delta Q$ avec Q symétrique.

On déduit $\mathbb{C}[X_1, \ldots, X_n]^{A_n} = \mathbb{C}[\sigma_1, \ldots, \sigma_n, \Delta]$ mais ces variables ne sont pas algébriquement indépendantes car $\Delta^2 = \prod_{i \neq j}(X_i - X_j) = D(\sigma_1, \ldots, \sigma_n)$. Le quotient algébrique n'est plus un espace vectoriel mais le lieu des solutions dans $\mathbb{C}^{n+1}$ d'une équation polynomiale (une variété algébrique affine).

Pas de problème avec la série de Hilbert qui s'écrit $P_{A_n} = \frac{1+t^{\frac{n(n-1)}{2}}}{(1-t)(1-t^2)\cdots(1-t^n)}$.

1.2.3 Un exemple singulier avec $\mathbb{Z}/2\mathbb{Z}$

On peut considérer un exemple encore plus simple, où $\mathbb{Z}^2$ agit sur $\mathbb{C}^2$ par $(x, y) \mapsto (-x, -y)$. L'algèbre des invariants est alors engendrée par $U = X^2, V = XY, W = Y^2$, et on a une description complète

$$\mathbb{C}[X, Y]^{\mathbb{Z}/2\mathbb{Z}} = \mathbb{C}[U, V, W]/(V^2 - UW).$$

On calcule alors $P = \frac{1+t^2}{(1-t^2)^2}$. Quand au quotient algébrique, c'est un cône (dessiner les solutions à coefficients réels).

1.2.4 La formule de Molien

Dans le cas où G est fini, on dispose d'une formule universelle pour calculer la série de Hilbert, due à Molien (1897)

Théorème 1. *Soit $n \geq 1$ et $G \subset \mathrm{GL}_n(\mathbb{C})$ un groupe fini. Alors en notant I_n la matrice identité de taille n, on a:*

$$P_G = \sum_{d \in \mathbb{N}} t^d \dim \mathbb{C}[X_1, \ldots, X_n]_d = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_n - tg)}$$

Exemple 1. *Dans le cas de $\mathbb{Z}/2\mathbb{Z}$ agissant sur $\mathbb{C}^2$ par $(x, y) \mapsto (-x, -y)$ on obtient la série $\frac{1}{2}(\frac{1}{\det(I_2 - tI_2)} + \frac{1}{\det(I_2 + tI_2)})$. En réduisant au même dénominateur, on retrouve bien le résultat précédent.*

Preuve. La preuve se base sur le fait bien connu que si $\rho : G \to \mathrm{GL}(W)$ est une représentation de dimension finie de G, alors $\dim W^G = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}\, \rho(g)$. Cette formule se démontre facilement en observant que $\Pi = \frac{1}{|G|} \sum_{g \in G} \rho(g)$ est un projecteur dont l'image est W^G puis en prenant la trace.

Prenons maintenant $g \in G$ et diagonalisons son action sur $V = \mathbb{C}^n$. C'est possible car g est d'ordre fini. Notons $e_1, \dots, e_n$ une base propre et $\lambda_1, \dots, \lambda_n$ les valeurs propres associées. On a tout de suite $\det(I_n - tg) = \prod_{i=1}^n (1 - t\lambda_i)$.

Si $X_1, \dots, X_n$ est la base duale de $e_1, \dots, e_n$, la famille $(X_1^{a_1} \cdots X_n^{a_n})$ où $a_1 + \cdots + a_n = d$ forme une base de $\mathbb{C}[V]_d$ propre pour l'action de g, avec valeur propre $\lambda_1^{a_1} \cdots \lambda_n^{a_n}$. On a donc

$$\operatorname{Tr} g|_{\mathbb{C}[V]_d} = \sum_{a_1 + \cdots + a_n = d} \lambda_1^{a_1} \cdots \lambda_n^{a_n}.$$

Développons formellement

$$\frac{1}{(1 - X_1) \cdots (1 - X_n)} = \sum_{a_1, \dots, a_n \in \mathbb{N}} X_1^{a_1} \cdots X_n^{a_n}.$$

En remplaçant X_i par $t\lambda_i$, on trouve l'égalité

$$\frac{1}{\det(I_n - tg)} = \sum_d t^d \operatorname{Tr} g|_{\mathbb{C}[V]_d}$$

Il ne reste plus qu'à sommer sur $g \in G$ pour prouver la formule. □

1.3 Cas des formes binaires

Cours 2

1.3.1 Le cas des formes quadratiques binaires

Étant donné un polynôme $P(X) = aX^2 + bX + c$ de degré 2, on note son discriminant

$$D(P) = b^2 - 4ac.$$

Indépendamment de son intérêt dans l'étude de ces polynômes, D satisfait des invariances remarquables. Par exemple, si on change $P(X)$ en $P(X - \lambda)$, le discriminant ne change pas, pas plus que si on change P en son polynôme réciproque $P^*(X) = a + bX + cX^2$.

Une bonne façon de saisir ces invariances est d'homogénéiser P en l'écrivant

$$P(X, Y) = aX^2 + bXY + Y^2 \in \mathbb{C}[X, Y]_2.$$

Le groupe $\mathrm{GL}_2(\mathbb{C})$ agit naturellement sur $V = \mathbb{C}^2$, puis sur $\mathbb{C}[X, Y]_2$ par la formule habituelle $g.P = P \circ g^{-1}$. L'invariance de D correspond ainsi à l'action des matrices suivantes

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, \lambda \in \mathbb{C}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Or ces deux matrices engendrent le groupe $G = \mathrm{SL}_2(\mathbb{C})$. En posant $W = \mathbb{C}[X, Y]_2$, on a donc $D \in C[W]^G$. Cela caractérise presque D, au sens de la proposition suivante:

Proposition 1. *Tout polynôme en a, b, c invariant par l'action de* $\mathrm{SL}_2(\mathbb{C})$ *est un polynôme en D. En formule*

$$\mathbb{C}[W]^G = \mathbb{C}[D].$$

Preuve. Prenons $P \in W$ avec $D(P) \neq 0$, on peut alors écrire $P = l_1 l_2$ où $l_1, l_2 \in V^*$. Cette écriture est unique quitte à échanger l_1 et l_2 ou faire la substitution $(l_1, l_2) \mapsto (\lambda l_1, \lambda^{-1} l_2)$. Prenons $l_1(X,Y) = \alpha X + \beta Y$ et $l_2(X,Y) = \gamma X + \delta Y$: on calcule alors

$$D(P) = D(\alpha\gamma X^2 + (\alpha\delta + \beta\gamma)XY + \beta\delta Y^2) = (\alpha\delta - \beta\gamma)^2$$

Une façon agréable de l'écrire est d'introduire la fonction $\det : V^* \times V^* \to \mathbb{C}$ définie par $\det(l_1, l_2) = \alpha\delta - \beta\gamma$ de sorte à avoir

$$D(l_1 l_2) = \det(l_1, l_2)^2$$

Comme $\det(g.l_1, g.l_2) = \det(l_1, l_2)$ pour tout $g \in \mathrm{SL}_2(\mathbb{C})$, l'invariance de D est alors particulièrement claire. Mais de plus, comme (l_1, l_2) forme une base de V^*, il existe $g \in \mathrm{GL}_2(\mathbb{C})$ telle que $l_1 = g.X$ et $l_2 = g.Y$. Si on se retreint à $\mathrm{SL}_2(\mathbb{C})$ on aura seulement $g.l_1 = \lambda X$ et $g.l_2 = \lambda.Y$ pour un certain $\lambda \in \mathbb{C}^*$.

Faisons maintenant le raisonnement en supposant qu'on dispose d'un invariant $I \in \mathbb{C}[a, b, c]^G$. Quitte à le décomposer en somme d'éléments homogènes, on peut supposer que I est de degré $d > 0$. Regardons la fonction $I(gP)$ comme une fonction de $g \in \mathrm{GL}_2(\mathbb{C})$). On a $I(gP) = \det(g)^{d/2} I((\det g)^{-1/2} gP) = \det(g)^{d/2} I(P)$. Cette fonction n'est algébrique que si d est pair, ce qu'on peut donc supposer. On a alors

$$I(P) = I(g.P) = I(\lambda^2 XY) = \lambda^{2d} I(XY)$$

Comme on a aussi $D(P) = D(\lambda^2 XY) = \lambda^4$, La fonction $I - I(XY)D^{d/2}$ est une fonction polynomiale sur W qui est nulle sur $U = \{P, D(P) \neq 0\}$. Or cet ouvert est dense (on verra cela bientôt) et donc cette fonction est identiquement nulle, prouvant bien que I est proportionnelle à $D^{d/2}$. $\square$

1.3.2 Résultant

Le discriminant d'un polynôme homogène à deux variables se généralise en tout degré: il faut pour cela intriduire la notion de résultant qui est d'importance cruciale en géométrie algébrique. On prend donc le temps de la développer.

Soit $n, m \in \mathbb{N}^*$ deux entiers et $P, Q \in \mathbb{C}[X, Y]$ deux polynômes homogènes de degrés respectifs n et m. Si P ou Q sont nuls, on pose $R(P, Q) = 0$, dans le cas inverse on peut toujours écrire

$$P = \prod_{i=1}^{n} \lambda_i, Q = \prod_{j=1}^{m} \mu_j \text{ avec } \lambda_i, \mu_j \in V^*$$

Ces écritures sont uniques à l'ordre près et à multiplication près par des scalaires. On constate alors que l'expression ci-dessous est bien définie

$$D(P,Q) = \prod_{i=1}^{n} \prod_{j=1}^{m} \det(\lambda_i, \mu_j).$$

De plus, l'invariance de det par l'action de $g \in \mathrm{SL}_2(\mathbb{C})$ montre immédiatement que R est $\mathrm{SL}_2(\mathbb{C})$-invariant au sens où

$$R(g.P, g.Q) = R(P, G).$$

Il ne reste plus qu'à montrer que R est un polynôme dans les coefficients de P et Q, ce qu'établit la proposition suivante.

Proposition 2. *Soit*

$$\Phi_{P,Q} : \begin{cases} \mathbb{C}[X,Y]_{m-1} \times \mathbb{C}[X,Y]_{n-1} \to \mathbb{C}[X,Y]_{n+m-1} \\ (U,V) \mapsto UP + VQ. \end{cases}$$

Alors, calculé dans les bases canoniques on a l'égalité $\det(\Phi_{P,Q}) = R(P,Q)$.

Preuve. On commence par montrer que Φ est injectif ssi P et Q n'ont pas de facteurs communs.

En effet, si $P = lP'$ et $Q = lQ'$, on n'a qu'à calculer $\Phi(Q', -P') = Q'P - P'Q = l(P'Q' - Q'P') = 0$. Réciproquement, si on a $UP = -VQ$ avec $\deg U < m$ et $\deg V < n$ et que P et Q n'ont pas de facteurs communs, alors écrivons $P = \prod l_j^{m_j}$ où les l_j sont deux à deux non proportionnels. Comme $l_j^{m_j}$ divise VQ mais l_j ne divise pas Q, on en déduit que $l_j^{m_j}$ divise V. En faisant le produit sur tous les j, on tire que P divise V mais comme $\deg V < n$, cela impose $V = 0$, puis $U = 0$. On en déduit bien que Φ est injective.

On compare maintenant les fonctions R et $\det(\Phi)$ mais plutôt comme les fonctions suivantes

$$\begin{cases} (V^*)^n \times (V^*)^m \to \mathbb{C} \\ A : (\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_m) \mapsto \prod_{i,j} \det(\lambda_i, \mu_j) \\ B : (\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_m) \mapsto \det(\Phi_{\prod \lambda_i, \prod \mu_j}) \end{cases}$$

Le raisonnement ci-dessus montre que B s'annule dès qu'il existe i et j tels que λ_i et μ_j soient proportionnels, autrement dit, dès que $\det(\lambda_i, \mu_j) = 0$. Anticipons le chapitre suivant, le Nullstellensatz nous apprend donc qu'il existe une certaine puissance k tel que B^k soit divisible par $\det(\lambda_i, \mu_j)$. Mais ces polynômes sont de degré 1, donc irréductibles ainsi $\det(\lambda_i, \mu_j)$ divise $\det(\Phi)$.

