Développements d'Algèbre et de Géométrie

Version préliminaire du 13 septembre 2009

Igor Kortchemski

Ce document regroupe les développements d'Algèbre et de Géométrie que j'ai préparés pour l'agrégation externe de mathématiques en 2009. Ceux-ci sont classés par thème, puis par degré « d'originalité ». Les développements plutôt originaux sont complètement rédigés. Quant aux autres, je me contente de citer le résultat et de renvoyer aux références, mais cela ne signifie pas nécessairement qu'ils sont plus faciles. Chaque développement est auto-suffisant, en ce sens qu'il n'admet pas de résultat intermédiaire délicat et, dans la mesure du possible, chacun est suivi d'un petit commentaire illustrant son *intérêt*.

Par ailleurs, j'espère qu'après avoir parcouru ce document le lecteur sera persuadé qu'on peut faire de belles mathématiques au niveau de l'agrégation.

Table des matières

Première partie
Algèbre générale

1 Développements un peu originaux

1.1 Groupes finis nilpotents

Ce développement vise à obtenir une caractérisation des groupes finis nilpotents. Nous verrons que ceux-ci sont exactement les groupes finis qui sont produits directs de ses sous-groupes de Sylow.

Définition 1.1. Soit G un groupe (pas nécessairement fini !). Posons $Z_0 = \{1\}$ et pour $i \geq 0$ définissons Z_{i+1} tel que :

$$Z_{i+1}/Z_i = Z(G/Z_i), \tag{1}$$

où nous avons noté $Z(H)$ le centre de H. On dit que G est *nilpotent* s'il existe i tel que $Z_i = G$.

Petite remarque : d'après le principe de correspondance, Z_i est distingué dans G pour tout i.

Théorème 1.2. *Soit G un groupe* fini. *Les équivalences suivantes ont lieu :*

1. *G est nilpotent,*
2. *Si $H \lneq G$, alors $H \lneq N_H$ où $N_H = \{g \in G; \quad gHg^{-1} = H\}$ est le normalisateur de H dans G.*
3. *Tous les p-Sylow de G sont distingués.*
4. *G est produit direct de ses p-Sylow.*

Preuve. Raisonnons comme suit.

$\boxed{1 \Rightarrow 2}$ Notons $H_0 = H$ et $H_{i+1} = \{g \in G; gH_ig^{-1} \in H_i\}$. Montrons par récurrence sur i que :

$$\forall i \in \mathbb{N}, \qquad Z_i \subset H_i.$$

Pour $i = 0$, c'est clair. Pour le passage de i à $i+1$, considèrons $h_i \in H_i$. Alors pour tout $z_{i+1} \in Z_{i+1}$, d'après (1) :

$$z_{i+1}Z_ih_iZ_i = h_iZ_iz_{i+1}Z_i,$$

d'où $z_{i+1}^{-1}h_i^{-1}z_{i+1}h_i \in Z_i$. L'hypothèse de récurrence implique ensuite que $z_{i+1}^{-1}h_i^{-1}z_{i+1} \in H_i$. Ainsi, $z_{i+1} \in N_{H_i} = H_{i+1}$. En définitive, $Z_{i+1} \subset H_{i+1}$, ce que nous voulions montrer.

On conclut que si $H \lneq G$ (c-à-d strictement inclus) et $H = N_H$, alors la suite (Z_i) reste incluse dans H ce qui contredit le caractère nilpotent de G.

$\boxed{2 \Rightarrow 3}$ Soit P un p-Sylow de G. En vertu du point 2, il suffit de montrer que $N_{N_P} = N_P$ car alors P est égal à son normalisateur, donc est distingué. Il est clair que $N_P \subset N_{N_P}$. Pour l'autre inclusion, choisissons $h \in N_{N_P}$ et montrons que $h \in N_P$.

Mais hPh^{-1} est un p-Sylow de N_P. Comme les p-Sylow de N_P sont conjugués dans N_P (!!), il existe donc $j \in N_P$ tel que :

$$hPh^{-1} = jPj^{-1}.$$

Il en découle que $j^{-1}h \in N_P$ et finalement que $h \in N_P$.

$\boxed{3 \Rightarrow 4}$ Notons $P_1, \dots, P_k$ les différents sous-groupes de Sylow correspondant respectivement aux nombres premiers $p_1, \dots, p_k$. Alors si $i \neq j$, $\alpha \in P_i$ et $\beta \in P_j$, alors $\alpha\beta = \beta\alpha$. En effet, d'une part $P_i \cap P_j = \{1\}$ (grâce au théorème de Lagrange), et d'autre part comme les sous-groupes de Sylow sont distingués, on a $(\beta^{-1}\alpha^{-1}\beta)\alpha = \beta^{-1}(\alpha^{-1}\beta\alpha) = P_i \cap P_j$.

Considérons alors $H = P_1 \cdots P_k$ qui est un sous-groupe de G (car les sous-groupes de Sylow sont dinstingués). Par récurrence, nous voyons que tout élément de H s'écrit de manière *unique* sous la forme $p_1 \cdots p_k$ avec $p_i \in P_i$ pour tout i. Conséquemment, pour une raison de cardinalité :

$$\begin{array}{rcl} P_1 \times \cdots \times P_k & \to & G \\ (\alpha_1, \cdots, \alpha_k) & \mapsto & \alpha_1 \cdots \alpha_k \end{array}$$

est un isomorphisme de groupes.

$\boxed{4 \Rightarrow 1}$ Il suffit de montrer qu'un p-groupe est nilpotent. Par l'absurde, soit donc i tel que $Z_i \neq G$ et $Z_{i+1} = Z_i$. En utilisant (1), il s'ensuit que $Z(G/Z_i) = 0$. Ceci est absurde car le centre d'un p-groupe non trivial est non trivial (pourquoi ?). ■

Références. Ceci est fait dans le désordre dans « The theory of groups » de Hall.

Remarques. Je trouve ce développement assez joli parce qu'il utilise beaucoup de notions de la théorie des groupes : principe de correspondance (qui dit comment les différentes notions passent au quotient), théorèmes de Sylow, théorème de Lagrange et argument de Fratini (c'est ainsi qu'est appelé le raisonnement fait dans 2 implique 3).

1.2 Théorème de Lie-Kolchin

Le but de ce développement est d'obtenir une preuve du théorème de Lie-Kolchin qui est un résultat de co-trigonalisation simultanée.

Définition 1.3. Soit G un groupe (non nécessairement fini). Appelons *sous-groupe dérivé* de G le sous-groupe de G engendré par les commutateurs de G, c-à-d par les éléments de la forme $ghg^{-1}h^{-1}$ avec $g, h \in G$, et notons le $D(G)$. Définissons par récurrence $D^0(G) = G$ et $D^{i+1}(G) = D(D^i(G))$. On dit que G est *résoluble* s'il existe i tel que $D^i = \{1\}$.

Théorème 1.4 (Lie-Kolchin)**.** *Soit G un sous-groupe connexe résoluble de $Gl_n(\mathbb{C})$. Alors il existe une base de $\mathbb{C}^n$ dans laquelle tous les éléments de G sont des matrices trigonales supérieures.*

Lemme 1.5. *Soit $H < G$. Notons*[1] *:*

$$\mathcal{E}_H = \{v \in \mathbb{C}^n, \quad v \text{ est un vecteur propre commun à tous les } h \in H\},$$

qu'on suppose non vide. À $v \in \mathcal{E}_H$ associons le morphisme de groupes[2] *$\chi_v : H \to \mathbb{C}^*$ de tel sorte que pour tout $h \in H$:*

$$\chi_v(h)v = h(v).$$

Alors χ_v est une application continue et $\{\chi_v; \quad v \in \mathcal{E}_H\}$ est fini.

