Exposé : Invariants des groupes finis
Le théorème de Chevalley-Shepard-Todd

$k = \mathbb{C}$

1 Généralités et notations

1.1 Fonctions polynomiales sur V

(Rapidement, comme rappel) : V un k-espace vectoriel de dimension finie n, on sait construire $V \otimes V$, et $V \otimes V \otimes V$ etc. qui permettent de former "formellement" des monômes en les vecteurs de V. On considère l'algèbre symétrique de V^* qui sont des polynômes en les formes linéaires, et on identifie $S(V^*) \cong k[X_1, \dots X_n]$ via $e_i^* \mapsto X_i$ morphisme d'algèbres, et on voit $P(e_1^*, \dots, e_n^*)$ comme un polynôme sur V. Ici (e_i) est une base de V et (e_i^*) sa base duale, mais cette définition peut être rendue canonique.

Si $G \subset GL(V)$ est un sous-groupe, il agit à droite dans V^* via $\sigma.f(x) = f(\sigma^{-1}(x))$, cette action est linéaire et multiplicative, et préserve le degré. Soit $G \subset GL(V)$ un groupe fixé.

1. On note S l'algèbre $S(V^*)$ des polynômes sur V
2. On note R l'algèbre des invariants de S sous l'action de G
3. On note R_+ les éléments de R de degré ≥ 1
4. On note p le projecteur particulier sur R donné par la moyenne $\frac{1}{|G|} \sum_{g \in G} g$

Le problème ici : dire des choses sur la structure de R comme k-algèbre, de S comme R-module, en fonction des propriétés de G.

1.2 Propriétés possibles

Très rapidement : k-algèbre de type fini, module de type fini

Base de transcendance Famille d'éléments algébriquement indépendants dans une extension $k \subset K$, on appelle base de transcendance = famille indépendante maximale. Zorn donne la :

Proposition 1 *$k \subset K$ admet une base de transcendance sur k et K est algébrique sur une telle base.*

Mentionner juste ? On a comme en algèbre linéaire : une famille indépendante maximale est une base, toute les bases ont même cardinal, toute famille indépendante peut se compléter en une base. On appelle "degré de transcendance" ce cardinal commun.

1.3 Formulation du problème

On montre d'abord que R est une k-algèbre de type fini, sans hypothèse sur G. Ensuite, on s'attache à montrer l'équivalences des trois propriétés :

1. G est engendré par les pseudo-réflexions qu'il contient (on reviendra mais une pseudo-réflexion est un $\sigma \in GL(V)$, diagonalisable, avec $n-1$ fois 1 comme vap i.e. qui fixe un hyperplan.)
2. R est de type fini, et peut même s'écrire $k[f_1, \dots, f_n]$ avec les f_n algébriquement indépendants (et $n = \dim_k V$)
3. S est un R-module libre.

2 R est une k-algèbre de type fini

On montre le

Théorème 1 *Soit $G \subset GL(V)$ un sous-groupe. Alors R est une algèbre de type fini, plus précisément. il existe $f_1, \ldots, f_m$ des polynômes homogènes de degré ≥ 1 tels que $R = k[f_1, \ldots, f_m]$*

Preuve On veut trouver des générateurs, comme on est dans un anneau de polynômes (donc noethérien) on sait que tous les idéaux sont de type fini : on dispose de l'idéal engendré (R^+) et on peut montrer (rapide mais il y a un petit passage technique) que ses générateurs comme idéal (que l'on peut supposer dans R^+ et pas seulement dans (R^+)) conviennent. C'est un réflexe humain (Rosso, G quelconque), mais il y a une preuve plus directe qui évite cette vérification fastidieuse (Springer). Mais cette fois on a besoin de G fini (? ?)

Proposition 2 *L'extension d'anneaux $R \subset S$ des invariants dans les polynômes en général est une extension entière.*

Preuve : si $f \in S$, considérer $\prod_{g \in G}(f - g.f) = 0$ qui donne un polynôme unitaire annulateur de f , avec coefficients dans R (cf. cours). On utilise G fini.

Proposition 3 *Rappel : si A est un anneau nothérien, tout sous-A-module d'un A-module de type fini est de type fini*

Preuve (juste l'idée) : comme les A-modules de type fini sont des quotients de A^r, on peut se ramener à montrer qu'un sous-module de A^r est encore de type fini. Pour $r = 1$ c'est la définition de la noethérianité (sous-modules = idéaux), puis par récurrence on peut décomposer $A^r = A \oplus A^{r-1}$ et étudier sur chaque composante par récurrence.