On observe aussi que B est de degré mn ce qui nous donne l'égalité

$$B = CA$$

pour une certaine constante C à déterminer. Prenons alors $P = X^n$ et $Q = Y^m$. On a alors $R(P,Q) = 1$ tandis que Φ est l'identité dans la base canonique. Le résultat est donc démontré. □

1.3.3 Discriminant

Pour $P \in \mathbb{C}[X,Y]_n$, on pose $D(P) = R(\frac{\partial P}{\partial X}, \frac{\partial P}{\partial Y})$. Il s'agit bien d'un élément de $\mathbb{C}[S^n V^*]$ de degré $2n-2$. Voyons deux exemples:

si $P = aX^2 + bXY + cY^2$, on a $\frac{\partial P}{\partial X} = 2aX + bY$ et $\frac{\partial P}{\partial Y} = 2bX + cY$. Ainsi

$$D(P) = \begin{vmatrix} 2a & b \\ b & 2c \end{vmatrix} = 4ac - b^2$$

Si $P = aX^3 + 3bX^2Y + 3cXY^2 + dY^3$, on a $\frac{\partial P}{\partial X} = 3aX^2 + 6bXY + 3cY^2$ et $\frac{\partial P}{\partial Y} = 3bX^2 + 6cXY + 3dY^2$ ce qui donne

$$D(P) = 3^4 \begin{vmatrix} a & 2b & c & 0 \\ 0 & a & 2b & c \\ b & 2c & d & 0 \\ 0 & b & 2c & d \end{vmatrix} = 3^4(a^2d^2 + 4ac^3 - 6abcbd + 4b^2d^2 - 3b^2c^2).$$

Proposition 3. *Si $P = \prod_{i=1}^n l_i$ alors $D(P) = \prod_{i \neq j} \det(l_i, l_j)$. En particulier, D est bien invariant par l'action de $\mathrm{SL}_2(\mathbb{C})$.*

Preuve. Cette fois encore on compare les deux applications $A, B : (V^*)^n \to \mathbb{C}$ définies respectivement par $A(l_1, \ldots, l_n) = D(\prod l_i)$ et $B = \prod_{i \neq j} \det(l_i, l_j)$. On remarque que s'il existe $i \neq j$ tel que $l_i = l_j$ alors l_i^2 divise P et donc l_i divise simultanément $\partial_X P$ et $\partial Y P$. D'après la proposition précédente, on a $D(P) = 0$. Ainsi $\det(l_i, l_j)$ divise A, par le même argument.

On en déduit que $\Delta = \prod_{i<j} \det(l_i, l_j)$ divise A: écrivons $A = \Delta A'$. Si on échange i et j, Δ change de signe et A ne change pas, ce qui montre que A' doit aussi s'annuler si deux l_i sont proportionnels. On en déduit que Δ^2 divise A et finalement $A = cB$ comme avant. Il ne reste qu'à calculer la constante sur un exemple, ce qui est relativement difficile et pas très utile pour la suite. □

Dans le cas du degré 3, le discriminant est à nouveau le seul invariant au sens de la proposition suivante.

Proposition 4. *Posons $W = \mathbb{C}[X,Y]_3$, muni de l'action usuelle de $G = \mathrm{SL}_2(\mathbb{C})$. On a*

$$\mathbb{C}[W]^G = \mathbb{C}[D].$$

Preuve. La preuve est très similaire au cas du degré 2 mais utilise le fait plus subtil suivant. L'action de G sur $\mathbb{P}^1 = \mathbb{P}(V^*)$ est triplement transitive: étant donné deux triplets (x,y,z) et (x',y',z') d'éléments deux à deux distincts, il existe un élément $g \in \mathrm{SL}_2(\mathbb{C})$ (unique au signe près) vérifiant $gx = x', gy = y', gz = z'$.

Prenons donc $P \in \mathbb{C}[X,Y]_3$ vérifiant $D(P) \neq 0$ que l'on écrit $P = l_1 l_2 l_3$. Comme les l_i sont deux à deux non proportionnels, les éléments $[l_1], [l_2], [l_3]$ sont deux à deux distincts, on peut donc les envoyer respectivement sur $[X], [Y], [X+Y]$. Cela signifie que l'on aura $gP = \lambda XY(X+Y)$ pour un certain $\lambda \in \mathbb{C}^*$. Le reste de la preuve est similaire, tout invariant homogène coincidera avec une puissance de D sur un ouvert dense, et donc partout. □

1.3.4 Le cas des quartiques

Intéressons nous aux polynômes de degré 4 que l'on va écrire

$$P(X,Y) = aX^4 + 4bX^3Y + 6cX^2Y^2 + 4dXY^3 + eY^4$$

On cherche donc les polynômes en a, b, c, d, e invariants par l'action de $\mathrm{SL}_2(\mathbb{C})$. La nouveauté par rapport aux cas précédents est que l'on va trouver deux invariants algébriquement indépendants.

Tout d'abord, rappelons que S^4V^* est par définition la partie symétrique de $(V^*)^{\otimes 4}$. Précisément, l'inclusion $S^4V^* \to (V^*)^{\otimes 4}$ est donnée par la formule:

$$l_1 \cdots l_n = \frac{1}{n!} \sum_{\sigma \in S_n} l_{\sigma(1)} \otimes \cdots \otimes l_{\sigma(n)}.$$

On a donc l'inclusion $S^4V^* \subset S^2(S^2V^*)$ dans laquelle $E = S^2V^*$ est de dimension 3 et donc S^2E de dimension 6.

Notons $U = X^2 = X \otimes X$, $V = 2XY = X \otimes Y + Y \otimes X$ et $W = Y^2 = Y \otimes Y$ une base de E. On calcule $X^4 = X \otimes X \otimes X \otimes X = U^2$, de même $Y^4 = W^2$, puis

$$\begin{aligned} 4X^3Y &= X \otimes X \otimes X \otimes Y + X \otimes X \otimes Y \otimes X + X \otimes Y \otimes X \otimes X + Y \otimes X \otimes X \otimes X \\ &= X \otimes X \otimes (X \otimes Y + Y \otimes X) + (X \otimes Y + Y \otimes X) \otimes X \otimes X \\ &= U \otimes V + V \otimes U = 2UV \end{aligned}$$

et de même, $4XY^3 = 2VW$. Pour finir on calcule

$$\begin{aligned} 6X^2Y^2 &= X \otimes X \otimes Y \otimes Y + Y \otimes Y \otimes X \otimes X + (X \otimes Y + Y \otimes X)^{\otimes 2} \\ &= 2UW + V^2 \end{aligned}$$

Si on pense à tous ces éléments comme des formes quadratiques en U, V, W, on peut écrire P sous la forme matricielle suivante

$$q_P = \begin{pmatrix} a & b & c \\ b & c & d \\ c & d & e \end{pmatrix}$$

Ainsi S^4V^* s'identifie aux matrices symétriques dont tous les coefficients sur l'antidiagonale sont égaux entre eux, cela donne bien un sous-espace de dimension 5.

Remarquons maintenant que d'après les formules $U = X^2, V = 2XY, W = Y^2$, on a $V^2 = 4UW$. En notant $q_0 = 4UW - V^2$ on définit une forme quadratique sur E qui est G-invariante.

Cela implique que le déterminant de la forme quadratique $q_P + \lambda q_0$ est invariant sous l'action de G. On calcule

$$\det(q_P + \lambda q_0) = \begin{vmatrix} a & b & c + 2\lambda \\ b & c - \lambda & d \\ c + 2\lambda & d & e \end{vmatrix} = 4\lambda^3 - \lambda I + J$$

avec $I = ae - 4bd + 3c^2$ et $J = \begin{vmatrix} a & b & c \\ b & c & d \\ c & d & e \end{vmatrix}$. On voit apparaître deux invariants de degré respectif 2 et 3 dont on peut montrer qu'ils engendrent tous les invariants. On a même le résultat suivant:

Théorème 2.
$$\mathbb{C}[S^4V^*]^G = \mathbb{C}[I, J].$$

Par exemple, $D = I^3 - 27J^2$. Pour comprendre géométriquement ce que l'on a fait, on dessine le lieu d'annulation de q_0 et q_P dans $\mathbb{P}^2(\mathbb{C})$. Ce sont deux coniques, notées C_0 et C_P. En choisissant un isomorphisme $C_0 \simeq \mathbb{P}^1(\mathbb{C})$, les points d'intersection de C_P avec C_0 forment les racines de P. Si ces racines sont distinctes,la famille $q_P + \lambda q_0$ forme un pinceau de coniques passant par les 4 points d'intersections $C_0 \cap C_P$. Le polynôme $\det(q_P + \lambda q_0)$ s'annule en trois points qui représentent des coniques dégénérées, à savoir des paires de droites passant par ces 4 points.

On en déduit en particulier que les 4 racines de P sont distinctes ssi le discriminant de $4\lambda^3 - \lambda I + J$ est non nul, ce qui explique une partie du théorème. Plus amusant encore, si on sait déterminer les solutions de ce polynôme (de degré 3), on aura pour C_P deux équations de droites: leur intersection avec C_0 sera une équation de degré 2. C'est le principe de la résolution des équations de degré 4!

Remarque 1. *Le quotient algébrique $S^4V^* /\!/ \mathrm{SL}_2(\mathbb{C})$ diffère du quotient ensembliste. Déterminons les polynômes P tel que $I(P) = J(P) = 0$. Comme $D(P) = 0$, P doit avoir au moins une racine double. Si $P = l^4$, on peut supposer $P = X^4$ et alors $I(P) = J(P) = 0$. Sinon P a au moins deux facteurs distincts et on l'écrit*

$$P(X, Y) = XY(4\alpha X^2 + 6\beta XY + 4\gamma Y^2)$$

On calcule alors $I = -4\alpha\gamma + 3\beta^2$ et $J = \begin{vmatrix} 0 & \alpha & \beta \\ \alpha & \beta & \gamma \\ \beta & \gamma & 0 \end{vmatrix}$, ce qui donne $\beta(2\alpha\gamma - \beta^2) = 0$. Si $\beta \neq 0$, ce système n'a pas de solution. Ainsi $\beta = 0$ puis $\alpha = 0$ ou $\gamma = 0$. Dans les deux cas, P a une racine triple. On a donc

$$I(P) = J(P) = 0 \iff P \text{ a une racine triple.}$$

2 Actions de groupes sur les variétés algébriques

Cours 3

2.1 Propriétés des algèbres de type fini

Dans toute cette partie, on va considérer une $\mathbb{C}$-algèbre A, commutative et unitaire et de type fini, à savoir qu'elle est engendrée en tant qu'algèbre par un nombre fini d'éléments. Autrement dit, il existe un entier n et morphisme d'algèbre surjectif $\Phi : \mathbb{C}[X_1, \ldots, X_n] \to A$. En notant $I = \ker \Phi$, on constate que l'application $J \mapsto \Phi^{-1}(J)$ établit une bijection entre les idéaux de A et ceux de $\mathbb{C}[X_1, \dots, X_n]$ qui contiennent I. Par ce procédé, on ramène beaucoup de raisonnements au cas des algèbres de polynômes.

Théorème 3. *Pour tout $n \in \mathbb{N}$, l'algèbre $\mathbb{C}[X_1, \dots, X_n]$ est noetherienne, à savoir que tout idéal est engendré par un nombre fini d'éléments. Il en est de même de toute algèbre de type fini.*

Preuve. On admet le premier point qui est un fait classique, se démontrant par récurrence sur n. Quant au deuxième, étant donné un idéal $J \subset A$ et une surjection $\Phi : \mathbb{C}[X_1, \dots, X_n] \to A$, l'idéal $\Phi^{-1}(J)$ est engendré par $f_1, \dots, f_m$ par le premier point. Il s'en suit que J est engendré par $\Phi(f_1), \dots, \Phi(f_m)$. $\square$

Définition 1. *Etant donné une $\mathbb{C}$-algèbre A, on dira que*

- *A est intègre si pour tout $f, g \in A$, $fg = 0$ implique $f = 0$ ou $g = 0$.*
- *$f \in A$ est inversible s'il existe $g \in A$ tel que $fg = 1$.*
- *$f \in A$ est irréductible si dès que $f = gh$ on a g ou h inversible.*
- *A est factoriel s'il est intègre et tout élément peut s'écrire comme produit d'éléments irréductibles, et ce de façon unique modulo réarrangement et multiplication par un inversible.*

Théorème 4. *Pour tout $n \in \mathbb{N}$, l'algèbre $\mathbb{C}[X_1, \dots, X_n]$ est factorielle.*

A nouveau, on admet ce fait classique qui se montre par récurrence sur n. Cette fois la propriété ne passe pas aux quotients. Par exemple

$$A = \mathbb{C}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1)$$

n'est pas factoriel même si ce n'est pas si facile à prouver.