Preuve. La continuité de χ_v est immédiate. Pour la seconde assertion, considèrons $\{v_1, \dots, v_r\}$ une famille libre maximale de $\mathcal{E}_H$. Soit $v \in \mathcal{E}_H$, qu'on écrit :

$$v = \sum_{i=1}^{r} \alpha_i v_i.$$

Appliquons $h \in H$:

$$\chi_v(h)(\sum_{i=1}^{r} \alpha_i v_i) = \sum_{i=1}^{r} \alpha_i \chi_{v_i}(h) v_i.$$

Par liberté des v_i, il existe donc i_0 tel que $\alpha_{i_0} \neq 0$. On conclut alors que $\chi_v = \chi_{v_{i_0}}$. ■

Lemme 1.6. *Supposons $H \lhd G$ (c-à-d H distingué dans G) et que $\mathcal{E}_H$ est non vide. Soit $v \in \mathcal{E}_H$. Alors pour tous $g \in G, h \in H$:*

$$\chi_{g(v)}(h) = \chi_v(g^{-1}hg) = \chi_v(h).$$

Preuve. Commençons par remarquer que comme H est distingué dans G, $g(v) \in \mathcal{E}_H$ car :

$$g^{-1}hg(v) = \chi_v(g^{-1}hg)v.$$

La première égalité en découle. Pour la seconde, notons :

$$S = \{g \in G; \quad \chi_{g(v)} = \chi_v\},$$

[1] Rappelons que, par définition, un vecteur propre est non nul.

[2] Le problème principal qu'il va falloir contourner est que $\mathcal{E}_H$ n'est *pas* un sous-espace vectoriel de $\mathbb{C}^n$.

qui est un sous-groupe fermé de G car :

$$S = \bigcup_{h \in H} \phi_h^{-1}(\{0\}),$$

où

$$\begin{aligned} \phi_h : G &\to \mathbb{C} \\ g &\mapsto \chi_v(g^{-1}hg) - \chi_v(h). \end{aligned}$$

Or $\{\chi_{g(v)}; \quad g \in G\}$ est fini d'après le premier lemme et $\chi_{g(v)} = \chi_{g'(v)}$ implique que $\chi_{g'^{-1}g(v)} = \chi_v$. Ainsi, S est d'indice fini dans G qui s'écrit :

$$G = \bigsqcup_{i=1}^{l} g_i S,$$

pour certains $g_i \in G$ et un entier l. Par connexité de G, on en déduit que $l = 1$, ce qui conclut. ■

Lemme 1.7 (mêmes hypothèses que le lemme précédent)**.** *Soit $v_0 \in \mathcal{E}_H$. Alors $\{v \in \mathbb{C}^n; \quad \forall h \in H, h(v) = \chi_{v_0}(h)v\}$ est un sev non réduit à $\{0\}$ de $\mathbb{C}^n$ stable par G.*

Preuve. Immédiate en utilisant le deuxième lemme. ■

Preuve du théorème. Raisonons par récurrence sur le plus petit entier i tel que $D^i(G) = \{1\}$. Si $i = 0$, alors $G = \{1\}$ et il n'y a rien à montrer. Pour le passage de i à $i+1$, quitte à effectuer une récurrence[3] sur la dimension n, supposons que G agit de manière irréductible, c'est-à-dire que :

si V est un sev de $\mathbb{C}^n$ stable par tous les éléments de G, alors $V = \{0\}$ ou $V = \mathbb{C}^n$.

Nous allons montrer que nécessairement $n = 1$.

Remarquons que $D(G)$ est un groupe connexe résoluble pour lequel l'hypothèse de récurrence s'applique. Montrons qu'il est connexe. On peut écrire $D(G) = \cup_{i \geq 1} U_i$ où $U_1 = \{ghg^{-1}h^{-1}; \quad g, h \in G$ est connexe car image de $G \times G$ (connexe) par l'application continue :

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto ghg^{-1}g^{-1}, \end{aligned}$$

et où pour $i \geq 0$, $U_i = \{c_1 \cdots c_i; \quad c_1, \cdots, c_i \in U_1\}$ est de même connexe. Comme pour $i \neq j$, $1 \in U_i \cap U_j$, les $U_i \cap U_j$ sont non vides ce qui permet d'affirmer que $D(G)$ est connexe. D'après l'hypothèse de récurrence, $\mathcal{E}_{D(G)}$ est non réduit à $\{0\}$.

Soit donc $v_0 \in \mathcal{E}_{D(G)}$. Alors d'après le troisième lemme :

$$\{v \in \mathbb{C}^n, \quad \forall h \in D(G), h(v) = \chi_{v_0}(h)v\}$$

est un sev non réduite à $\{0\}$ de $\mathbb{C}^n$, qui est donc égal à C^n par irréductibilité. Soit alors $g_0 \in G$. Par suite, $\langle g_0, D(G) \rangle$, le sous-groupe de G engendré par g_0 et $D(G)$ est distingué (pourquoi ?).

[3] S'en convaincre !

Soit w_0 un vecteur propre de g_0 (on utilise ici le fait que $\mathbb{C}$ est algébriquement clos). Alors $w_0 \in E_{\langle g_0, D(G)\rangle}$. Comme précédemment, nous en déduisons que :

$$\{v \in \mathbb{C}^n; \quad \forall g \in \langle g_0, D(G)\rangle, h(v) = \chi_{w_0}(h)v\} = \mathbb{C}^n.$$

En particulier, pour tous $v \in \mathbb{C}^n, g_0 \in G$, $g_0(v) \in \mathbb{C}v$. Par irréductibilité, on en déduit que $n = 1$.
■

Références. « Lie Algebras and Lie Groups » de Serre (chapitre 5).

Remarques.

1. La notion de sous-groupe résoluble provient de la notion de résolubilité par radicaux des racines d'un polynôme. Voir le livre de Cox (« Galois Theory ») pour plus d'informations et le lien très important entre les deux notions.
2. On pourra comparer ce résultat au suivant (théorème de ?) : si U est une sous-algèbre de Lie résoluble [4] de $\mathcal{L}(\mathbb{C}^n)$, alors les éléments de U sont co-trigonalisables.

[4] Voir le développement concernant le théorème d'Engel pour une définition de sous-algèbre de Lie. La résolubilité signifie que la suite définie par $U_0 = U$ et $U_{i+1} = [U_i, U_i]$ finit par atteindre $\{0\}$.

2 Développements moins originaux

2.1 Groupes d'ordre 12

Il s'agit ici de classifier les groupe d'ordre 12.

Théorème 2.1. *À isomorphisme près, il y a 5 sous-groupes d'ordre 12 qui sont :*

$$\mathbb{Z}/12\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \rtimes V_4, \quad \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \rtimes V_4,$$

où V_4 désigne $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, le groupe de Klein, et où $G \rtimes H$ désigne l'unique produit semi-direct non direct de G par H.

Preuve. Soit G un groupe d'ordre 12. Notons n_i le nombre de i Sylow de G, de sorte que d'après un théorèmede Sylow n_3 divise 4 en étant congru à 1 modulo 3.

Cas 1 : $n_3 = 1$**.**Notons N l'unique 3-Sylow qui est donc distingué dans G. Soit H un 4-Sylow[5]. Notons que d'après la classification des groupes d'ordre 4, $H \simeq \mathbb{Z}/4\mathbb{Z}$ ou $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ensuite, pour des raisons d'ordre, $N \cap H = \{1\}$ et $NH = G$. En effet, d'une part $NH \subset G$ et d'après un théorème d'isomorphime :

$$NH/N \simeq H/N \cap H,$$

d'où $|NH| = |N||H| = 12 = |G|$. On en déduit que $G \simeq \mathbb{Z}/3\mathbb{Z} \rtimes H$.

Cas 1.1 : $H \simeq \mathbb{Z}/4\mathbb{Z}$**.** Il s'agit de trouver tous les morphismes de groupes $\mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \simeq (\mathbb{Z}/3\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$. Il n'en existe qu'un seul qui ne soit non trivial. Ainsi, G est isomorphe à $\mathbb{Z}/12\mathbb{Z}$ ou à $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.

Cas 1.2 : $H \simeq V_4$**.** Il s'agit de trouver tous les morphismes de groupes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. En faisant un petit tableau, on s'aperçoit aisément qu'il en existe exactement quatre, dont trois non triviaux, et que si on note ceux-ci ϕ_1, ϕ_2 et ϕ_3, alors pour $i \neq j$, il existe $\alpha \in \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ tel que $\phi_i = \phi_j \circ \alpha$ (on voit que $\mathrm{Aut}(V_4) \simeq \mathfrak{S}_3$). En vertu du lemme qui suit, les trois produits semi-directs correspondants sont isomorphes. On trouve donc que G est isomorphe à $\mathbb{Z}/12\mathbb{Z}$ (d'après le lemme chinois) ou à $\mathbb{Z}/3\mathbb{Z} \rtimes V_4$.