On peut maintenant démontrer le théorème : S est clairement une k-algèbre de type fini puisqu'on a dit que $S = k[X_1, \ldots, X_n]$. Comme S est entière sur R, chaque X_i possède un polynôme annulateur avec des coefficients $r_{i,k}$ $(k \leq n_i < \infty)$ dans R, et si on note A la k-algèbre A engendrée par tous ces coefficients, c'est une k-algèbre noethérienne (puisque c'est $k[\text{les } r_{i,k}]$) sur laquelle S est toujours entière (puisqu'on a gardé les coefficients des polynômes annulateurs d'un système de générateurs de S). Comme S est de type fini sur k et entière sur A, S est en fait un A-module de type fini (pour chaque X_i, le $A[X_i]$ est un module de type fini par intégralité, on a donc une somme finie de A-modules de type fini...). Finalement, R est un sous-A-module de S, avec A noethérien, donc d'après la proposition précédente R est encore un A-module de type fini, et comme A est elle-même une k-algèbre de type fini...

Notons qu'on peut avoir "précisément" l'énoncé (homogénéité des générateurs) en décomposant selon les composantes homogènes, qui sont également invariantes car G conserve le degré.

3 1) $\Longrightarrow$ 2) Théorème de Chevalley

On ne donnera pas la preuve entière, on essaye simplement de montrer comment traduire l'hypothèse faite sur G, et on donne le schéma de la démonstration.

3.1 Traduction de l'hypothèse

La seule chose que l'on sait sur G (en plus de la finitude) c'est qu'il contient "beaucoup" de pseudo-réflexions, i.e. d'automorphismes qui fixent un hyperplan point par point. À un hyperplan on sait associer une forme linéaire sur V, qui est la brique essentielle de V^* (des polynômes sur V). On traduit ça en deux lemmes :

Lemme 1 (Brique élémentaire) *Soit f un polynôme sur V (i.e. $f \in S$), et l une forme linéaire de noyau H, alors l divise f en tant que polynôme si et seulement si f s'annule sur H.*

Preuve : un sens est évident. Réciproquement, dans une base adaptée, on fait la division euclidienne par rapport à X_n (qui correspond à un supplémentaire de H) : f s'écrit $AX_n + B$ et en évaluant sur H on a B nul.

En particulier, si σ est une réflexion d'hyperplan H, comme $\sigma \equiv$ Id sur H, alors $\sigma(f) - f$ est divisible par toute forme linéaire qui s'annule sur H. En effet $\sigma(f) - f$ s'annule sur H.

Lemme 2 *Soit f un polynôme dans S, tel que le polynôme "moyenne" $p(f)$ (qui est "la" projection sur R) est nul ou non constant. On suppose que $\sigma(f) - f$ est dans l'idéal engendré par R^+ pour toute réflexion σ, alors en fait f est lui-même dans cet idéal*

Évidemment, comme G est supposé être engendré par les réflexions, l'information "pour toute réflexion" donne plus qu'apparemment. On démontre par récurrence sur le nombre de réflexions engendrant $g \in G$, que $g(f) - f$ est dans l'idéal pour tout $g \in G$. Donc c'est encore le cas de $p(f) - f$. Finalement, $f \in p(f) + (R^+)$, l'hypothèse faite sur $p(f)$ permet de conclure.

3.2 Schéma de conclusion

On veut trouver un "ensemble basique" c'est à dire des polynômes $f_1, \ldots, f_m$ qui engendrent R comme k-algèbre (ça on sait que ça existe) et qui soient algébriquement indépendants. Il est naturel de prendre une famille "minimale" de générateurs de R comme k-algèbre. Pour montrer que ça convient, on raisonne par l'absurde : on trouve P un grand polynôme non nul tel que $P(f_1, \ldots, f_m)$ soit nul. On dérive formellement l'égalité $P(f_i) = 0$ selon x_k, on obtient une relation de liaison entre les $\partial P/\partial X_i(f_1, \ldots, f_m)$ (qui sont des sommes de produits de trucs dans R, donc est dans R). Ensuite il faut travailler pour montrer qu'une telle relation de liaison entraîne une relation de liaison entre les f_i, utiliser les lemmes précédents.. Une idée que l'on peut noter : on se retrouve avec des $\partial f_i/\partial x_k$, et on veut remonter aux f_i, on utilise l'identité d'Euler :

$$\sum_{k=1}^{m} x_k \partial f/\partial x_k = (\deg f) f \tag{1}$$

Remarque sur les générateurs. On peut les choisir homogènes (on prend une famille minimale de générateurs.. homogènes). Il y en a au plus n parce que le degré de transcendance de $k(X_1, \ldots, X_n)$ sur k est exactement n et qu'on a des inclusions. Il y en a au moins n parce qu'on passe au corps des fractions (cf. Rosso)