Pour finir, admettons le Nullstellensatz faible:

Théorème 5. *Si A est à la fois une $\mathbb{C}$-algèbre de type fini et un corps, alors $A = \mathbb{C}$.*

Dernière série de définitions:

Définition 2. *Soit A une $\mathbb{C}$-algèbre.*

- *un idéal $\mathcal{M} \subset A$ est dit maximal s'il est différent de A et maximal pour l'inclusion.*
- *un idéal $\mathcal{P} \subset A$ est premier si $fg \in \mathcal{P}$ implique $f \in \mathcal{P}$ ou $g \in \mathcal{P}$.*
- *pour tout idéal $I \subset A$ on note $\sqrt{I} = \{f, \exists n \in \mathbb{N}, f^n \in I\}$.*
- *l'idéal I est dit radical si $\sqrt{I} = I$.*
- *A est dit réduit si pour tout $n \in \mathbb{N}^*$ et $f \in A$, $f^n = 0 \implies f = 0$.*

On observe immédiatement que $\mathcal{P}$ est premier ssi $A/\mathcal{P}$ est intègre et I est radical ssi A/I est réduite.

Prenons A de type fini et $\mathcal{M}$ maximal: alors $A/\mathcal{M}$ est un corps et l'application quotient $\phi : A \to A/\mathcal{M}$ est surjective. En vertu du Nullstellensatz faible, on en déduit que ϕ induit un isomorphisme entre $\mathbb{C}$ et $A/\mathcal{M}$. Réciproquement, tout morphisme d'algèbre $\phi : A \to \mathbb{C}$ a pour noyau un idéal maximal. On peut donc identifier ces deux objets.

Montrons pour finir ces rappels le thèorème suivant qui prendra tout son sens dans la section suivante:

Théorème 6. *Soit A une $\mathbb{C}$-algèbre de type fini: alors*

$$\bigcap_{\mathcal{M} \text{ maximal}} \mathcal{M} = \sqrt{(0)}$$

Preuve. Un sens est facile: si $f \in \sqrt{(0)}$ alors $f^n = 0$ pour un certain $n \geq 1$. Tout $\mathcal{M}$ maximal est le noyau d'un morphisme surjectif $\phi : A \to \mathbb{C}$. On a donc $\phi(f^n) = \phi(f)^n = 0$ d'où $\phi(f) = 0$ et $f \in \mathcal{M}$.

Pour la réciproque, prenons $f \notin \sqrt{(0)}$. Cela signifie qu'aucun des f^n avec $n \in \mathbb{N}$ n'est nul. Dans ces conditions le localisé $A_f = A[T]/(Tf - 1)$ est non-trivial. Cette algèbre est à nouveau de type fini, on en choisit un idéal maximal $\mathcal{M}'$. Puis en notant $\phi : A \to A_f$ le morphisme naturel, on pose $\mathcal{M} = \phi^{-1}\mathcal{M}'$.

L'application $A/\mathcal{M} \to A_f/\mathcal{M}'$ est une injection mais comme $A_f/\mathcal{M}' = \mathbb{C}$, on a aussi $A/\mathcal{M} = \mathbb{C}$ et donc $\mathcal{M}$ est maximal. Pour conclure, on remarque que f est inversible dans A_f (d'inverse T) et donc $f \notin \mathcal{M}'$ et par suite on a aussi $f \notin \mathcal{M}$ et le résultat est démontré.

□

2.2 Topologie de Zariski

2.2.1 Définition du spectre

On se donne maintenant une $\mathbb{C}$-algèbre de type fini A et on pose

$$\operatorname{Spec} A = \{\mathcal{M} \subset A, \mathcal{M} \text{ idéal maximal}\}$$

On peut alors penser à A comme à une algèbre de fonctions sur $\operatorname{Spec} A$. Précisément, si on voit plutôt

$$A = \{\phi : A \to \mathbb{C}, \text{ morphisme d'algèbre}\}$$

on a qu'à poser $f(\phi) = \phi(f)$!

Il y a un piège: si $f(\phi) = 0$ pour tout $\phi \in \operatorname{Spec} A$, alors f est dans l'intersection de tous les idéaux maximaux, et d'après le théorème précédent, on a $f^n = 0$ pour un certain $n \in \mathbb{N}$. Il y a donc des fonctions non nulles qui "valent identiquement 0".

Exemple 2. *L'application suivante est une bijection*

$$\begin{cases} \mathbb{C}^n \to \operatorname{Spec} \mathbb{C}[X_1, \ldots, X_n] \\ (x_1, \ldots, x_n) \mapsto (X_1 - x_1, \ldots, X_n - x_n) \end{cases}$$

Il est clair que tous les idéaux ainsi produits sont maximaux. Réciproquement, tout morphisme d'algèbre $\phi : \mathbb{C}[X_1, \ldots, X_n]$ est déterminé par les valeurs $x_1 = \phi(X_1), \ldots, x_n = \phi(X_n)$. Son noyau est bien l'idéal associé à $(x_1, \ldots, x_n)$. Il est d'usage de noter $\mathbb{A}^n$ à la place de $\mathbb{C}^n$ quand on y pense comme une variété algébrique et non comme un espace vectoriel.

Dans le cas d'une algèbre présentée sous la forme $A = \mathbb{C}[X_1, \ldots, X_n]/I$, on se donne $P_1, \ldots, P_m$ des générateurs de I. Tout morphisme $\phi : A \to \mathbb{C}$ défini par les valeurs $x_1 = \Phi(X_1), \ldots, x_n = \phi(X_n)$ passe au quotient ssi $P_1(x_1, \ldots, x_n) = \cdots = P_m(x_1, \ldots, x_n) = 0$.

L'ensemble $\operatorname{Spec} A$ s'identifie au lieu des zéros communs de $P_1, \ldots, P_m$ dans $\mathbb{A}^n$. L'avantage du point de vue abstrait adopté ici est que la définition de $\operatorname{Spec} A$ est intrinsèque.

2.2.2 Definition de la topologie

Cours 4

Soit A une algèbre de type fini sur $\mathbb{C}$. On appelle fermé pour la topologie de Zariski tout ensemble de la forme

$$V(I) = \{\mathcal{M} \in \operatorname{Spec} A, I \subset \mathcal{M}\}$$

On a bien $V((0)) = \operatorname{Spec} A$ et $V(A) = \emptyset$, puis

$$\bigcap_{j \in J} V(I_j) = V(\sum_{j \in J} I_j)$$

et enfin $V(I) \cup V(J) = V(IJ)$, rappelons pourquoi. L'idéal IJ est l'idéal engendré par les éléments fg avec $f \in I$ et $g \in J$. On a donc $IJ \subset I \cap J$ d'où $V(I) \cup V(J) \subset V(IJ)$. Réciproquement si $\mathcal{M} \in V(IJ)$ alors $fg \in \mathcal{M}$ pour tout $f \in I$ et $g \in J$. Si $I \not\subset \mathcal{M}$ alors il existe $f \in I \setminus \mathcal{M}$ et pour tout $g \in J$ on a $fg \in \mathcal{M}$ donc $g \in \mathcal{M}$ car $\mathcal{M}$ est maximal (ça marcherait aussi avec premier). Il s'agit donc bien d'une topologie.

Notons $D(f) = \operatorname{Spec} A \setminus V((f))$: il s'agit d'un ouvert, dans l'interprétation fonctionnelle c'est simplement le lieu où f ne s'annule pas. Montrons qu'il s'agit d'une base d'ouverts: tout ouvert s'écrit $U = \operatorname{Spec} A \setminus V(I)$. Par noetherianité, $I = (f_1, \ldots, f_n)$ et donc $V(I) = \bigcap_{i=1}^n V(f_i)$. Par passage au complémentaire, on a bien

$$U = \bigcup_{i=1}^{n} D(f_i).$$

On prendra bien garde que cette topologie n'est jamais séparée: dans $\mathbb{A}^n$, tous les ouverts sont denses, et en particulier deux ouverts s'intersectent toujours non trivialement.

2.2.3 Produit

Étant données deux $\mathbb{C}$-algèbres de type fini A et B, leur produit tensoriel est aussi de type fini. Tout morphisme $\phi : A \otimes B \to \mathbb{C}$ est de la forme $\phi = \phi_A \phi_B$ où $\phi_A : A \to \mathbb{C}$ et $\phi_B : B \to \mathbb{C}$ sont des morphismes.

En effet, on pose $\phi_A(f) = \phi(f \otimes 1)$ et $\phi_B(g) = \phi(1 \otimes f)$ de sorte à avoir $\phi(f \otimes g) = \phi(f \otimes 1 \cdot 1 \otimes g) = \phi_A(f)\phi_B(g)$. On a donc un isomorphisme canonique

$$\mathrm{Spec}(A \otimes B) = \mathrm{Spec}(A) \otimes \mathrm{Spec}\, B.$$

Ce sera notre définition du produit: $X \times Y = \mathrm{Spec}(\mathbb{C}[X] \otimes \mathbb{C}[Y])$.

2.2.4 Composantes irréductibles

Définition 3. *Un espace topologique X est dit irréductible si on ne peut pas l'écrire sous la forme $X = X_1 \cup X_2$ avec X_1, X_2 deux fermés propres. De manière équivalente, X est irréductible si deux ouverts non vide ont toujours une intersection non triviale.*

Par exemple si A est intègre ssi $\mathrm{Spec}\, A$ est irréductible. En effet, deux ouverts contiennent chacun un ouvert de la forme $D(f)$ et $D(g)$, et alors $D(f) \cap D(g) = D(fg)$. Mais si f et g sont non nuls, alors $fg \neq 0$ et $D(fg) \neq \emptyset$.

Une composante irréductible de X est un fermé irréductible maximal pour l'inclusion. On peut démontrer que $\mathrm{Spec}\, A$ se décompose de manière unique en un nombre fini de composantes irréductibles. Par exemple, $\mathrm{Spec}\, \mathbb{C}[X, Y]/(XY)$ est la réunion de deux droites (irréducibles) données par les équations $X = 0$ et $Y = 0$. Bien sûr, le point est que l'idéal (XY) n'est pas premier, la décomposition en composantes irréductibles correspond à une décomposition de cet idéal en produit.

2.2.5 Dimension

Etant donné une $\mathbb{C}$-algèbre de type fini A et $X = \mathrm{Spec}\, A$, on ne peut pas construire une suite infinie décroissante de fermés strictement emboités. Cela provient du fait qu'en posant $F_j = V(I_j)$, on aurait une suite croissante infinie d'idéaux ce qui est impossible dans un anneau noethérien.

En effet, si on a une suite croissante d'idéaux $I_0 \subset I_1 \subset \cdots$, notons $\mathcal{I}$ la réunion. C'est un idéal, et comme il est de type fini, il existe k tel que I_k contienne les générateurs de $\mathcal{I}$. Ainsi cette suite stationne.

Définition 4. *La dimension de X est le plus grand entier d tel qu'il existe une suite de fermés irréductibles (non vides) strictement emboîtés $F_0 \subset \cdots \subset F_d = X$.*

Proposition 5. *Soit X une variété affine intègre, $\mathbb{C}[X]$ son anneau de fonctions et $\mathbb{C}(X)$ le corps des fractions de $\mathbb{C}[X]$. La dimension de X est égale au degré de transcendance de $\mathbb{C}(X)$, i.e. le nombre maximal d'éléments algébriquement indépendants.*

A priori, il n'est pas clair qu'un tel entier soit fini mais on a bien

$$\dim \mathbb{A}^n = \deg.\mathrm{tr}.\mathbb{C}(X_1, \ldots, X_n) = n.$$

Par ailleurs, il est clair que toute surjection $\mathbb{C}[X_1, \ldots, X_n] \to A$ donne lieu à un plongement $X \subset \mathbb{A}^n$ de sorte qu'on a $\dim X \leq n$.

2.2.6 Morphismes

Soit $X = \operatorname{Spec} A$ et $Y = \operatorname{Spec} B$ deux variétés algébriques affines. On voudrait définir un morphisme algébrique $f : X \to Y$ de sorte que l'application $f^* : B \to A$ qui à g associe $g \circ F$ soit un morphisme d'algèbre. Et bien ce sera notre définition!

Autrement dit, un morphisme $f : X \to Y$ est défini comme un morphisme d'algèbre $f^* : B \to A$. Ensemblistement, il envoie $\mathcal{M}$ sur $f^{-1}(\mathcal{M})$.

Par exemple, les morphismes $X \to \mathbb{C}$ s'identifient donc aux morphismes d'anneaux $1 \to A$, à savoir A. Si on veut privilégier le point de vue géométrique, on notera $A = \mathbb{C}[X]$ cette algèbre.