Lemme 2.2. *Soient $G \rtimes_\phi H$ et $G \rtimes_\psi H$ deux produits semi-directs de G par H donnés par les morphismes ϕ, ψ de H dans $Aut(G)$ tels qu'il existe $\alpha \in Aut(H)$ tel que $\phi = \psi \circ \alpha$. Alors les deux produits semi-directs sont isomorphes.*

Cas 2 : $n_3 = 4$**.** Comme un groupe d'ordre 3 est monogène, l'intersection des différents 3-Sylow est réduite à l'identité et leur union U est de cardinal $1 + 2 \times 4 = 9$. Soit N un 4-Sylow. Alors $N = (G \backslash U) \cup \{Id\}$. En particulier, il n'y a qu'un seul 4-Sylow, distingué, de G qu'on notera N. Raisonons comme précédemment ; soit H un 3-Sylow de sorte que $G \simeq N \rtimes \mathbb{Z}/3\mathbb{Z}$.

Cas 2.1 : $N \simeq \mathbb{Z}/4\mathbb{Z}$**.** Il s'agit de trouver tous les morphismes de groupes $\mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \simeq (\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$. Comme N est monogène, il est facile de voir qu'il n'y en a qu'un seul qui ne soit non trivial. Ainsi, G est isomorphe à $\mathbb{Z}/12\mathbb{Z}$ ou à $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$.

Cas 2.2 : $N \simeq V_4$**.** Il s'agit de trouver tous les morphismes de groupes $\mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(V_4) \simeq \mathfrak{S}_3$. Il y en a exactement deux non-triviaux caractérisés par l'image de $\overline{1}$ comme suit : $\phi_1(\overline{1}) = (123)$ et $\phi_2(\overline{1}) = (132)$ (ici, (123) désigne le cycle de $\mathfrak{S}_3$ qui envoie 1 sur 2, etc.). Or $\phi_1 = (23)\phi_2(23)^{-1}$, ce qui implique que les produit semi-directs qu'ils définissent sont isomorphes d'après le lemme qui suit. Finalement, G est isomorphe à $Z/12\mathbb{Z}$ ou à $V_4 \rtimes \mathbb{Z}/3\mathbb{Z}$.

[5]Qui existe bien d'après un théorème de Sylow !

Lemme 2.3. *Soient $G \rtimes_\phi H$ et $G \rtimes_\psi H$ deux produits semi-directs de G par H donnés par les morphismes ϕ, ψ de H dans $Aut(G)$ tels qu'il existe $\beta \in Aut(G)$ tel que $\phi = \beta \circ \psi \circ \beta^{-1}$. Alors les deux produits semi-directs sont isomorphes.*

■

Références. « Thèmes de géométrie ; Groupes en situation géométrique » (Alessandri) pour le développement et les exercices d'algèbre 1 pour l'agrégation de Francinou/Gianella pour les deux lemmes.

Remarques.

1. Ce développement permet de mettre en oeuvre sur un exemple concret le principe suivant : pour trouver les morphismes de G dans H, il est parfois commode de connaître des générateurs de G et/ou de H.
2. Ce développement illustre de manière concrète l'utilisation des théorèmes de Sylow pour comprendre la structure d'un groupe.
3. Les deux lemmes répondent en partie à la questions suivante : « Quand est-ce que deux produits semi-directs *différents* sont *isomorphes* » ? Question qui n'a pas de réponse en toute généralité... !

2.2 Groupes simples d'ordre 60

Le but de ce développement est de voir que tout groupe simple d'ordre 60 est isomorphe à A_5. On commence par vérifier que A_5 est bien un groupe simple.

Lemme 2.4. *A_5 est engendré par les 3-cycles.*

Lemme 2.5. *Les doubles transpositions et les 3-cycles sont conjugués d ans A_5.*

Théorème 2.6. *A_5 est simple.*

Preuve. La démonstration consiste à démontrer que si un sous-groupe distingué non trivial de A_5 contient un élément d'ordre i, alors il contient tous les éléments d'ordre i. ■

Théorème 2.7. *Tout groupe simple d'ordre 60 est isomorphe à A_5.*

Preuve. Soit G un groupe simple d'ordre 60. Soit H un sous-groupe de G non réduit à l'identité et *distinct de* G. Alors $|G/H| \geq 5$, car G agit par translation *non trivialement* sur G/H, ce qui fournit un morphisme de groupes :

$$G \to \mathfrak{S}_{G/H},$$

dont le noyau, nécessairement non trivial lorsque $|G/H| < 5$, et par ailleurs distinct de G car l'action est non triviale, est un sous-groupe distingué de G, qui est simple par hypothèse.

Montrons qu'il existe un sous-groupe H de G tel que $|G/H| = 5$. Raisonnons par l'absurde. Notons n_2 le nombre de 2-Sylow de G. Alors d'après des théorèmes de Sylow $n_2|15$ et $n_2 > 1$, car G est simple. Soit N le normalisateur d'un 2-Sylow S, c-à-d le stabilisateur de S dans l'action de G sur l'ensemble des 2-Sylow de G par conjugaison :

$$g.S = gSg^{-1}.$$

Ainsi n_2, qui est égal au nombre d'orbites car l'action est transitive (d'après un théorème de Sylow, tous les 2-Sylow sont conjugués), vaut $|G|/|N|$. Comme $n_2 > 1$, $N \neq G$ et nous pouvons utiliser ce qui précède : $n_2 > 5$. Donc $n_2 = 15$.

Soit maintenant $\widetilde{S}$ un autre 2-Sylow, soit $t \in S \cap \widetilde{S}$ et supposons $t \neq Id$. Notons :

$$C_G(t) = \{g \in G; \quad gt = tg\}.$$

Comme tout groupe d'ordre 4 est commutatif, il vient $S, \widetilde{S} \subset C_G(t)$. Donc $|C_G(t)| > 4$, et d'après le théorème de Lagrange $4|C_G(t)$. Ceci fournit $|C_G(t)| \geq 12$ car 60 doit être divisible par $C_G(t)$. Finalement, $|G/C_G(t)| \leq 5$, ce qui impose, d'après le premier paragraphe, $G = C_G(t)$, de sorte que $Z(G) \neq \{Id\}$, ce qui contredit la simplicité de G. Ainsi, les 2-Sylow sont d'intersection deux à deux triviale.

En définitive, il y a donc $15 \times 3 = 45$ éléments distincts d'ordre 2 ou 4 et comme $n_5 = 6$ (le nombre de 5-Sylow, vérifie $n_5|12$ et $n_5 = 1[5]$), nous trouvons au moins $6 \times 4 = 24$ éléments distincts d'ordre 5, soit en tout 69 éléments ; absurde.

En considérant H tel que $|G/H| = 5$, nous tombons donc, comme précédemment, sur un morphisme de groupes injectif (par simplicité de G) non trivial :

$$\phi : G \to \mathfrak{S}_5.$$

Ainsi, $G \simeq \phi(G)$. Or $\phi(G)$ est d'indice 2 dans $\mathfrak{S}_5$, donc distingué dans $\mathfrak{S}_5$. Par passage au quotient, il vient un morphisme de groupes $\mathfrak{S}_5/\phi(G) \to \mathbb{Z}/2\mathbb{Z}$ non trivial, qui est nécessairement la signature (l'image d'une transposition est $\overline{1}$ car les transpositions engendent S_5). Il en découle que $\phi(G) = A_5$, ce qui permet de conclure. ■

Références. « Cours d'algèbre » (Perrin) pour la simplicité de A_5 et le livre d'Alperin/Bell sur les groupes (p. 69) pour la suite.

Remarques.

1. La première partie est classique. Il existe plusieurs méthodes pour poursuivre, mais j'aime bien cette approche-ci qui illustre sympathiquement les trois théorèmes de Sylow et l'intérêt de la dualité entre action de groupes et morphismes dont le but est un groupe symétrique.
2. On peut montrer que tout groupe simple d'ordre 168 est isomorphe à $PGL_2(\mathbb{F}_3)$ (voir par exemple les Exercices d'Algèbre d'Ortiz). D'où la question : quel est le plus petit n tel qu'il existe deux groupes simples d'ordre n non isomorphes ? Réponse (partielle ;-)) : 20160.