4 $2 \Longrightarrow 1$: Théorème de Shepard-Todd

Théorème 2 *Soit G un groupe fini de $GL(V)$, si R admet un ensemble basique, alors G est engendré par les pseudo-réflexions qu'il contient*

Preuve : soit H le sous-groupe engendré par les pseudo-réflexions, on va mq $G = H$. D'après le sens direct appliqué à H, il y a des polynômes h_i homogènes et libres tels que $R_H = k[h_1, \ldots, h_n]$. Supposons que R_G admette lui-aussi un ensemble basique, écrit $k[f_1, \ldots, f_n]$: comme on a clairement $R_G \subset R_H$, on peut décomposer $f_i = F_i(h_1, \ldots, h_n)$. Dérivons selon X_k :

$$\frac{\partial f_i}{\partial X_k} = \sum_{j=1}^{n} \frac{\partial F_i}{\partial Y_j} \frac{\partial h_j}{\partial X_k} \tag{2}$$

Et ce pour tout i, k, ce qui se ré-ecrit

$$\left(\frac{\partial f_i}{\partial X_k}\right)_{1 \leq i,k \leq n} = AB \tag{3}$$

En appliquant det, le terme de gauche, c'est le jacobien des f_i, et le terme de droite c'est le produit de deux jacobiens : celui des F_i et celui des h_i (remarque : c'est simplement de la dérivation composée). Comme le jacobien des f_i est non nul (par liberté), c'est aussi le cas du Jacobien des F_i. Il existe un terme non nul, i.e. une permutation $\sigma \in S_n$ telle que le long le produit est non nul, ce qui impose que $\frac{\partial F_i}{\partial Y_{\sigma(i)}} \neq 0$, donc $h_{\sigma(i)}$ apparaît vraiment dans $f_i = F_i(h_1, \ldots, h_n)$. Ainsi $\deg f_i \geq \deg h_{\sigma(i)}$.

Mais comme il y a autant de réflexions dans H et dans G, et que c'est relié à

$$\sum_{i=1}^{n} (\deg f_i - 1) \tag{4}$$

Les degrés sont égaux. Ensuite, on sait relier $|H|$ égal le produit des degrés donc $|H| = |G|$ CQFD.

En fait il faut montrer que si les f_i sont libres leur jacobien est non nul (et réciproquement). C'est pas dur.

5 Exemple en guise de conclusion

On prend S_n (vu comme les réflexions de vecteur normal $\epsilon_i - \epsilon_j$ (les transpositions) et $\mathbb{Z}/2\mathbb{Z}^n$ vu comme les réflexions de vecteur normal ϵ_i. On note G le sous-groupe engendré par les deux, c'est clairement un

groupe fini, engendré par des (vraies) réflexions, et on a même G comme produit semi-direct des deux qui précèdent, donc le cardinal de G c'est le produit des deux à savoir $2^n n!$. On cherche un ensemble basique, déjà il faut être stable par changement de signe de chaque composante (puisqu'on a $\mathbb{Z}/2\mathbb{Z}$) et puis être symétrique, donc on considère les $f_i = \sum x_k^{2i}$ pour i de 1 à n, ce qui donne bien $|G| = \prod$ degrés . Les f_i sont évidemment libres (calculer leur Jacobien si besoin est, on tombe sur un Vandermonde). Ils sont donc libres, homogènes, et le produit des degré est le bon. Est-ce que ça suffit ?

Ben oui. On sait qu'il existe un vrai ensemble basique, ordonnons les degrés de chacun. On montre que les degrés du nouveau sont supérieurs aux degrés de l'ancien (essentiellement parce que l'ancien s'écrit en fonction du nouveau et qu'on est homogènes donc on ne peut pas se simplifier). Mais comme les produits des degrés coïncident en fait ce sont les mêmes point par point (remarque c'est sensiblement le même raisonnement que précédemment). Et finalement, comment faire retour sur les invariants (et pas sur le cardinal comme précédemment) ? On a une formule qui va bien :

$$\sum \dim R_k t^k = \prod \frac{1}{1-t^{d_i}} \tag{5}$$