Pour tester la cohérence, prenons $A = \mathbb{C}[X_1, \ldots, X_n]$ et $B = \mathbb{C}[Y_1, \ldots, Y_m]$: un morphisme $f^* : A \to B$ est donné par n polynômes à m variables $P_1, \ldots, P_n$. On a alors explicitement

$$f : \begin{cases} \mathbb{C}^m \to \mathbb{C}^n \\ (x_1, \ldots, x_m) \mapsto (P_1(x_1, \ldots, x_m), \ldots, P_n(x_1, \ldots, x_m)). \end{cases}$$

Dès qu'on a une surjection $f^* : A \to B$, elle induit une injection $\operatorname{Spec} B \to \operatorname{Spec} A$ que l'on appelle plongement (l'image d'un fermé est fermée). En particulier, toute variété algébrique affine X "se plonge" dans $\mathbb{A}^n$ puisqu'il existe par hypothèse une surjection $\mathbb{C}[X_1, \ldots, X_n] \to \mathbb{C}[X]$.

On aura besoin de deux théorèmes concernant respectivement l'image et les fibres d'un morphisme.

Définition 5. *Soit $f : X \to Y$ une application algébrique entre deux schémas affines (c'est-à-dire un morphisme $f^* : \mathbb{C}[Y] \to \mathbb{C}[X]$). On dira qu'il est dominant si son image est dense dans Y (pour la topologie de Zariski). Il est équivalent de demander que le morphisme $f^* : \mathbb{C}[Y] \to \mathbb{C}[X]$ soit injectif modulo les nilpotents ($\ker f^* \subset \sqrt{(0)}$).*

En effet, si g est non nilpotente et vérifie $g \circ f = 0$ alors l'image de f est incluse dans le lieu d'annulation de g. Elle ne peut être dense puisqu'elle ne rencontre pas l'ouvert non vide $D(g)$.

Réciproquement, supposons f^* injective modulo les nilpotents. Le même raisonnement montre que $\operatorname{Im} f \cap D(g) \neq \emptyset$ pour tout g non nilpotent. Comme ces ouverts forment une base, $\operatorname{Im} f$ est bien dense.

Théorème 7. *Soit $f : X \to Y$ un morphisme dominant entre deux variétés affines. Alors $\operatorname{Im} f$ contient un ouvert de Y.*

Ce théorème nous dit que l'image d'un morphisme peut être décrit à l'aide d'équations algébriques, en effet tout morphisme $f : X \to Y$ est dominant quitte à le restreindre au but à $\overline{f(X)}$. Prenons U l'ouvert contenu dans $f(X)$, son complémentaire est une réunion de fermés de dimension strictement plus petite. On restreint f à chacun de ces fermés et on réapplique le théorème, on trouve que $f(X)$ est une union finie d'intersections $U \cap F$ avec U ouvert et F fermé. On dit qu'il est constructible. La preuve utilise de manière cruciale les résultants!

L'exemple canonique est l'application $f : \mathbb{C}^2 \to \mathbb{C}^2$ définie par $f(x, y) = (x, xy)$ dont l'image est la réunion de l'ouvert $\{x \neq 0\}$ et du fermé $\{(0, 0)\}$.

Théorème 8. *Soit $f : X \to Y$ un morphisme dominant entre deux variétés affines irréductibles et réduites.*

1. *Il existe un ouvert $U \subset Y$ tel que pour tout $y \in U$, toutes les composantes irréductibles de $f^{-1}(\{y\})$ sont de dimension $\dim Y - \dim X$.*
2. *L'application $x \mapsto \dim f^{-1}(\{f(x)\})$ est semi-continue supérieurement (sur X).*
3. *Si f est propre, l'application $y \mapsto \dim f^{-1}(\{y\})$ est semi-continue supérieurement (sur Y).*

Un exemple simple est donnée par un système linéaire à paramètre, i.e. on se donne $A(T) \in M_{m,n}(\mathbb{C}[T])$ et $B(T) \in \mathbb{C}[T]^m$ puis on pose

$$X = \{(x, t) \in \mathbb{C}^{n+1}, A(t)x = B(t)\}$$

et on définit $f : X \to \mathbb{C}$ par $f(x, t) = t$. La fibre $f^{-1}(\{t\})$ est alors un espace affine dont la dimension vaut $n - \operatorname{rg} A(t)$. Le rang étant semi-continu inférieurement, la dimension l'est supérieurement.

2.3 Groupes algébriques

Cours 5

2.3.1 Définition et exemples

Un groupe algébrique affine G est une variété affine munie d'une structure de groupe compatible. C'est-à-dire que $G = \operatorname{Spec}(A)$ où A est une $\mathbb{C}$-algèbre de type fini et la structure de groupe est donnée par les morphismes suivants:

unité	$e : \{pt\} \to G$	counité	$e^* : A \to \mathbb{C}$
multiplication	$G \times G \to G$	comultiplication	$m^* : A \to A \otimes A$
inversion	$i : G \to G$	coinversion	$i^* : A \to A$

Les axiomes de groupe se traduisent directement en terme des counités, comultiplication et coinversion. Par exemple, $x \cdot e = x$ pour tout $x \in G$ se traduit par $m \circ (\mathrm{Id} \times e) = \mathrm{Id}$ et donc $(\mathrm{Id} \otimes e^*) \circ m^* = \mathrm{Id}$, etc.

Intuitivement, si on pense à A comme l'algèbre des fonctions sur G on a $e^*(f) = f(e), (m^*f)(g, h) = f(gh)$ et $i^*f(g) = f(g^{-1})$.

Voyons quelques exemples:

- Le groupe additif $\mathbb{C}$, noté $\mathbb{G}_a$. On a $\mathbb{C}[\mathbb{G}_a] = \mathbb{C}[t]$ avec $e^*(t) = 0$, $m^*(t) = t \otimes 1 + 1 \otimes t$ et $i^*(t) = -t$.

- Le groupe multiplicatif $\mathbb{C}^*$, noté $\mathbb{G}_m$. On a $\mathbb{C}[\mathbb{G}_m] = \mathbb{C}[t, t^{-1}]$, $e^*(t) = 1$, $m^*(t) = t \otimes t$ et $i^*(t) = t^{-1}$.

- Le groupe SL_n est défini par $\mathbb{C}[\mathrm{SL}_n] = \mathbb{C}[x_{ij}, i, j \in \{1, \ldots, n\}]/(\det(x_{ij}) - 1)$. La counité est donnée par $e^*(x_{ij}) = \delta_{ij}$, la comultiplication par $m^* x_{ij} = \sum_k x_{ik} \otimes x_{kj}$ et $i^*(x_{ij}) = (x_{ij})^{-1}_{ij}$. On remarque que dans cette dernière formule la matrice $(x_{ij})^{-1}$ est donnée par la transposée de la comatrice, c'est donc bien une matrice à coefficients dans A.

- On définit de façon analogue les groupes classiques, GL_n, O_n, Sp_{2n} et même les groupes exceptionnels.

- Un groupe fini est aussi un groupe algébrique affine. Par exemple le groupe μ_n des racines n-ièmes de l'unité est donné par $\mathbb{C}[\mu_n] = \mathbb{C}[t]/(t^n - 1)$ avec les mêmes formules que pour $\mathbb{G}_m$.

On va montrer bientôt que tout groupe algébrique affine G est un sous-groupe affine d'un groupe linéaire GL_n.

On peut observer qu'il n'y a qu'une seule composante irréductible qui contienne e. Notons $C_1, \ldots, C_n$ l'ensemble de ces composantes ainsi que l'application produit $p : C_1 \times \cdots C_n \to G$ définie par $p(g_1, \ldots, g_n) = g_1 \cdots g_n$. Comme chaque C_i est irréductible, le produit aussi, et donc l'image de p appartient à une et une seule composante C_i. C'est impossible car $x \in C_j$ est dans l'image de p (prendre les autres variables égales à e). Il n'y a donc qu'une seule composante qu'on appelle G_0.

On vérifie facilement qu'elle forme un sous-groupe distingué fermé. La décomposition de G en classes à gauche de G_0 correspond à la décomposition en composantes irréductibles. Ainsi G/G^0 est fini. On renvoie à [**?**, **?**] pour les preuves et beaucoup d'autres choses.

2.3.2 Actions de groupes

Soit G un groupe affine et X une variété algébrique affine. Une action de G sur X est un morphisme $G \times X \to X$ satisfaisant les axiomes d'action de groupe.

En notant $\sigma : G \times X \to X$ l'application définie par $\sigma(g, x) = g^{-1}x$, l'action de G est décrite par le morphisme

$$\sigma^* : \mathbb{C}[X] \to \mathbb{C}[G] \otimes \mathbb{C}[X]$$

On peut donc écrire $\sigma^* f = \sum h_i \otimes f_i$ qui doit se comprendre comme $f(g^{-1}x) = \sum_i h_i(g) f_i(x)$. Une telle formule induit une représentation $G \to \mathrm{Aut}(\mathbb{C}[X])$ par la formule $g.f = \sum_i h_i(g) f_i$.

Considérons l'exemple où $G = \mathbb{G}_m$. Comme $\mathbb{C}[\mathbb{G}_m] = \bigoplus_{i \in \mathbb{Z}} \mathbb{C} t^i$ on a pour tout $f \in A = \mathbb{C}[X]$

$$\sigma^* f = \sum_{i \in \mathbb{Z}} t^i \otimes f_i \tag{1}$$

L'application π_i envoyant f sur f_i est un projecteur sur un sous-espace noté A_i. En effet, la formule (1) se comprend sous la forme $f(t^{-1}x) = \sum_i t^i f_i(x)$: en substituant t par ts, on trouve

$$f((ts)^{-1}x) = \sum_{i\in\mathbb{Z}} t^i \sum_{j\in\mathbb{Z}} s^j (f_i)_j.$$

En identifiant les puissances de s et t, on trouve $(f_i)_j = \delta_{ij} f_i$ ce qui montre bien que $f_i \in A_i = \{f \in A, t.f = t^i f\}$.

On a donc $A = \bigoplus_{i\in\mathbb{Z}} A_i$ avec $A_i \cdot A_j \subset A_{i+j}$ pour tout $i, j \in \mathbb{Z}$. Ainsi, A est une algèbre graduée, et réciproquement, toute algèbre graduée admet une coaction de $\mathbb{G}_m$ par la formule (1). Par exemple, à l'action de $\mathbb{G}_m$ sur $\mathbb{A}^n$ correspond la décomposition de $A = \mathbb{C}[x_1, \ldots, x_n]$ en composantes homogènes, précisément $A_{-d} = \mathbb{C}[x_1, \ldots, x_n]_d$.

On a vu que toute variété affine se plonge dans $\mathbb{A}^n$. On peut montrer un résultat analogue en ajoutant l'action d'un groupe G.

Proposition 6. *Pour tout groupe algébrique G agissant algébriquement sur une variété algébrique affine, il existe une action algébrique de G sur un espace vectoriel V et un plongement G-équivariant $i : X \to V$ i.e. vérifiant $i(gx) = gi(x)$.*

Preuve. On commence par observer une propriété très utile de la représentation régulière $G \to \operatorname{Aut} \mathbb{C}[X]$: tout élément est inclus dans un sous-espace vectoriel de dimension finie et G-invariant. En effet, on écrit $\sigma^*(f) = \sum_{i=1}^n h_i \otimes f_i$. Notons $W = \operatorname{Vect}\{f_1, \ldots, f_n\}$. On a $g.f = \sum_i h_i(g) f_i$ ainsi l'espace vectoriel $U = \operatorname{Vect}\{g.f, g \in G\}$ est G-invariant et de dimension finie car inclus dans W.

On se donne maintenant des générateurs $f_1, \ldots, f_m$ de $\mathbb{C}[X]$ et un sous-espace de dimension finie W qui soit G-invariants et qui les contienne tous. L'application $i : X \to W^*$ définie par $i(x) = (f \mapsto f(x))$ est un morphisme G-équivariant. Elle induit une surjection $\mathbb{C}[W^*] \to \mathbb{C}[X]$ puisque W contient les générateurs de X. Ainsi i est bien un plongement. □

Comme application, considérons pour un groupe affine quelconque G l'action par multiplication à gauche. Le lemme précédent permet d'identifier G à une sous-variété G-invariante d'un espace vectoriel de dimension finie V sur lequel G agit linéairement. L'action de G dans V définit un morphisme $G \to \mathrm{GL}(V)$ qui est un plongement. Ceci prouve que G est linéaire, à savoir un sous-groupe fermé de $\mathrm{GL}(V)$.

2.3.3 Adhérence des orbites

Cours 6

Définition 6. *Soit G un groupe affine agissant sur une variété affine X et x un point de X. On appelle orbite de x par l'action de G et on note $G \cdot x$ l'image du morphisme $\sigma_x : G \to X$ défini par $g \mapsto g.x$. On pose $G_x = \sigma_x^{-1}(x)$ et on l'appelle stabilisateur de x.*

Le stabilisateur G_x est un sous-groupe fermé de G, l'orbite $G \cdot x$ n'est pas forcément fermée mais on a le résultat général suivant:

Proposition 7. *Supposons que G agisse algébriquement sur une variété affine X réduite et irréductible.*

1. *Toute orbite $G \cdot x$ est ouverte dans son adhérence.*
2. *L'adhérence d'une orbite $\overline{G \cdot x}$ est la réunion de l'orbite et d'une famille finie d'orbites de dimensions strictement plus petite. En particulier, cette adhérence contient une orbite fermée.*
3. *Pour tout $x \in X$ on a $\dim G \cdot x + \dim G_x = \dim G$.*
4. *Pour tout $n \in \mathbb{N}$, l'ensemble des $x \in X$ tels que $\dim G \cdot x \leq n$ est fermé dans X.*

Preuve. On suppose que G est connexe. Le cas général est laissé en exercice.