3 Développements plus classiques

3.1 Théorème de Wedderburn

Théorème 3.1. *Toute algèbre à division finie est commutative.*

J'aime bien la preuve de Witt qui figure dans le Perrin (Cours d'algèbre). Celle-ci se fait en utilisant les polynômes cyclotomiques, notés ϕ_n :

Lemme 3.2. *On a :*

$$X^n - 1 = \prod_{d|n} \phi_d(X).$$

Lemme 3.3. *On a $\phi_n(X) \in \mathbb{Z}[X]$ et ce dernier polynôme est unitaire.*

Preuve. La démonstration utilise l'existence et unicité de la division euclidienne dans $\mathbb{Z}[X]$ par un polynôme unitaire de $\mathbb{Z}[X]$, mais pas la factorialité de $\mathbb{Z}[X]$. ■

Preuve du théorème. En notant k une algèbre à division finie, l'idée de la preuve consiste à faire agir k^* sur k^* par conjugaison, à écrire l'équation aux classes et à utiliser le lemme suivant :

Lemme 3.4. *Pour q, d, n des entiers avec $q \geq 2$, nous avons $pgcd(q^d - 1, q^n - 1) = q^{pgcd(d,n)} - 1$. En particulier, si $q^d - 1$ divise $q^n - 1$, alors d divise n.*

Preuve. La division euclidienne de $q^n - 1$ par $q^d - 1$ se fait de la même manière que celle de n par d. Plus précisément, si $n = du + r$ avec $0 \leq r < d$, alors :

$$q^n - 1 = \left(q^d - 1\right)\left(q^{d(u-1)+r} + \cdots + q^r\right) + q^r - 1.$$

■

3.2 Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

Théorème 3.5. *On a les isomorphismes suivants :*

1. *(théorème chinois) Pour $p_1, \dots, p_k$ premiers et $\alpha_1, \dots, \alpha_k$ des entiers :*
$$(\mathbb{Z}/p_1^{\alpha_1} \cdots p_k^{\alpha_k}\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times .$$
2. *Pour p premier impair et $\alpha \geq 1$:*
$$(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}.$$
3. *Pour $\alpha \geq 2$:*
$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Pour faire tenir ça en 15 minutes, je pense qu'il vaut mieux admettre le cas $\alpha = 1$ dans le deuxième point (c-à-d que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique), qui reste bien sûr fondamental.

Référence. « Cours d'algèbre » (Perrin)

Remarque. Un exemple d'utilisation de ce résultat peut consister en la recherche des produits semi-directs d'un groupe $\mathbb{Z}/n\mathbb{Z}$ par G, qui passe en effet par l'étude des morphismes de groupes de G dans $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, ce dernier groupe étant isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$.

Deuxième partie
Théorie des anneaux et des corps

4 Développements un peu originaux

4.1 $\mathfrak{S}_p$ est le groupe de Galois d'un certain polynôme de $\mathbb{Q}[X]$

Soit $P \in \mathbb{Q}[X]$. On appelle groupe de Galois de P, qu'on note $Gal(P/\mathbb{Q})$ le groupe suivant :

$$Gal(P/\mathbb{Q}) = \{\sigma : \mathrm{Dec}(P) \to \mathrm{Dec}(P); \quad \sigma \text{ est un automorphisme de corps tel que } \forall x \in \mathbb{Q}, \sigma(x) = x\},$$

où $\mathrm{Dec}(P)$ est le plus petit sous-corps de $\mathbb{C}$ contenant les racines de P.

Théorème 4.1. [6] *Soit p un nombre premier impair. Il existe un polynôme irréductible $P \in \mathbb{Q}[X]$ tel que son groupe de Galois soit isomorphe à $\mathfrak{S}_p$.*

On commence par le lemme suivant (on verra que le polynôme qui y figure répondra aux exigences du théorème) :

Lemme 4.2. *Il existe un polynôme $P \in \mathbb{Q}[X]$ irréductible possédant exactement $p-2$ racines réelles distinctes et 2 racines complexes.*

Preuve. On part de :

$$P_0 = \prod_{i=1}^{p-2}(X+i)(X^2+1),$$

qu'on rend irréductible sans trop changer ses racines en utilisant le critère d'Eisentein comme suit. Soit $Q \in \mathbb{Z}[X]$ tel que $P_0 + Q = X^p - p$. On considère alors :

$$P_k(X) = (kp^2+1)P_0 + Q \in \mathbb{Z}[X],$$

de sorte que $P_k \equiv P_0 + Q[p^2]$. Ainsi, d'après le critère d'Eisentein, P_k est irréductible (dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$, étant unitaire).

De plus, d'une part les zéros de $P_0 + Q/(kp^2+1)$ sont les même que ceux de P_k et d'autre part $P_0 + Q/(kp^2+1)$ tend uniformément vers P_0 uniformément sur tout compact du plan complexe. D'après le théorème de Rouché, il existe k tel que les racines de $P_0 + Q/(kp^2+1)$ aient ses racines dans les disques de la figure 1.

Vérifions que ce P_k convient. Chaque disque centré sur l'axe des abscisses contient un unique zéro (par construction de k) qui est nécessairement réel, car sinon son conjugué serait également racine et on pourrait trouver deux zéros distincts dans l'un de ses disques. Les deux disques restants contiennent chacun un unique zéro de P_k et ces deux zéros sont forcément conjugués. ■

Preuve du théorème. On vérifie que le polynôme P_k (de degré p) obtenu dans le lemme précédant convient. Notons α_1, α_2 les racines complexes non réelles de P et $\alpha_3, \ldots, \alpha_p$ les autres[7], $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_p)$ le corps de décomposition de P sur $\mathbb{Q}$.

[6] Proposé à la préparation d'Ulm par Nicolas Tholozan.

[7] Une remarque en passant : changer la numérotation des racines ne fera que conjuguer les groupes de Galois obtenus dans ce qui suit.

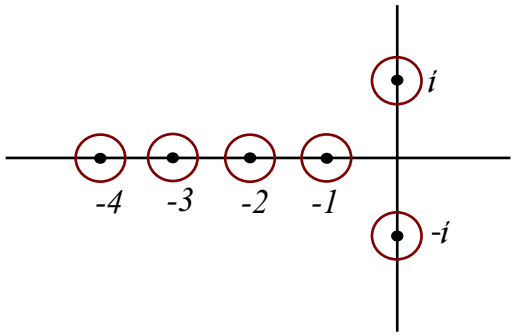

FIG. 1 – Lieux espérés des zéros de P_k.

Lemme 4.3. *Le groupe $Gal(P/\mathbb{Q})$ agit fidèlement transitivement sur les racines $Z = \{\alpha_1, \alpha_2, \dots, \alpha_p\}$ de P_k.*

Preuve. Remarquons tout d'abord que $Gal(P/\mathbb{Q})$ agit bien sur l'ensemble des racines Z, puisque si $P(\alpha_i) = 0$ et $\sigma \in Gal(P/\mathbb{Q})$, alors :

$$\sigma(P(\alpha_i)) = P(\sigma(\alpha_i)) = 0,$$

car $P \in \mathbb{Q}[X]$ et tout élément de $Gal(P/\mathbb{Q})$ fixe $\mathbb{Q}$.

L'action est fidèle car si un élément de $Gal(P/\mathbb{Q})$ fixe tous les α_i, alors il fixe L tout entier, de sorte que c'est en fait l'identité. Ainsi, nous pouvons identifier $Gal(P/\mathbb{Q})$ au sous-groupe de $\mathfrak{S}_{\{\alpha_1,\dots,\alpha_p\}} \simeq \mathfrak{S}_k$ de la manière usuelle (rappelons que se donner une action de G sur X revient à se donner un morphisme de G dans $\mathfrak{S}_X$), ce qu'on fera par la suite.

Soient $i \neq j$. Comme P est irréductible, il existe[8] $\phi : \mathbb{Q}(\alpha_i) \to \mathbb{Q}(\alpha_j)$ automorphisme de corps stabilisant $\mathbb{Q}$ et envoyant α_i sur α_j. D'où le joli diagramme :

$$\begin{array}{ccc} \mathbb{Q}(\alpha_i) & \to & L \\ \phi \downarrow & & \vdots \\ \mathbb{Q}(\alpha_j) & \to & L \end{array}$$

Mais, d'une part L est le corps de décomposition de P sur le corps $\mathbb{Q}(\alpha_i)$, d'autre part L est le corps de décomposition de $\phi(P) = P$ sur le corps $\mathbb{Q}(\alpha_j)$. D'après le résultat d'unicité des corps de décomposition, il existe un autormorphisme du corps L, noté ψ, qui prolonge ϕ. Comme $\psi(\alpha_i) = \alpha_j$, l'action décrite précédemment est transitive sur Z. ■

Nous sommes maintenant en mesure de pouvoir achever la preuve du théorème. Tout d'abord, la conjugaison complexe induit un élément de $Gal(P/\mathbb{Q})$ de sorte que $Gal(P/\mathbb{Q})$ contient une transposition. Ensuite, en notant $\Theta(\alpha_1)$ l'orbite de α_1, nous avons :

$$p = |\Theta(\alpha_1)| = \frac{|G|}{|Stab(\alpha_1)|}.$$

[8]Remarquer que c'est cet argument qu'on utilise lorsqu'on construit un corps de rupture d'un polynôme *irréductible*.

De ceci nous déduisons que p divise $|G|$. Par suite, d'après un résultat de Cauchy, G contient un élément d'ordre p, donc un p-cycle (car G est un sous-groupe de $\mathfrak{S}_p$) noté σ.

Montrons finalement que $Gal(P/\mathbb{Q}) \simeq \mathfrak{S}_p$. Soit $k \in \mathbb{N}^*$ tel que $\sigma^k(\alpha_1) = \alpha_2$. Par primalité[9] de p, σ^k est soit l'identité, soit un p cycle. Comme $\alpha_1 \neq \alpha_2$, σ^k est un p-cycle. Mais il est classique que la transposition (12) et le p-cycle $(12\dots p)$ engendrent $\mathfrak{S}_p$, ce qui conclut. ■

Références. Il n'y en a pas, si ce n'est des partielles, mais ce développement s'apprend aisément. Pour la transitivité évoquée dans le lemme, voir l'ouvrage de Théorie de Galois de Cox ou de Stewart. Pour l'argument final, c'est fait pour $p = 5$ dans le Stewart si je ne m'abuse.

Remarques.

1. J'aime beaucoup ce développement qui mélange beaucoup de domaines (théorie des polynômes, des corps, des groupes :-)) et je trouve l'argument des disques particulièrement élégant !
2. La construction est quasi-explicite, il suffit de choisir k suffisamment grand.
3. L'argument ne fonctionne pas dans le cas général (exercice : trouver un entier n, une transposition et un n-cycle de $\mathfrak{S}_n$ qui n'engendrent pas $\mathfrak{S}_n$), mais le résultat est vrai. C'est évidemment plus délicat (se référer au Cox par exemple).
4. Ainsi, il existe des polynômes non résolubles par radicaux de degré aussi grand qu'on veut.
5. Nous avons fait de la théorie de Galois sans vraiment le dire ; en particulier, nous n'avons rien admis :-) !

[9] Remarquer que c'est le seul endroit où on utilise ce fait.

4.2 Théorèmes de Chevalley-Warning et EGZ

Le but de ce développement[10] est de démontrer le théorème d'Erdös-Ginzburg-Ziv en usant du théorème de Chevalley-Warning. Ici, p désigne un nombre premier et $[n]$ l'ensemble $\{1, 2, \dots, n\}$.

Théorème 4.4 (Chevalley-Warning)**.** *Soit q une puissance de p et (f_α) une famille d'éléments de $\mathbb{F}_q[X_1, \dots, X_n]$ telle que :*

$$\sum deg\ f_\alpha < n.$$

Notons V l'ensemble des zéros communs des f_α. Alors :

$$|V| \equiv 0\,[p].$$

Preuve. Voir le cours d'arithmétique de Serre (pp. 12-12). ■

Théorème 4.5 (EGZ)**.** *Soit $n \geq 1$ et $a_1, \dots, a_{2n-1}$ des entiers. Alors il existe des indices $i_1, \dots, i_n$ tels ques :*

$$a_{i_1} + \cdots + a_{i_n} \equiv 0\,[n].$$

Preuve. On se ramène au cas où n est premier et nous conclurons en utilisant le théorème précédent.

Supposons que l'énoncé soit vrai pour des entiers m, n et montrons le pour mn. Soient donc $a_1, \dots, a_{2mn-1}$ des entiers. Prenons en $2n-1$ (disons les $2n-1$ premiers pour fixer les idées) et choisissons n indices $I_1 \subset [2mn-1]$ de sorte que :

$$\sum_{i \in I_1} a_i \equiv 0\,[n].$$

Considérons ensuite les entiers (a_i) avec i parcourant $[2mn-1]\backslash I_1$. Prenons en $2n-1$ et choisissons n indices $I_2 \subset [2mn-1]\backslash I_1$ de sorte que :

$$\sum_{i \in I_2} a_i \equiv 0\,[n].$$

Terminons ce procédé avoir choisi les indices I_{2m-1}, ce qui es possible car au bout de $2m-2$ étapes, il reste $2mn - 1 - n(2m-2) = 2n-1$ entiers. Pour $j \in [2m-1]$, soit c_j défini par :

$$\sum_{i \in I_j} a_i = nc_j.$$

Extrayons finalement de $[2m-1]$ un sous-ensemble d'indices J tel que $\sum_{j \in J} c_j$ soit divisible par m. Alors :

$$\sum_{j \in J} \sum_{i \in I_j} a_i \equiv 0\,[mn],$$

ce qui montre que ces mn derniers entiers répondent aux exigences imposées.

[10] Proposé à la préparation d'Ulm par Samuel Baumard.

Prouvons maintenant le théorème pour p premier. Nous travaillons désormais dans $\mathbb{F}_p$ et considérons :

$$f_1 = \sum_{i=1}^{2p-1} a_i X_i^{p-1} \qquad \text{et} \qquad f_2 = \sum_{i=1}^{2p-1} X_i^{p-1}.$$

Comme $\deg(f_1) + \deg(f_2) = 2p - 2 < 2p - 1$ (le nombre de variables), le théorème de Chevalley-Warning s'applique. En reprenant ses notations, p divise $|V|$. Or $(0, \dots, 0) \in V$. Donc $|V| \geq 2$. Il existe donc $(x_1, \dots, x_{2p-1}) \in \mathbb{F}_p^{2p-1}$ non nul tel que pour $i = 1, 2$, $f_i(x_1, \dots, x_{2p-1}) = 0$. Or $x^{p-1} = 1$ si, et seulement si x est non nul. On en déduit qu'il existe $i_1, \dots, i_p$ tels que $x_k = 1$ si k est l'un des i_j et 0 sinon. Il suffit alors d'écrire que $f_1(x_1, \dots, x_{2p-1}) = 0$ pour conclure. ■

Référence. Pour EGZ, se référer à *Additive number theory* , Nathanson, pp. 50-51.

Remarques.

1. La conclusion du théorème de Chevalley-Warning peut être remplacée par la conclusion plus forte : « q divise $|V|$ », mais c'est beaucoup plus délicat.
2. Il n'existe pas de démonstration simple d'EGZ.

5 Développements moins originaux

5.1 Le problème des pièces de monnaie

Théorème 5.1. *Soient $\alpha_1, \dots, \alpha_p \in \mathbb{N}^*$ des entiers premiers entre eux. Notons :*

$$N_n = |\{(n_1, \dots, n_p) \in \mathbb{N}^p; \quad n_1\alpha_1 + \cdots + n_p\alpha_p = n\}|.$$

Alors :

1. *Si $p = 2$, en notant $a = \alpha_1$ et $b = \alpha_2$, alors $N_n > 0$ pour $n \geq (a-1)(b-1)$ et $N_{(a-1)(b-1)-1}$. De plus, entre 0 et $(a-1)(b-1)-1$, exactement la moitié des entiers est représentable (k est dit représentable sir $N_k > 0$).*
2. *Lorsque n tend vers $+\infty$:*
$$N_n \sim \frac{1}{\alpha_1 \cdots \alpha_p} \frac{n^{p-1}}{(p-1)!}.$$
En particulier, N_n est non nul à partir d'un certain rang.