(1) L'application $G \to \overline{G \cdot x}$ est dominante. Son image contient donc un ouvert non vide $U \subset \overline{G \cdot x}$. Comme G agit transitivement dans $G \cdot x$, on a $G \cdot x = \bigcup_{g \in G} gU$. Cette orbite est donc ouverte dans $\overline{G \cdot x}$.

(2) En remplaçant X par $\overline{G \cdot x}$, on peut supposer que $G \cdot x$ est ouvert dans X. Ainsi $X \setminus G \cdot x$ est un fermé G-stable de dimension strictement plus petite. On conclut par récurrence.

(3) Les fibres du morphisme $G \to G \cdot x$ sont les translatés de G_x. Ainsi, ils ont tous la même dimension égale à celle de G_x. On conclut par le Théorème 8.

(4) Considérons le morphisme $G \times X \to X \times X$ défini par $(g, x) \mapsto (x, gx)$. Sa fibre en (g, x) est isomorphe à G_x. D'après le théorème 8, l'ensemble des couples (g, x) tels que $\dim G_x \geq n$ est fermé dans $G \times X$ pour tout n. On conclut grâce au point précédent. $\square$

Regardons quelques exemples.

1. Si $\mathbb{C}^*$ agit sur $\mathbb{C}^n$ par multiplication, il n'y a qu'une orbite fermée $\{0\}$, toutes les autres orbites, indexées par $\mathbb{P}^{n-1}(\mathbb{C})$ lui étant adhérentes. Si on enlève $\{0\}$, toutes les orbites deviennent fermées.

2. Si $\mathrm{GL}_n(\mathbb{C})$ agit sur $\mathbb{C}^n$, il n'y a qu'une orbite fermée - $\{0\}$ - et une orbite ouverte, son complémentaire.

3. Soit $G = \mathrm{GL}_n(\mathbb{C})$ agissant sur $M_n(\mathbb{C})$ par conjugaison. Si $P \in \mathbb{C}[X]$ est un polynôme unitaire de degré n à racines simples, l'ensemble

$$\{M \in M_n(\mathbb{C}), \det(XI - M) = P(X)\}$$

est fermé et représente une classe de conjugaison. Maintenant, toute matrice M est conjuguée à une matrice par blocs de Jordan

$$J = \begin{pmatrix} \lambda & 1 & \dots & 0 \\ 0 & \lambda & \cdots & 0 \\ 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & \lambda \end{pmatrix}$$

En conjugant cette matrice par une matrice diagonale de coefficients $t^{a_1}, \dots, t^{a_n}$, on remplace le 1 en i-ème ligne par $t^{a_{i+1} - a_i}$. Si $a_{i+1} = a_i + 1$, on constate que la matrice converge vers $\lambda\,\mathrm{Id}$ à laquelle elle n'est pas conjuguée. Ainsi, l'orbite de M est fermée seulement si M est diagonalisable. On peut d'ailleurs comprendre précisément quelles orbites sont dans l'adhérence d'une matrice sous forme de Jordan: n'importe quelle matrice obtenue en remplaçant certains 1 par 0.

4. Prenons comme dernier exemple le cas des formes binaires de degré d. Une telle forme s'écrit $q = \prod_i l_i$ où chaque l_i est une forme linéaire. Le groupe $\mathrm{SL}_2(\mathbb{C})$ agit sur q par la formule

$$g.q = \prod_i g.l_i.$$

En particulier, si au moins trois de ces formes sont deux à deux linéairement indépendantes, le stabilisateur G_q est fini, et d'après le point 3 de la Proposition 7, l'orbite $G \cdot q$ est de dimension 3. Supposons donc $d \geq 3$ et prenons q à racines distinctes, i.e. $D(q) \neq 0$. Alors l'orbite $G \cdot q$ est fermée. En effet, on a $\overline{G \cdot q} \subset D^{-1}(D(q))$. Le fermé $D^{-1}(D(q))$ ne contient que des orbites de dimension 3 d'après ce qui précède. Le point 2 de la Proposition 7 implique que l'orbite de q est fermée.

3 Quotient des variétés affines

3.1 Groupes réductifs

Soit G un groupe algébrique et $\rho : G \to \mathrm{GL}(V)$ une représentation de G, éventuellement de dimension infinie.

Définition 7. *On dit que V est rationnelle si pour tout vecteur $v \in V$ il existe un sous-espace G-invariant $W \subset V$ tel que $v \in W$ et telle que le morphisme induit $G \to \mathrm{GL}(W)$ soit algébrique.*

Un exemple évident est celui d'une représentation algébrique de dimension finie $\rho : G \to \mathrm{GL}(V)$, un autre est celui de $\mathbb{C}[X]$ où X est une variété algébrique affine sur laquelle G agit algébriquement.

Définition 8. *Soit V une représentation rationnelle de G. On dit que*

1. *V est simple si V n'admet pas de sous-espace G-invariant non trivial.*
2. *V est semi-simple si, de façon équivalente, V se décompose en somme directe de représentations simples ou tout sous-espace G-invariant de V admet un supplémentaire invariant.*

Enfin, on dit que G est réductif si toute représentation rationnelle de V est semi-simple.

Commençons par un non-exemple: le groupe $\mathbb{G}_a$ n'est pas réductif, en effet, la représentation

$$\mathbb{G}_a \to \mathrm{GL}_2(\mathbb{C}),\ t \mapsto \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

admet $\mathbb{C} \times \{0\}$ comme espace invariant qui n'admet aucun supplémentaire invariant.

Sur $\mathbb{C}$, l'unique source d'exemples de tels groupes est donnée par le critère suivant.

Proposition 8. *Si G admet un sous-groupe compact K Zariski dense, alors G est réductif.*

La preuve repose sur l'existence de la mesure de Haar sur K, ce que l'on admettra. Les exemples à avoir en tête sont

1. $\mathbb{G}_m$ qui admet le sous-groupe compact $S^1 = \{e^{i\theta}, \theta \in \mathbb{R}/2\pi\mathbb{Z}\}$ avec sa mesure $d\theta$. Ce sous-groupe étant infini, il est Zariski dense.

2. $\mathrm{GL}_n(\mathbb{C})$ qui admet le sous-groupe $\mathrm{U}(n) = \{M \in M_2(\mathbb{C}), \overline{M}^T M = I_n\}$ qui est de dimension réelle n. Pour montrer qu'il est Zariski dense, on se ramène à montrer que $\mathbb{R}^n$ est Zariski dense dans $\mathbb{C}^n$.

3. $\mathrm{SL}_n(\mathbb{C})$ admet le sous-groupe $\mathrm{SU}(n)$ comme sous-groupe compact Zariski dense.

4. Tout groupes de Lie semi-simple complexe est réductif, car il est le complexifié de son compact maximal.

Preuve. Soit K le sous-groupe compact Zariski dense de G et μ la mesure de Haar de K normalisée. Notons $R : V \to V$ l'opérateur défini par $R(v) = \int_K \rho(g)(v)d\mu(g)$. On constate que $gR(v) = R(v)$: en effet c'est le cas si $g \in K$ et l'application de G dans V définie par $g.R(v) - R(v)$ étant algébrique et nulle sur K est donc identiquement nulle.

Si W est un sous-espace G-invariant de V, la donnée d'un supplémentaire invariant S est équivalente à celle d'une rétraction G-invariante r de la suite en prenant $S = \ker r$. Partons d'une rétraction quelconque $r \in \mathrm{Hom}(V, W)$. Le groupe G agit rationnellement sur $\mathrm{Hom}(V, W)$ par la formule $(g.f)(x) = gf(g^{-1}x)$, on peut donc appliquer R à r, on vérifie que l'identité $r|W = \mathrm{Id}_W$ implique $R(r)|_W = \mathrm{Id}_W$. Finalement, $R(r)$ est donc une rétraction G-équivariante et la proposition est démontrée. $\square$

Remarque 2. *Il existe toujours une et une seule projection G-invariante $R : V \to V^G$. On l'appelle l'opérateur de Reynolds. En effet, soit V un G-module rationnel et décomposons V en sous-modules simples. On aura $V = V^G \oplus \bigoplus_i V_i$ où la somme porte sur les facteurs simples non triviaux. Toute application G-invariante $p_i : V_i \to V^G$ est nulle car sinon, son noyau serait un sous-espace G-invariant non trivial, ce qui est impossible. Ainsi R est nécessairement égal à la projection de V sur V^G parallèlement à $\bigoplus_i V_i$.*

Le théorème fondamental de finitude du à Hilbert est le suivant.

Théorème 9. *Soit G un groupe réductif agissant rationnellement sur une algèbre de type fini A. Alors l'algèbre invariante A^G est de type fini, et c'est un facteur direct de A. De plus pour tout idéal I de A^G on a $AI \cap A^G = I$.*

Preuve. Soit $f \in A^G$. On a pour tout $\phi \in A$ l'égalité $R(f\phi) = fR(\phi)$ de manière évidente en pensant à la définition intégrale de R. Ainsi, le morphisme $R : A \to A^G$ est un morphisme de A^G-modules et donc A^G est un facteur direct de A.

Soit I un idéal de A^G. On a bien sûr $I \subset AI \cap A^G$. Réciproquement, si $f \in AI \cap A^G$ alors $f = \sum_i \phi_i f_i$ et

$$R(f) = f = \sum_i R(\phi_i f_i) = \sum_i R(\phi_i) f_i \in I.$$

Vérifions que A^G est noethérienne, sachant que A l'est par hypothèse. Soit I_k une suite croissante d'idéaux de A^G. La suite AI_k est une suite croissante d'idéaux de A qui doit donc se stabiliser. Comme $I_k = AI_k \cap A^G$, la suite I_k se stabilise, prouvant que A^G est noethérienne.

Soit $f_1, \ldots, f_n$ des générateurs de A. Il existe un sous-G-module rationnel W de dimension finie qui contienne $f_1, \ldots, f_n$. L'application linéaire G-équivariante $W \to A$ s'étend en un morphisme d'algèbre surjectif $\mathbb{C}[W^*] \to A$. Il suffit donc de montrer que $\mathbb{C}[V]$ est de type fini où on a posé $V = W^*$.

L'algèbre $\mathbb{C}[V]$ est naturellement graduée et on a

$$\mathbb{C}[V]^G = \bigoplus_{n=0}^{\infty} \mathbb{C}[V]_n^G.$$

Soit I l'idéal engendré par les invariants homogènes non constants. Comme $\mathbb{C}[V]$ est noethérienne, I est engendré par un nombre fini d'éléments $g_1, \ldots, g_r$ que l'on peut supposer homogènes. Si $f \in \mathbb{C}[V]_n^G$ avec $n > 0$, on aura $f = \sum_i \phi_i g_i$ avec $\phi_i \in \mathbb{C}[V]$ homogènes. On en déduit que $f = R(f) = \sum R(\phi_i) g_i$ avec $R(\phi_i)$ invariant et homogène de degré strictement inférieur à celui de f. Par récurrence sur le degré de f, on en déduit que f est un polynôme dans les g_i. □

3.2 Quotient affine

Cours 7

3.2.1 Construction

Soit X une variété affine sur laquelle agit un groupe réductif G. L'algèbre $\mathbb{C}[X]^G$ est de type fini par le théorème de Hilbert. Ainsi, la variété

$$X//G = \mathrm{Spec}(\mathbb{C}[X]^G)$$

est une variété affine, on l'appelle le quotient de X et on note $p : X \to X//G$ l'application induite par l'inclusion $\mathbb{C}[X]^G \to \mathbb{C}[X]$.

Voyons tout de suite quelques exemples élémentaires.

1. Le groupe $\mathbb{Z}/2\mathbb{Z} = \{\pm 1\}$ agit sur $\mathbb{A}$ par multiplication. Son action sur $\mathbb{C}[\mathbb{A}] = \mathbb{C}[X]$ est simplement donnée par $P(X) \mapsto P(-X)$.

   Les polynômes invariants sont les polynômes pairs: en posant $Y = X^2$ on a donc $\mathbb{C}[X]^{\mathbb{Z}/2\mathbb{Z}} = \mathbb{C}[Y]$. Ainsi on a $\mathbb{A}//(\mathbb{Z}/2\mathbb{Z}) = \mathbb{A}$ et l'application quotient est l'application $x \mapsto x^2$.