Preuve. 1. Soit $n \geq 0$ et écrivons la décomposition de Bézout $n = xa + yb$ en imposant la condition $0 \leq x < b$, de sorte que cette écriture est unique. Remarquons ensuite que n est représentable si, et seulement si $y \geq 0$. Ainsi, le plus grand entier non représentable est $(b-1)a - b$, qu'on note $\kappa - 1$ avec $\kappa = (a-1)(b-1)$. De plus, $n' = \kappa - 1 - m = (b-1-x)a + (-1-y)b$ avec $0 \leq b-1-x < b$. Donc, pour $n \leq \kappa - 1$, n est représentable si, et seulement si, n' ne l'est pas.

2. Voir le Gourdon d'analyse, p. 97.

■

Références. Pour le premier point, *Generatingfunctionology* de Wilf (p. 97). Pour le second, voir le Gourdon d'analyse, p. 97.

Remarque. Le deuxième point est classique, mais un peu trop court pour constituer un développement à part entière. Le premier point permet alors d'ajouter une légère touche d'originalité à la chose.

5.2 Autour de la mesure de Mahler

Théorème 5.2. *Soit $P \in \mathbb{C}[X]$ unitaire. On note $z_1, \dots, z_n$ ses racines,*

$$||P|| = \sqrt{\sum_{i=0}^{n} |a_i|^2} \qquad et \qquad M(P) = \prod_{|z_i| \geq 1} |z_i|,$$

appelée mesure de Mahler *de P.*

1. *On a $M(P) \leq ||P||$.*
2. *Si $P \in \mathbb{Z}[X]$, $P(0) \neq 0$ et $M(P) = 1$, alors tous les z_i sont de module un (ce qui implique que P est produit de polynômes cyclotomiques).*

Référence. Oraux X-ENS, algèbre 1.

Remarques.

1. Le défaut de ce développement est qu'il constitué de deux résultats indépendants.
2. L'intérêt provient de la conjecture suivante (Lehmer, 1933) :

$$\liminf_{P \in \mathbb{Z}[X], \text{unitaire}, M(P) > 1} M(P) > 1,$$

et cette liminf serait atteinte pour $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$, dont la mesure de Mahler vaut environ $1,176$.

6 Développements plus classiques

6.1 Irréductibilité des polynômes cyclotomiques

Ici n est un entier non nul fixé.

Définition 6.1. Notons μ_n^* l'ensemble des racines primitives n-ièmes de l'unité :

$$\mu_n^* = \{e^{\frac{2ik\pi}{n}}; \quad 1 \leq k \leq n,\, k \wedge n = 1\},$$

et définissions ϕ_n le n-ième polynôme cyclotomique par :

$$\phi_n(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta) \in \mathbb{C}[X].$$

Lemme 6.2. *Les assertions suivantes sont vérifiées :*

1. *Considérons le polynôme $X^n - 1 \in \mathbb{F}_p[X]$ où p est un nombre premier ne divisant pas n. Alors ses racines sont simples dans un corps de décomposition.*
2. *On a :*
$$X^n - 1 = \prod_{d|n} \phi_d(X).$$
3. *Le polynôme $\phi_n(X)$ est en fait unitaire à coefficients entiers.*

Théorème 6.3. *Le polynôme ϕ_n est irréductible sur $\mathbb{Q}[X]$.*

Référence. La preuve est assez détaillée dans le cours d'Algèbre de Perrin (voir cependant les remarques qui suivent).

Remarques.

1. Ce résultat implique que la degré de l'extension $\mathbb{Q}[e^{\frac{2i\pi}{n}}]/\mathbb{Q}$ est de degré $\phi(n)$. Ceci est utile pour trouver tous les polygones réguliers constructibles à la règle et au compas. Les polynômes cyclotomiques interviennent plus généralement en théorie algébrique des nombres (voir par exemple *A classical introduction to modern number theory* de Ireland et Rosen ou *Théorie algébrique des nombres* de Samuel).
2. Bien que ce développement soit classique, quelques points méritent d'être soulignés. Tout d'abord, la factorialité de $\mathbb{Z}[X]$ n'intervient pas dans la preuve du lemme mais lors de la preuve du théorème via le lemme suivant (dont la preuve utilise le théorème de Gauss (celui avec le contenu des polynômes)) :

   Lemme 6.4. *Soient $P, Q \in \mathbb{Q}[X]$,* unitaires*, tels que $PQ \in \mathbb{Q}[X]$. Alors $PQ \in \mathbb{Z}[X]$.*

   La remarque suivante est également utilisée : si $\zeta, \zeta' \in \mu_n^*$, alors il existe $m \in \mathbb{N}^*$ tel que $\zeta' = \zeta^m$ et $m \wedge n = 1$.

Troisième partie
Algèbre linéaire et multi-linéaire

7 Développements un peu originaux

7.1 Décomposition de Dunford généralisée

Ce développement [11] vise à donner une version générale de la décomposition de Dunford valable sur n'importe quel corps parfait. Ici, k est un corps et E un k-ev de dimension finie.

Définition 7.1. Un corps k est dit *parfait* si n'importe quel polynôme irréductible sur k est scindé à racines simples dans un corps de décomposition.

Définition 7.2. Un endomorphisme $u \in \mathcal{L}(E)$ est dit *semi-simple* si son polynôme minimal Π_u est sans facteur carré.

Théorème 7.3 (Décomposition de Dunford généralisée)**.** *Soit E un k-ev de dimensions finie n. Supposons que k soit parfait. Alors il existe un unique couple (d, n) d'endomorphismes de E tels que :*

1. *$u = d + n$*
2. *d est semi-simple et n nilpotent.*
3. *d et n commutent.*

De plus, d et n sont des polynômes en u (à coefficients dans k)

Commençons par montrer deux lemmes (qui sont importants en soi).

Lemme 7.4. *Soit K un corps, $S \in K[X]$ un polynôme de degré $n \geq 2$ et L un corps de décomposition de S sur K. Soit $x \in L \backslash K$ et P le polynôme minimal de x sur K. Alors P est scindé[12] (vu comme élément de $L[X]$)*

Preuve. Écrivons $L = K(\alpha_1, \ldots, \alpha_n)$ et $x = R(\alpha_1, \ldots, \alpha_n)$ avec $R \in K[X_1, \ldots, X_n]$. Soit :

$$\widetilde{P} = \prod_{\sigma \in \mathfrak{S}_n} \left(X - R(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})\right).$$

Il suffit de montrer que $\widetilde{P} \in K[X]$ car ce dernier polynôme, scindé sur L, annulerait x, donc P diviserait $\widetilde{P}$ et P serait lui aussi scindé sur L.

Écrivons :

$$\prod_{\sigma \in \mathfrak{S}_n} \left(X - R(X_{\sigma(1)}, \ldots, X_{\sigma(n)}\right) = \sum_{i=1}^{n!} P_i(X_1, \ldots, X_n) X^i,$$

avec $P_i \in K[X_1, \ldots, X_n]$ des polynômes manifestement symétriques. Notons $\sigma_1, \ldots, \sigma_n$ les polynômes symétriques élémentaires. Il existe donc des polynômes $Q_j \in K[X_1, \ldots, X_n]$ tels que pour tout i :

$$P_i = Q_i(\sigma_1, \ldots, \sigma_n).$$

[11] D'après une discussion entre Nicolas Tholozan et moi.

[12] Il est clair que $P \in K[X]$, mais toutes ses racines n'ont, a priori, aucune raison d'appartenir à L.

Fixons i. Ainsi :

$$P_i(\alpha_1, \dots, \alpha_n) = Q_i(\sigma_1(\alpha_1, \dots, \alpha_n), \dots, \sigma_n(\alpha_1, \dots, \alpha_n)).$$

Or $\sigma_i(\alpha_1, \dots, \alpha_n)$ est, au signe près, le i-ième coefficient de S, donc est dans K. En conclusion, $P_i(\alpha_1, \dots, \alpha_n) \in K$ et nous avons bien obtenu le résultat désiré. ■

Définition 7.5. Soit L un surcorps du corps K. Notons :

$$Gal(L/K) = \{\sigma : L \to L; \quad \sigma \text{ est un automorphisme de corps tel que } \forall x \in K, \sigma(x) = x\},$$

qui coincide avec $Gal(P/\mathbb{Q})$ défini dans un développement précédent lorsque $K = \mathbb{Q}$ et $L = \mathrm{Dec}(P)$.

Lemme 7.6 (même notations que dans le lemme précédent)**.** *Soit $x \in L \backslash K$. Alors il existe $\sigma \in Gal(L/K)$ tel que $\sigma(x) \neq x$.*

Preuve. L'idée est la suivante : de toute façon, σ envoie x sur une autre racine du polynôme minimal de x. Le caractère parfait du corps et le premier lemme vont nous permettre de trouver une telle racine distincte de x, disons x'. Nous allons donc envoyer x sur x' et prolonger ensuite cet automorphisme à L tout entier.

Rappelons que P désigne le polynôme minimal de x sur K. Comme $x \in K$, le degré de P est supérieur ou égal à 2. Comme K est parfait, d'après le premier lemme, P est à racines simples dans L. Il existe donc $x' \neq x$ tel que $P(x') = 0$ avec $x' \in L$. Nous avons donc affaire au diagramme suivant[13] :

$$\begin{array}{ccc} K[x] & \to & L \\ \phi \downarrow & & \vdots \\ K[x'] & \to & L \end{array}$$

où $\phi(x) = x'$. Mais, d'une part L est le corps de décomposition de P sur le corps $K[x]$, d'autre part L est le corps de décomposition de $\phi(P) = P$ sur le corps $K[x']$. D'après le résultat d'unicité des corps de décomposition, il existe un autormorphisme du corps L, noté σ, qui prolonge ϕ. Comme $\sigma(x) = x' \neq x$, le lemme en découle. ■

Preuve du théorème. Traitons le problème matriciellement. Soit $(e_i)_i$ une base de E et U la matrice de u dans cette base. Soit $\chi_u \in K[X]$ le polynôme caractéristique de u et L un corps de décomposition de χ_u sur K. Ainsi, d'après la décomposition de Dunford usuelle, il existe un unique couple de matrices $(D, N) \in \mathcal{M}_n(L)$ telles que :

1. $U = D + N$
2. D est semi-simple et N nilpotent.
3. D et N commutent.

De plus, D et N sont des polynômes en U (à coefficients dans L).

Soit maintenant $\sigma \in Gal(L \backslash K)$. Comme $U \in \mathcal{M}_n(K)$:

$$U = \sigma(U) = \sigma(D) + \sigma(N).$$

Or σ est un automorphisme du corps L. Ainsi :

[13] Rappelons que l'irréductibilité de P implique que $K[x]$ et $K[X']$ sont des corps.

1. $\sigma(N)$ est nilpotent
2. D est semi-simple, donc son polynôme minimal est sans facteur carré. Or ce dernier polynôme divise le polynôme caractéristique de D qui est celui de U, donc χ_U. Or χ_U est scindé sur L (par choix de L !). Finalement, D est scindé à racines simples sur L, donc diagonalisable dans L. Donc D s'écrit $D = PD'P^{-1}$, avec D' diagonale. Mais alors :

$$\sigma(D) = \sigma(P)\sigma(D')\sigma(P)^{-1},$$

   ce qui entraîne que $\sigma(D)$ est diagonalisable, donc semi-simple.
3. $\sigma(D)$ et $\sigma(N)$ commutent.

Par *unicité* de la décomposition de Dunford usuelle, $\sigma(D) = D$ et $\sigma(N) = N$. Le deuxième lemme permet de conclure.

Il reste à voir que D est un polynôme en U (on procéderait de même pour N). Écrivons $D = T(U)$ avec $T \in L[X]$ et notons Π l'endomorphisme de L qui est la projection sur K parallèlement à un supplémentaire de K. Alors :

$$D = \Pi(D) = \Pi(T(U)) = (\Pi T)(U),$$

ce qui conclut. ■

Références. Il n'y a pas de référence universelle pour ce développement, mais des références correspondant aux différentes étapes.

1. Pour tout ce qui concerne les corps parfaits et les endomorphismes semi-simples se référer à *Objectif Agrégation* (Beck et al.).
2. Pour le premier lemme (qui dit qu'une extension de type (corps de décomposition/corps) est normale), voir le livre de Stewart sur la théorie de Galois.
3. Pour le deuxième lemme (cas particulier de la correspondance de Galois), voir le livre de Cox sur la théorie de Galois.

Remarques.

1. On peut montrer que k est parfait si et seulement k est de caractéristique nulle ou bien le l'élévation à la puisssance p-ième (le « Frobenius ») est bijectif. Par exemple, tout corps fini est parfait, mais $\mathbb{F}_p(T)$ ne l'est pas ($X^p - T \in \mathbb{F}_p(T)[X]$ est irréductible sur $\mathbb{F}_p(T)$, mais possède une seule racine dans un corps de décomposition).
2. On peut montrer que u est semi-simple si, et seulement si, tout sev de E stable par u admet un supplémentaire stable par u.
3. L'intérêt de cette décomposition est surtout théorique, mais je trouve la méthode mise en jeu très intéressante : en considérant un corps de décomposition, on se ramène à un cas connu, puis on montre que tout se passe ne fait dans le corps de base grâce à une certaine « symétrie ». Bref, il s'agit d'un de mes développements préférés :-).
4. Ce résultat est faux en général. En effet, prenons $k = \mathbb{F}_p(T)$ qui n'est pas parfait. Considérons $P = X^p - T$, irréductible, puis le k-ev $k[X]/(P^2)$, noté E. Soit u l'endomorphisme de E correspondant à la multiplication par (la classe de) X. Remarquons que le polynôme minimal de u est P^2.

Dans le dessein d'obtenir une contradiction, supposons que $u = d+n$ soit la décomposition de Dunford généralisée de u. Alors le polynôme caractéristique de u, et donc de d, est P^2. Donc le polynôme minimal de d divise P^2. Or celui-ci est sans facteur carré car d est semi-simple. Donc le polynôme minimal de d est P. Donc $k[d]$ est un corps. Comme d et n commutent, n peut être vu comme un endomorphisme de E vu comme $k[d]$ espace vectoriel. De plus, la dimension de E sur $k[d]$ est p. Ceci implique que $n^p = 0$. Finalement :

$$u^p - T = (d+n)^p - T = d^p + n^p - T = P(d) = 0.$$

Donc $P(u) = 0$, ce qui en contradiction avec le fait que le polynôme minimal de u est P^2.

Pour plus de précisions, le lecteur pourra consulter la RMS, numéro **117-2** (janvier 2007), pp. 10-22.

7.2 Le critère de nilpotence de Cartan

Ce développement donne un critère de nilpotence utile en théorie des algèbres de Lie.

Théorème 7.7. *Soit k un corps algébriquement clos de caractéristique nulle, V un k-ev de dimension finie notée n et $A \subset B \subset \mathcal{L}(V)$ des sev de $\mathcal{L}(V)$. On pose :*

$$M = \{x \in \mathcal{L}(V); \quad [x, B] \subset A\}.$$

Soit $x \in M$. On suppose que pour tout $y \in M$, $tr(xy) = 0$. Alors x est nilpotent.

Preuve. Remarquons tout d'abord que pour $A = B = \mathcal{L}(V)$, l'énoncé est vérifié car x est alors nul.

Dans le cas général, soit $x \in M$ vérifiant les conditions de l'énoncé et écrivons la décomposition de Dunford de x sous la forme $x = d + n$ avec d diagonalisable, n nilpotente avec $d \circ n = n \circ d$. Afin de montrer que x est nilpotente, nous allons montrer que $d = 0$. Traitons le problème matriciellement en choisissant une base $\beta = (e_1, \dots, e_n)$ de V telle que $\mathrm{Mat}_\beta(n)$ soit trigonale supérieure et telle que :

$$\mathrm{Mat}_\beta(d) = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \vdots \\ \vdots & 0 & a_{n-1} & 0 \\ 0 & \cdots & 0 & a_n \end{pmatrix}$$

où les a_i sont rationnels (en effet, k étant de caractéristique nulle, son sous-corps premier est $\mathbb{Q}$). Considérons $E = \mathrm{Vect}_{\mathbb{Q}}(a_1, \dots, a_n)$. Nous allons montrer que $E = 0$ en montrons que le dual de E, E^*, est réduit à $\{0\}$.