2. Faisons agir le même groupe par multiplication sur $\mathbb{A}^2$. On a $\mathbb{C}[\mathbb{A}^2] = \mathbb{C}[X, Y]$ et tout polynôme invariant est un polynôme en X^2, XY, Y^2. En notant U, V, W ces trois polynômes on se convainc qu'on a plus précisément $\mathbb{C}[X, Y]^{\mathbb{Z}/2\mathbb{Z}} = \mathbb{C}[U, V, W]/(V^2 - UW)$. Ainsi le quotient $\mathbb{A}^2//(\mathbb{Z}/2\mathbb{Z})$ est le cône de $\mathbb{A}^3$ d'équation $v^2 = uw$. Il présente en particulier une singularité en 0.

3. Faisons agir $\mathbb{G}_m$ sur $\mathbb{A}^2$ par $t.(x, y) = (tx, t^{-1}y)$. On a alors $\mathbb{C}[X, Y]^{\mathbb{G}_m} = \mathbb{C}[XY]$ et le quotient est simplement $\mathbb{A}$.

Il est clair que p est G-invariante et universelle pour cette propriété au sens où tout morphisme G-invariant $f : X \to Y$ vers une variété affine se factorise par p (on dit que c'est un quotient catégorique). Ecrivons le diagramme pour marquer le coup:

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "p"'] & & Y \\ & X//G \arrow[ur, dashed] & \end{tikzcd}$$

On peut montrer d'autres propriétés de p.

Théorème 10. *Soit G un groupe réductif agissant sur une variété affine X.*

1. *Le morphisme $p : X \to X//G$ est surjectif.*

2. *Si $Z \subset X$ est un fermé G-invariant, son image $p(Z)$ est fermée et la restriction $p|_Z : Z \to p(Z)$ est le quotient de Z par G.*

3. *Si Z_1 et Z_2 sont deux fermés G-invariants alors $p(Z_1 \cap Z_2) = p(Z_1) \cap p(Z_2)$.*

4. *Si $x \in X$, la fibre $p^{-1}(p(x))$ contient une unique orbite fermée, notée $\mathcal{O}_x$. De plus $p^{-1}(p(x))$ est l'ensemble des points z tels que $\mathcal{O}_x \subset \overline{G \cdot z}$.*

Preuve. (1) Soit x un point de $X//G$ et I_x l'idéal maximal correspondant dans $\mathbb{C}[X]^G$. D'après le Théorème 9, on a $\mathbb{C}[X]I_x \cap \mathbb{C}[X]^G = I_x$. En particulier, $\mathbb{C}[X]I_x$ n'est pas égal à $\mathbb{C}[X]$ et il existe donc un idéal maximal $\mathbb{C}[X]I_x \subset I_y \subset \mathbb{C}[X]$. On aura alors $p(y) = x$.

(2) L'application $\mathbb{C}[X] \to \mathbb{C}[Z]$ est surjective. Il en est donc de même de l'application $\mathbb{C}[X]^G \to \mathbb{C}[Z]^G$. Ainsi le deuxième point est montré. On a même que l'idéal définissant $p(Z)$ est $I \cap \mathbb{C}[X]^G = I^G$ où I est l'idéal définissant Z.

(3) Soit I_1 et I_2 les idéaux associés à Z_1 et Z_2. L'idéal associé à $p(Z_1 \cap Z_2)$ est $(I_1 + I_2)^G = I_1^G + I_2^G$. On reconnaît l'idéal associé à l'intersection de $p(Z_1)$ et $p(Z_2)$. Précisons l'égalité $(I_1 + I_2)^G = I_1^G + I_2^G$: pour tout $f = f_1 + f_2 \in (I_1 + I_2)^G$ on a $f = R(f) = R(f_1) + R(f_2)$. On conclut en observant que R stabilise I_1 et I_2.

(4) Puisque $p^{-1}(p(x))$ est un fermé G-invariant, il contient une orbite fermée. D'après le point (3), deux fermés G-invariants disjoints ont des images disjointes,

ainsi il ne peut y avoir deux orbites fermées dans $p^{-1}(p(x))$. Si l'adhérence de $G \cdot z$ contient $\mathcal{O}_x$ alors $p(z) = p(x)$. Réciproquement, si $p(z) = p(x)$ alors $\overline{G \cdot z}$ contient une orbite fermée qui ne peut être que celle associée à x. $\square$

3.2.2 Stabilité

On vient donc de construire un quotient avec d'excellentes propriétés et ceci dans une grande généralité. Pour autant, le quotient peut être très dégénéré comme le montrent les exemples de la Section 7. Le quotient se comportera mieux si on se restreint au lieu stable.

Définition 9. *Soit G un groupe réductif agissant sur X affine. On dit que $x \in X$ est stable si l'orbite $G \cdot x$ est fermée et le stabilisateur G_x est fini.*

Si x est stable, on a nécessairement $p^{-1}(p(x)) = G \cdot x$. On en déduit la proposition suivante:

Proposition 9. *L'ensemble X_s est un ouvert G-invariant de X (peut-être vide) et la restriction $p : X^s \to p(X^s)$ s'identifie au quotient topologique.*

Preuve. La seule chose qui n'est pas claire, c'est que le lieu stable soit ouvert. Cependant, d'après les points (3) et (4) de la Proposition 7 et le fait que G_x est fini si et seulement si sa dimension est nulle, on sait que le lieu $Y = \{x \in X, \dim G_x > 0\}$ est fermé dans X et G-invariant.

Soit x un point stable. Comme $G \cdot x$ et Y sont des fermés G-invariants disjoints, il existe $f \in \mathbb{C}[X]^G$ tel que $f|_Y$ soit nulle et $f(x) \neq 0$. Alors l'ouvert $X_f = \{x \in X, f(x) \neq 0\}$ contient x. Montrons que tout point y de X_f est stable. Par construction G_y est fini et donc toutes les orbites dans X_f sont de dimension égale à celle de G. Si $G \cdot y$ n'est pas fermée, il existe un point z adhérent à $G \cdot y$ dont l'orbite est de dimension strictement plus petite que celle de y. Mais comme z est adhérent à l'orbite de y, $f(z) \neq 0$ et on a une contradiction. Ainsi x appartient à l'ouvert X_f qui est entièrement contenu dans le lieu stable. $\square$

3.2.3 Normalité

Cours 8

Soit A un anneau intègre et K son corps des fractions. On dit que A est normal si tout élément de K entier sur A, c'est-à-dire racine d'un polynôme unitaire à coefficients dans A, est en fait dans A.

On constate par exemple que si A est factoriel, alors A est normal. En effet, posons $x = \frac{a}{b}$ avec a et b premiers entre eux et supposons qu'on ait $x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0$. En multipliant par b^n on trouve

$$a^n + b(c_{n-1}a^{n-1} + \cdots + c_0 b^{n-1}) = 0$$

Ainsi b divise a^n ce qui est impossible à moins que b soit inversible, auquel cas $x \in A$.

On rappelle la notion de localisation: soit $S \subset A \setminus \{0\}$ une partie multiplicative, avec A intègre pour simplifier. On note $A_S \subset K$ le sous-anneau formé des fractions $\frac{f}{s}$ avec $f \in A$ et $s \in S$.

Alors si A est normal, A_S aussi en effet, si x est solution d'un polynôme unitaire à coefficients dans A_S, on peut chasser les dénominateurs et conclure qu'il existe $s \in S$ tel que sx soit solution d'un polynôme unitaire à coefficients dans A. Par normalité de A, on a $sx \in A$ puis $x \in A_S$.

On a en fait la caractérisation suivante liée aux idéaux premiers $\mathcal{P}$ de hauteur 1, i.e minimal parmi les idéaux non nuls. A de tels idéaux correspondent des sous-variétés fermées irréductibles $D = V(\mathcal{P})$ de codimension 1, que l'on appelle diviseurs. L'anneau $A_{\mathcal{P}}$ est par définition le localisé de A en $A \setminus \mathcal{P}$. C'est un anneau local au sens où il a un unique idéal maximal, noté $\mathcal{P}A_{\mathcal{P}}$. Intuitivement, $A_{\mathcal{P}}$ est l'anneau des fonctions rationnelles f qui sont définies en au moins un point de D tandis que $\mathcal{P}A_{\mathcal{P}}$ est le sous-anneau des fonctions qui s'annulent sur D.

Proposition 10. *Soit A une $\mathbb{C}$-algèbre intègre de type fini. Alors A est normale ssi*

1. *Pour tout idéal premier $\mathcal{P}$ de hauteur 1, l'anneau local $A_{\mathcal{P}}$ est principal (anneau de valuation discrète).*
2. *On a $A = \bigcap_{ht(\mathcal{P})=1} A_{\mathcal{P}}$.*

Bien sûr, on dira qu'une variété X affine, irréductible et réduite est normale si $\mathbb{C}[X]$ l'est. On peut toujours considérer la clôture intégrale de $\mathbb{C}[X]$ dans $\mathbb{C}(X)$, à savoir l'algèbre des fractions qui sont solutions d'une équation polynômiale unitaire à coefficients dans $\mathbb{C}[X]$. Cette algèbre est encore de type fini, donc de la forme $\mathbb{C}[\tilde{X}]$ pour une certaine variété $\tilde{X}$ munie d'une application dominante $\pi : \tilde{X} \to X$. La variété $\tilde{X}$ est par construction normale, on peut y penser comme une désingularisation de X.

Géométriquement, la proposition précédente nous dit qu'une fonction f algébrique qui n'est pas inversible doit s'annuler le long d'un diviseur, en effet sinon $\frac{1}{f}$ serait dans l'intersection de tous les $A_{\mathcal{P}}$, d'où $f \in A^{\times}$.

Proposition 11. *Soit G un groupe réductif agissant sur une variété normale X. Alors*

1. *Le quotient $X//G$ est normal.*
2. *Si $\pi : X \to Y$ est un morphisme G-invariant avec Y normal tel que les fibres générales ont une unique orbite fermée et tel que l'image de π rencontre tout diviseur de Y alors Y est isomorphe au quotient algébrique.*

Preuve. (1) On a les inclusions suivantes

$$\begin{tikzcd}
\mathbb{C}[X]^G \arrow[r] \arrow[d] & \mathbb{C}[X] \arrow[d] \\
\mathbb{C}(X//G) \arrow[r] & \mathbb{C}(X).
\end{tikzcd}$$

Si $f \in \mathbb{C}(X//G) = \mathrm{Frac}(\mathbb{C}[X]^G)$ est entière sur $\mathbb{C}[X]^G$, elle est entière sur $\mathbb{C}[X]$, donc dans $\mathbb{C}[X]$. Etant aussi G-invariante, elle est dans $\mathbb{C}[X]^G$ ainsi $X//G$ est normal.

(2) Le morphisme $\pi : X \to Y$ induit un unique morphisme $f : X//G \to Y$ qui vérifie $p = f \circ \pi$. Soit $y \in Y$ telle que $\pi^{-1}(y)$ contienne une unique orbite fermée. Il lui correspond un unique point $x \in X//G$ tel que $f(x) = y$. Ainsi f est bijective sur un ouvert (on dit birationnelle). On conclut avec le lemme ci-dessous. □

Lemme 1. *Soit $f : X \to Y$ un morphisme birationnel entre deux variétés irréductibles et réduites avec Y normal et tel que l'image de f rencontre tout diviseur de Y. Alors f est un isomorphisme.*

Preuve. Considérons le morphisme $f^* : \mathbb{C}[Y] \to \mathbb{C}[X]$. Comme f est bijective sur un ouvert, f est dominante, donc f^* est injective. Montrons que f^* induit un isomorphisme $f^* : \mathbb{C}(Y) \to \mathbb{C}(X)$. D'après le théorème sur les fibres d'un morphisme, on observe que X et Y ont la même dimension, et donc f^* est une extension finie. Son degré est précisément le nombre de préimages d'un point générique, ici 1.