Soit donc $f \in E^*$; il s'agit donc de montrer que $f = 0$. Introduisons l'endomorphisme $y \in \mathcal{L}(E)$ tel que :

$$\mathrm{Mat}_\beta(y) = \begin{pmatrix} f(a_1) & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \vdots \\ \vdots & 0 & f(a_{n-1}) & 0 \\ 0 & \cdots & 0 & f(a_n) \end{pmatrix}.$$

Admettons pour l'instant que $y \in M$. Alors $\mathrm{tr}(xy) = \mathrm{tr}(dy) = \sum_i f(a_i)a_i$, de sorte que :

$$0 = f\left(\sum_{i=1}^{n} f(a_i)\right) = \sum_{i=1}^{n} f(a_i)^2,$$

grâce à la linéarité de f. Comme $f(a_i) \in \mathbb{Q}$, il vient que pour tout i, $f(a_i) = 0$ et donc $f = 0$.

Il reste donc à montrer que $y \in M$. Pour $u \in \mathcal{L}(E)$, notons ad_u l'endomorphisme de $\mathcal{L}(E)$ (et donc l'élement de $\mathcal{L}(\mathcal{L}(E))$) défini par :

$$\begin{aligned} ad_u : \mathcal{L}(E) &\to \mathcal{L}(E) \\ s &\mapsto us - su, \end{aligned}$$

Nous voulons montrer que $ad_y(B) \subset A$ en sachant que $ad_x(B) \subset A$. Nous allons y parvenir en recherchant un lien entre ad_y et ad_x. Tout d'abord, ad_y est diagonalisable, et ses valeurs propres, au nombre de n^2, sont les $f(a_i) - f(a_j) = f(a_i - a_j)$ avec i, j entiers entre 1 et n. En effet,

dans la base de $\mathcal{L}(E)$ définie par $(e_i(e_j)^t)_{i,j}$, ad_y est diagonale, d'entrées $f(a_i - a_j)$. De même, ad_d est diagonalisable et ses valeurs propres sont les $a_i - a_j$. Il existe par suite un polynôme d'interpolation de Lagrange $P \in k[X]$ tel que $ad_y = P(ad_d)$ avec $P(0) = 0$.

Or la décomposition de Dunford de ad_x est $ad_x = ad_d + ad_n$ (pourquoi ?). Il existe donc $Q \in k[X]$ tel que $ad_d = Q(ad_x)$ et $Q(0) = 0$. Cela implique que $ad_y = PQ(ad_x)$. D'où :

$$ad_y(B) = PQ(ad_x)(B) \subset A,$$

car $ad_x(B) \subset A$ et par récurrence, pour $i \geq 0$:

$$(ad_x)^{(i+1)}(B) \subset (ad_x)^{(i)}(A) \subset (ad_x)^{(i)}(B) \subset A$$

. ■

Références. Voir « Introduction to Lie Algebras and Representation Theory » p. 19 (Humphreys) ou un exercice d'« Objectif Agrégation » (Beck et al.), où la preuve est particulièrement bien expliquée.

Remarques.

1. Nous avons utilisé que si $x = d + n$ est la décomposition de Dunford de x, alors celle de ad_x est $ad_x = ad_d + ad_n$. Il a été vu que ad_d est diagonalisable. Il est facile de voir que ad_d et que ad_n commutent (car d et n commutent) et que ad_n est nilpotent, comme différence de deux endomorphismes nilpotents qui commutent entre eux ; ce qui démontre l'énoncé cité.
2. Rappelons que si $u = d + n$ est la décomposition de Dunford de u sur un k-ev E de dimension finie avec k algébriquement clos, il existe $Q \in k[X]$ tel que $d = Q(u)$ *et* $Q(0) = 0$ (voir par exemple le Beck). Cette légère amélioration de la décomposition de Dunford citée usuellement est fondamentale ici.
3. Ce développement illustre, assez élégamment à mon avis, l'utilisation de la dualité et de la décomposition de Dunford de l'application adjointe.
4. Ce théorème est utile dans la théorie des algèbres de Lie (il permet d'établir qu'une algèbre de Lie est semi-simple si, et seulement si, sa forme quadratique de Killing est non dégénerée).
5. Lorsque j'ai proposé ce développement à mon oral d'agrégation (qui portait sur les espaces vectoriels de dimension finie), on m'a demandé : de quel Cartan s'agit-il ?
6. La caractéristique nulle de k est fondamental dans la preuve (on a utilisé que si $x \in \mathbb{Q}$ vérifie $x^2 = 0$, alors $x = 0$). A-t-on besoin du fait que k est algébriquement clos ?

7.3 L'image de $M_n(\mathbb{R})$ par l'exponentielle

7.4 Le théorème de l'amitié

Ce développement [14] utilise un argument d'algèbre linéaire pour répondre à un problème combinatoire.

Théorème 7.8 (∼1960)**.** *Soit G un graphe fini tel que deux sommets distincts quelconques aient exactement un voisin en commun. Alors il existe un sommet adjacent à tous les autres.*

Preuve. La démonstration consiste à raisonner par l'absurde en montrant d'abord que tous les sommets ont même degré par un argument combinatoire. On introduit ensuite la matrice d'adjacence du graphe (qui est réelle symétrique), on la diagonalise et on aboutit à une contradiction. ■

Référence. Le chapitre consacré au *théorème de l'amitié* dans « Raisonnements divins »(Aigner et al.). La preuve y est limpide.

Remarques. Je trouve que cette démonstration illustre de manière élégante l'utilisation d'algèbre linéaire (diagonalisation d'une matrice symétrique réelle) en combinatoire.

[14] Proposé à la préparation d'Ulm par Oriane Blondel.

8 Développements moins originaux

8.1 Sous-algèbre de Lie de $\mathcal{L}(E)$ formée de diagonalisables

8.2 Théorème d'Engel

9 Développements plus classiques

9.1 Facteurs invariants

9.2 Lemmes de Dedekind et d'Artin

Quatrième partie
Groupes orthogonaux

10 Développements un peu originaux

10.1 $O(p,q)$ a quatre composantes connexes

10.2 Normes euclidiennes en dimension 2

11 Développements moins originaux

11.1 Points extrémaux de la boule unité de $\mathcal{L}(E)$

Ce développement [15]

11.2 Simplicité de $PSO_n(\mathbb{R})$

12 Développements plus classiques

12.1 Ellipsoïde de John

12.2 Sous-groupes compacts de $GL_n(\mathbb{R})$

[15] Proposé à la préparation d'Ulm par Robin Stephenson.

Cinquième partie
Formes quadratiques

13 Développements un peu originaux

13.1 Théorème de Milnor

13.2 Entiers algébriques sur un anneau d'entiers

13.3 Théorème de Cassels-Pfister

Ce développement[16]

[16]Proposé à la préparation d'Ulm par Olivier Taïbi.

Sixième partie
Géométrie

14 Développements un peu originaux

14.1 Le petit théorème de Poncelet

Ce développement[17]

14.2 Le groupe circulaire

14.3 Alternative de Steiner

Ce développement[18]

14.4 Théorème de Dandelin

Ce développement[19]

15 Développements plus classiques

15.1 Sous-groupes finis de $SO_3(\mathbb{R})$

15.2 Coloriages du cube

[17] Je dois entièrement ce qui suit à Nicolas Tholozan.
[18] D'après le développement proposé à la préparation d'Ulm par Stéphane Benoist.
[19] Proposé à la préparation d'Ulm par Patrick Hoscheit.

Notations utilisées

$Z(G)$	Centre du groupe G
$\|X\|$	Cardinal de l'ensemble X
$H < G$	H est un sous-groupe du groupe G
$H \lhd G$	H est distingué dans G
$H \not\leq G$	H est un sous-groupe strict de G
$\mathcal{L}(E)$	l'ensemble des endomorphismes de l'espace vectoriel E
$\mathrm{Aut}(G)$	l'ensemble des automorphismes de groupe du groupe G
$\mathfrak{S}_n$	le groupe symétrique à n éléments
A_n	le groupe alterné à n éléments
G/H	l'ensemble quotient de G par H, muni d'une structure naturelle de groupe lorsque $H \lhd G$