Comme Y est normale, l'algèbre $\mathbb{C}[Y]$ s'identifie à l'intersection des sous-anneaux locaux $\mathcal{O}_{Y,D}$ où D parcourt les diviseurs irréductibles de Y. Rappelons que $\mathcal{O}_{Y,D}$ est l'anneau des fonctions de $\mathbb{C}(Y)$ qui sont définies en au moins un point de D. Soit $\phi \in \mathbb{C}[X]$: il existe $\psi \in \mathbb{C}(Y)$ telle que $\phi = \psi \circ f$. L'application ψ est donc définie sur l'image de f: comme cette image rencontre tout diviseur, $psi \in \mathcal{O}_{Y,D}$ pour tout D. Ainsi $\psi \in \mathbb{C}[Y]$ et f^* induit un isomorphisme. □

3.3 Exemples

3.3.1 Classes de conjugaison

Considérons à nouveau l'action de $G = \mathrm{GL}_n(\mathbb{C})$ par conjugaison sur $M_n(\mathbb{C})$. Les coefficients du polynôme caractéristique

$$\det(X\,\mathrm{Id} - M) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

définissent un morphisme G-invariant et surjectif $\pi : M_n(\mathbb{C}) \to \mathbb{A}^n$. Une fibre générale correspond à la classe de conjugaison d'une matrice à valeurs propres distinctes qui est fermée (cf Section 2.3.2). Comme $\mathbb{A}^n$ est normale, la Proposition 11 implique que $\mathbb{A}^n$ est bien le quotient algébrique.

3.3.2 Formes binaires

Soit V le dual de $\mathbb{C}^2$. On rappelle que $S^dV = \mathbb{C}[X,Y]_d$ s'identifie à l'espace des formes binaires de degré d, muni de l'action algébrique de $\mathrm{SL}_2(\mathbb{C})$. Revenons à l'étude du quotient $S^dV /\!/ \mathrm{SL}_2(\mathbb{C})$.

Considérons l'application

$$\Phi : \begin{cases} V^d \to S^dV \\ (l_1, \ldots, l_d) \mapsto \prod_i l_i \end{cases}$$

Posons $T_d = \{(t_1, \ldots, t_d) \in \mathbb{G}_m^d, \prod_i t_i = 1\}$. Ce groupe agit par multiplication sur V^d de sorte que Φ soit T_d-invariante, de même le groupe symétrique S_d. Ainsi, le groupe $\Gamma_d = T_d \rtimes S_d$ agit sur V^d en laissant Φ invariante.

Toute forme q de degré d non nulle s'écrit comme un produit de d-formes linéaires, uniquement définies à permutation et normalisation près. Le critère s'applique une nouvelle fois, montrant que Φ induit un isomorphisme $V^d /\!/ \Gamma_d \to S^dV$. En termes d'algèbre de fonctions, on a:

$$\Phi^* : \mathbb{C}[S^dV] \xrightarrow{\sim} \mathbb{C}[V^d]^{\Gamma_d}.$$

Cet isomorphisme préservant les degrés, on a pour tout n un isomorphisme

$$\mathbb{C}[S^dV]_n \to \mathbb{C}[V^d]_{n\times d}^{\Gamma_d}.$$

Ici, $\mathbb{C}[V^d]_{n\times d}^{T_d}$ désigne l'espace des fonctions polynomiales sur V^d qui sont homogènes de degré n sur chaque facteur. Autrement dit, $\mathbb{C}[V^d]_{n\times d}^{T_d} \simeq (S^nV)^{\otimes d}$. Considérant la partie symétrique, on obtient finalement la loi de réciprocité d'Hermite:

Proposition 12. *L'application naturelle ci-dessous est un isomorphisme de* $\mathrm{SL}_2(\mathbb{C})$*-modules*

$$\mathbb{C}[S^dV]_n \to \mathbb{C}[S^nV]_d.$$

On en déduit en particulier qu'il y a autant d'invariants de degré n des formes de degré d que d'invariants de degré d des formes de degré n. Par exemple, il y a un invariant de degré 3 des formes quartiques (J) et un invariant de degré 4 des formes cubiques (D). Autre exemple: comme il y a un seul invariant de degré $2d$ des formes binaires quadratiques et aucun de degré impair, il y a un seul invariant de degré 2 des formes paires (par exemple I) et aucun des formes impaires.

3.3.3 Les d-uplets de vecteurs

L'exemple précédent nous amène naturellement à étudier le quotient de V^d par $\mathrm{SL}_2(\mathbb{C})$. Considérons l'application $\mathrm{SL}_2(\mathbb{C})$-invariante suivante:

$$\begin{array}{lll} \Psi & : V^d & \to \mathbb{C}^{\frac{d(d-1)}{2}} \\ & (l_1, \ldots, l_d) & \mapsto (\det(l_i, l_j))_{i<j} \end{array}$$

Si on considère 4 formes l_1, l_2, l_3, l_4, elles sont linéairement dépendantes, donc le déterminant de la matrice $(\det(l_i, l_j))_{i,j=1,\ldots,4}$ s'annule. Cette matrice est antisymétrique, et son déterminant est le carré de son Pfaffien

$$\mathrm{Pfaff}(\det(l_i, l_j)) = \det(l_1, l_2)\det(l_3, l_4) - \det(l_1, l_3)\det(l_2, l_4) + \det(l_2, l_3)\det(l_1, l_4)$$

On en déduit que Ψ prend ses valeurs dans la sous-variété Y_d de $\mathbb{C}^{\frac{d(d-1)}{2}}$ définie par les équations de Plücker

$$a_{ij}a_{kl} - a_{ik}a_{jl} + a_{il}a_{jk} = 0.$$

Si on se donne un élément $a = (a_{ij})$ non nul de Y_d - supposons par exemple qu'on a $a_{12} = 1$. On se propose de décrire la fibre $p^{-1}(a)$: on pose tout d'abord $l_1 = (1, 0)$ et $l_2 = (0, 1)$. Ensuite, pour tout $i > 1$ on doit avoir $\det(l_1, l_i) = a_{1i}$ et $\det(l_2, l_i) = a_{2i}$ donc on pose $l_i = (-a_{2i}, a_{1i})$. On vérifie aisément que $a = \Psi(l_1, \ldots, l_n)$: ainsi $\Psi^{-1}(a)$ consiste en une unique orbite de $\mathrm{SL}_2(\mathbb{C})$. On peut conclure en utilisant le critère pourvu qu'on ait montré que Y_d est une variété normale.

On déduit de ce résultat que tout invariant de degré n des formes binaires de degré d s'écrit comme un polynôme dans les variables a_{ij} $i, j \in \{1, \ldots, d\}$ dans lequel chaque variable i apparaît n fois, et invariant par permutation des variables.

1. Cas $d = 2$. La variable a_{12} est antisymétrique, son carré a_{12}^2 est le générateur de $\mathbb{C}[V^2]^{\mathrm{SL}_2 \times \Gamma_2}$. Il s'agit du discriminant des formes quadratiques.

2. Cas $d = 3$. On a $\mathbb{C}[V^3]^{\mathrm{SL}_2} = \mathbb{C}[a_{12}, a_{23}, a_{13}]$. Les invariants pour T_3 sont engendrés par $a_{12}a_{23}a_{13}$ qui est antisymétrique. Ainsi, l'unique invariant est $a_{12}^2 a_{23}^2 a_{13}^2$ qui correspond au discriminant des formes cubiques.

3. Cas $d = 4$. L'algèbre $\mathbb{C}[V^4]^{\mathrm{SL}_2 \times T_4}$ est engendrée par $x = a_{12}a_{34}, y = -a_{13}a_{24}, z = a_{14}a_{23}$ avec la relation $x + y + z = 0$. On prouve que les deux quantités $I = x^2 + y^2 + z^2$ et $J = x^3 + y^3 + z^3$ identifient le quotient à $\mathbb{C}^2$. On retrouve ainsi les deux invariants fondamentaux des formes binaires quartiques.

4. Cas $d = 5$. C'est nettement plus compliqué mais c'est encore possible. Le calcul complet a été fait par Hermite [?],Première Partie, §IV-VII.

3.4 Le critère de Hilbert-Mumford

On a pu voir l'importance des orbites fermées, ce sont celles qui se comportent bien dans le quotient. Il est difficile en général de déterminer si l'orbite d'un point x dans une variété algébrique affine X sur laquelle G agit est fermée: le critère ci-dessous montre qu'on peut se ramener aux sous-groupes de G à un paramètre, c'est-à-dire aux images des morphismes $\lambda : \mathbb{G}_m \to G$.

On commence par étudier de manière plus systématique les actions de tores $T \simeq (\mathbb{G}_m)^n$. On note $X^*(T)$ le groupe des morphisme algébriques $\chi : T \to \mathbb{G}_m$ (caractères) et $X_*(T)$ le groupe des morphismes $\lambda : \mathbb{G}_m \to T$ (sous-groupes à un paramètre).

Proposition 13. *1. Tout caractère multiplicatif $\chi \in X^*(T)$ s'écrit de la forme $\chi(t_1, \dots, t_n) = t_1^{a_1} \cdots t_n^{a_n}$ pour un unique vecteur $(a_1, \dots, a_n) \in \mathbb{Z}^n$.*

2. *Tout sous-groupe à un paramètre $\lambda \in X_*(T)$ s'écrit de la forme $\lambda(t) = (t^{b_1}, \dots, t^{b_n})$ pour un unique vecteur $(b_1, \dots, b_n) \in \mathbb{Z}^n$.*

3. *Pour tous $(\chi, \lambda) \in X^*(T) \times X_*(T)$ on a $\chi(\lambda(t)) = t^{\langle \chi, \lambda \rangle}$ et la forme bilinéaire $\langle \cdot, \cdot \rangle$ est non-dégénérée.*

4. *Tout T-module rationnel V est somme directe des sous-modules*

$$V_\chi = \{v \in V, t.v = \chi(t)v\}$$

où χ parcourt $X^*(T)$.

Soit V un T-module rationnel et $v \in V$. On note $v = \sum_\chi v_\chi$ la décomposition précédente et on pose $\chi(v) = \{\chi \in X^*(T), v_\chi \neq 0\}$. On note $C(v)$ le cône convexe engendré par $\chi(v)$ dans $X^*(T)_\mathbb{R} \simeq \mathbb{R}^n$. Pour chaque face F de $C(v)$, on note $\mathcal{O}_F$ l'orbite par T du vecteur

$$v_F = \sum_{\chi \in \chi(v) \cap F} v_\chi.$$

On rappelle qu'une face de $C(v)$ est par définition l'intersection $C(v) \cap \{f = 0\}$ où f est une forme linéaire vérifiant $f(x) \geq 0$ pout tout $x \in C(v)$.

Proposition 14. *L'application $F \mapsto \mathcal{O}_F$ est une bijection entre les faces de $C(v)$ et l'ensemble des T-orbites dans $\overline{Tv}$. De plus, pour deux faces arbitraires F et F', on a $F \subset F'$ si et seulement si $\mathcal{O}_F \subset \overline{\mathcal{O}_{F'}}$.*

Preuve. L'application $f : T \to V$ qui envoie t sur tv induit le morphisme $f^* : \mathbb{C}[V] \to \mathbb{C}[T]$ défini par $f^*P(t) = P(tv)$. Comme $v = \sum_{\chi \in \chi(v)} v_\chi$, on a $t.v = \sum_{\chi \in \chi(v)} \chi(t) v_\chi$. On en déduit que l'image de f^* est engendrée par les caractères $\chi \in \chi(v)$. Géométriquement, cette algèbre est l'algèbre des fonctions sur $X = \overline{Tv}$. L'application dominante $T \to X$ qui envoie t sur tv induit un morphisme injectif T-équivariant $\mathbb{C}[X] \to \mathbb{C}[T]$. Or, on a la décomposition $\mathbb{C}[T] = \bigoplus_{\chi \in X^*(T)} \mathbb{C}\chi$. Ainsi, $\mathbb{C}[X]$ doit se décomposer comme une somme

$$\mathbb{C}[X] = \bigoplus_{\chi \in S} \mathbb{C}\chi$$

où S est un semi-groupe de $X^*(T)$. D'après la remarque initiale, S est engendré par les éléments de $\chi(v)$.

Si $Y \subset X$ est une sous-variété fermée irréductible et stable par T, il lui correspond un idéal premier T-invariant $I \subset \mathbb{C}[X]$. On peut alors l'écrire

$$I = \bigoplus_{\chi \in S_I} \mathbb{C}\chi$$

avec $S_I \subset S$ un sous-ensemble S-invariant vérifiant pour tout $\alpha, \beta \in S$: $\alpha + \beta \in S_I \iff \alpha \in S_I$ ou $\beta \in S_I$.

On se convainc qu'un tel sous-ensemble S_I est associé à une unique face F de $C(v)$ tel que $\chi \in S_I \iff \chi \in S \setminus F$.

Montrons que $Y = \overline{\mathcal{O}_F}$. Puisque F est une face de $C(v)$, il existe une forme linéaire λ sur $X^*(T)_\mathbb{R}$ nulle sur F et positive sur $C(v)$. Comme $C(v)$ est engendrée par des points de $X^*(T)$, on peut choisir λ dans le réseau dual $X_*(T)$. Ainsi, pour tout $f \in \mathbb{C}[X]$ et pour tout $x \in X$, la fonction $f(\lambda(t)x)$ est un polynôme de Laurent à exposants positifs, ainsi la limite $\lim_{t \mapsto 0} f(\lambda(t)x)$ existe. Finalement, la limite $\lim_{t \to 0} \lambda(t).x$ existe et est dans Y. L'application

$$\begin{array}{ccc} X & \to & Y \\ x & \mapsto & \lim\limits_{t \to 0} \lambda(t)x \end{array}$$

est un morphisme surjectif et T-équivariant. Il envoie v sur v_F, d'où l'assertion. On a prouvé que toute sous-variété irréductible fermée et T-invariante de X était de la forme $\overline{\mathcal{O}_F}$. De plus, si F' est une sous-face de F alors on a $I \subset I'$ et $\mathcal{O}_{F'} \subset \overline{\mathcal{O}_F}$ comme annoncé. □

Théorème 11. *Soit G un groupe algébrique opérant sur une variété affine X et x un point de X. Notons $\mathcal{O}$ l'unique orbite fermée adhérente à $G \cdot x$. Alors il existe un sous-groupe à un paramètre λ de G tel que la limite $\lim_{t \to 0} \lambda(t)x$ existe et est dans $\mathcal{O}$.*

Preuve. **Première étape:** On suppose que G est un tore T. On peut aussi supposer que X est une sous-variété fermée d'un espace vectoriel V sur lequel T agit rationnellement. On peut donc appliquer la Proposition 14. Le point $x \in X$ correspond au vecteur $v \in V$, les T-orbites contenues dans $\overline{Tv}$ correspondent aux faces F de $C(v)$. Il y a une unique face minimale de $C(v)$ qui est décrite par une forme linéaire $\lambda \in X_*(T)$. Elle vérifie bien l'énoncé du théorème.

Deuxième étape: Utilisons la décomposition de Cartan $G = KTK$ où K est un sous-groupe compact maximal de G et T est le complexifié d'un tore maximal de K (dans le cas $G = \mathrm{GL}_n(\mathbb{C})$, on peut prendre $K = U(n)$ et T le sous-groupe des matrices diagonales). On munit aussi V d'un produit scalaire K-invariant. S'il existe $g \in G$ tel que $\overline{Tgx}$ rencontre $\mathcal{O}$ alors, d'après la première étape, il existera un sous-groupe à un paramètre λ de T tel que $\lim_{t \to 0} \lambda(t)gx$ existe et appartient à $\mathcal{O}$. En appliquant g^{-1}, on trouve que le sous-groupe à un paramètre $g^{-1}\lambda g$ répond à la question.

Supposons donc par l'absurde que pour tout g, on a $\overline{Tgx} \cap \mathcal{O} = \emptyset$. Posons $y = gx$. Les deux ensembles $\overline{Tgx}$ et $\mathcal{O}$ sont des fermés T-invariants. Donc d'après le Théorème 10, il existe une fonction $f_y \in \mathbb{C}[X]^T$ telle que $f_y(y) = 1$ et $f_y(z) = 0$ pour tout $z \in \mathcal{O}$.

Notons $U_y = \{z \in X, f_y(z) \neq 0\}$ et recouvrons Kx avec un nombre fini d'entre eux. On a

$$Kx \subset \bigcup_{i=1}^{n} U_{y_i}.$$

La fonction $F = \sum_i |f_{y_i}|$ est continue, T-invariante, nulle sur $\mathcal{O}$ et supérieure à ϵ sur Kx. On aura donc

$$F(z) \geq \epsilon \text{ pour tout } z \in \overline{TKx}.$$

Mais comme K est compact, on a $K\overline{TKx} = \overline{KTKx} = \overline{Gx}$ qui rencontre $\mathcal{O}$ par hypothèse, une contradiction. □

Ce théorème permet de décider quelles sont les points stables d'une action.

Corollaire 1. *Soit G un groupe réductif agissant sur une variété affine X. Alors $x \in X$ est stable si et seulement si pour tout sous-groupe à un paramètre non trivial $\lambda : \mathbb{G}_m \to G$ l'application $t \mapsto \lambda(t)x$ n'a pas de limite quand $t \mapsto 0$.*

Preuve. Supposons x stable, c'est-à-dire que Gx est fermée et G_x est fini. Si on a $\lim_{t\to 0} \lambda(t)x = y$, alors $y \in Gx$ et λ stabilise y, contredisant l'hypothèse. Réciproquement, d'après le critère de Hilbert-Mumford, l'orbite Gx est fermée. Si G_x était infini, il contiendrait un sous-groupe à un paramètre, contredisant l'hypothèse. □

3.5 Applications du critère

Supposons que G agisse rationnellement sur un espace vectoriel V.

Définition 10. *On appelle nilcône de V l'ensemble $\mathcal{N}(V) = p^{-1}(p(0))$ où $p : V \to V//G$ est l'application quotient.*

Les éléments de $\mathcal{V}$ seront dits instables. On a de ces éléments les caractérisations suivantes:

$$\mathcal{N}(V) = \{v \in V, 0 \in \overline{Gv}\} = \{v \in V, \exists \lambda : \mathbb{C}^* \to G, \lim_{t\to 0} \lambda(t)v = 0\}.$$

On a montré dans la Section **??** qu'une quartique q était instable si et seulement si elle avait une racine triple.

On peut grâce au critère de Hilbert-Mumford retrouver et généraliser ce résultat. Soit q une forme binaire de degré d instable. Alors il existe un sous-groupe à un paramètre $\lambda : \mathbb{C}^* \to \mathrm{SL}_2(\mathbb{C})$ tel que $\lim_{t\to 0} \lambda(t)q = 0$.

Dans une base adaptée, on a $\lambda(t) = \begin{pmatrix} t^n & 0 \\ 0 & t^{-n} \end{pmatrix}$. On peut même supposer que l'on a $n = 1$ ci-dessous. Si on écrit $q = \sum_{i=0}^{d} a_i x^i y^{n-i}$ dans cette base, on aura $\lambda(t).q = \sum_{i=0}^{d} a_i t^{n-2i} x^i y^{n-2i}$. Ainsi:

$$\lim_{t\to 0} \lambda(t)q = 0 \iff \forall i > \frac{d}{2},\, a_i = 0 \iff q \text{ a une racine de multiplicité } > \frac{d}{2}$$

De même, on obtient que q est stable si et seulement si toutes ses racines ont multiplicité $< \frac{d}{2}$.

Reprenons maintenant l'exemple des formes cubiques ternaires. On a admis que le quotient $S^3V/\!/\operatorname{SL}_3$ est décrit par les deux invariants d'Aronhold S et T. Ainsi, le nilcône est l'ensemble des formes q telles que $S(q) = T(q) = 0$. C'est aussi celles qui vérifient $\lim_{t\to 0}\lambda(t)q = 0$ pour un sous-groupe à un paramètre λ dans $\mathrm{SL}_3(\mathbb{C})$. On sait que de telles formes doivent être singulières puisqu'une forme non-singulière vérifie $\Delta(q) \neq 0$ où Δ est le discriminant.

Dans une base adapté, ce sous-groupe s'écrit

$$\lambda(t) = \begin{pmatrix} t^a & 0 & 0 \\ 0 & t^b & 0 \\ 0 & 0 & t^c \end{pmatrix}$$

avec a, b, c des entiers vérifiant $a+b+c = 0$. Les seuls monômes $x^iy^jz^k$ pouvant intervenir dans q doivent satisfaire $ai+bj+ck > 0$. Dans la figure 1, on place les monômes dans le plan affine d'équation $i+j+k = 3$. L'équation $ai+bj+kc = 0$ définit une droite qui passe par le monôme xyz. Quitte à changer les coordonnées x, y, z, on constate qu'une forme est instable si et seulement si elle s'écrit

$$q(x, y, z) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2z$$

pour certains complexes a, b, c, d, e.

Figure 1: Cubiques instables

La courbe algébrique $C(q)$ associée présente les singularités suivantes

- Si $e \neq 0$ $d \neq 0$, alors $C(q)$ a un point de rebroussement de coordonnée $[0, 0, 1]$ et de tangente $x = 0$.
- Si $e \neq 0, d = 0, c \neq 0$, alors $C(q)$ est la réunion de la conique $ax^2 + bxy + cy^2 + exz = 0$ et de sa tangente $x = 0$.
- Si $c = d = 0$ ou si $e = 0$, alors $C(q)$ est réunion de trois droites concourantes, éventuellement confondues.

On appelle semi-stable toute orbite non instable. Il nous reste les possibilités suivantes

- une cubique non-singulière.
- SS1: une cubique nodale irréductible, $xyz + x^3 + y^3 = 0$
- SS2: a réunion d'une conique et d'une droite non tangente, $xyz + x^3 = 0$
- SS3: la réunion de trois droites non concourantes $xyz = 0$.

Le premier cas est stable comme vu précédemment. Dans chacun des cas suivants, on constate que toute forme q dans le cas considéré est équivalente à l'exemple joint. De plus, le sous-groupe $\lambda(t) = (1, t, t^{-1})$ préserve la courbe $SS2$ tandis que les matrices diagonales préservent $SS3$. On en déduit que les orbites correspondantes ont dimension au plus 7 et 6 respectivement. On constante qu'on peut faire dégénérer $SS1$ en $SS2$ puis en $SS3$. Ainsi, l'orbite de $SS1$ contient l'orbite de $SS2$ dans son adhérence qui contient l'orbite de $SS3$ dans son adhérence. A elles trois, elle forment donc une seule fibre du quotient, et $SS3$ en est le représentant d'orbite fermée.

Variétés de caractères

Soit Γ un groupe de type fini et $R(\Gamma) = \mathrm{Hom}(\Gamma, \mathrm{GL}_n(\mathbb{C}))$ la variété des représentations de Γ dans $\mathrm{GL}_n(\mathbb{C})$. C'est une variété algébrique affine que l'on peut voir comme sous-variété de $\mathrm{GL}_n(\mathbb{C})^k$ par l'application $\rho \mapsto (\rho(\gamma_1), \ldots, \rho(\gamma_k))$ où $\gamma_1, \ldots, \gamma_k$ sont des générateurs de Γ. Faisons agir $\mathrm{SL}_n(\mathbb{C})$ par conjugaison sur $R(\Gamma)$ et notons $X(\Gamma) = R(\Gamma) /\!/ \mathrm{GL}_n(\mathbb{C})$ le quotient algébrique.

Proposition 15. *Une représentation $\rho \in R(\Gamma)$ est stable si et seulement si elle est irréductible.*

Preuve. D'après le critère de Hilbert-Mumford, si ρ n'est pas stable, il existe $\lambda : \mathbb{C}^* \to \mathrm{SL}_n(\mathbb{C})$ un sous-groupe à un paramètre non trivial tel que $\lambda(t)\rho\lambda(t)^{-1}$ converge quand $t \to 0$. On peut écrire $\lambda(t)$ comme une matrice diagonale d'entrées $t^{a_1}, \ldots, t^{a_n}$ avec $a_1 \leq \cdots \leq a_n$. La conjugaison par λ multiplie le coefficient de ρ d'indice (i, j) par $t^{a_i - a_j}$. Ainsi la convergence en $t = 0$ force ρ à être triangulaire par blocs et donc réductible. ☐

On peut montrer qu'une représentation sera d'orbite fermée si et seulement si elle est somme directe de représentations irréductibles. Citons le théorème suivant de Procesi [?] dans l'esprit de la théorie classique des invariants.

Théorème 12.

1. *L'algèbre des invariants $\mathbb{C}[X(\Gamma)] = \mathbb{C}[R(\Gamma)]^{\mathrm{SL}_n(\mathbb{C})}$ est engendrée par les fonctions traces $t_\gamma(\rho) = \mathrm{tr}(\rho(\gamma))$ pour tout $\gamma \in \Gamma$.*

2. *Par les formules de Newton, les coefficients a_i du polynôme caractéristique $\det(M - \lambda \,\mathrm{Id}) = \sum_{i=0}^n a_i(M)\lambda^i$ peuvent s'exprimer comme des polynômes $F_i(\mathrm{Tr}\, M, \ldots, \mathrm{Tr}\, M^n)$. De même il existe un polynôme F tel que $\mathrm{Tr}\, M^{n+1} = F(\mathrm{Tr}\, M, \ldots, \mathrm{Tr}\, M^n)$.*

   Alors $\mathbb{C}[X(\Gamma)] = \mathbb{C}[t_\gamma, \gamma \in \Gamma]/I$ où I est l'idéal engendré par les relations $\sum F_i(t_{\gamma^i})t_{\gamma^i}$ et $t_{\gamma^{n+1}} - F(t_\gamma, \ldots, t_{\gamma^n})$.

Citant Procesi, toutes les relations parmi les traces se déduisent du théorème de Cayley-Hamilton.