Degré d'une somme de nombres algébriques

Le but de cette note est d'expliquer le résultat suivant, dû à Isaacs.

***Théorème 1* (Isaacs, 1970).** — *Soit a et b deux nombres algébriques, de degrés respectifs m et n. Supposons m et n premiers entre eux. Alors $a+b$ est algébrique de degré mn.*

La démonstration d'Isaacs [**1**] permet en fait d'établir le résultat plus fort suivant.

***Théorème 2* (Isaacs, 1970).** — *Soit a et b deux nombres algébriques vérifiant la condition $[\mathbf{Q}(a,b):\mathbf{Q}] = [\mathbf{Q}(a):\mathbf{Q}][\mathbf{Q}(b):\mathbf{Q}]$. Alors $\mathbf{Q}(a,b) = \mathbf{Q}(a+b)$. En particulier, le degré de $a+b$ est égal au produit des degrés de a et de b.*

Expliquons les notations intervenant dans cet énoncé. On note $\mathbf{Q}(a)$ (resp. $\mathbf{Q}(b)$) l'extension de $\mathbf{Q}$ engendrée par a (resp. b), de sorte que $[\mathbf{Q}(a):\mathbf{Q}]$ (resp. $[\mathbf{Q}(b):\mathbf{Q}]$) n'est autre que le degré de a (resp. b), c'est-à-dire le degré de son polynôme minimal sur $\mathbf{Q}$.

L'extension composée $\mathbf{Q}(a,b)$ est définie comme le plus petit corps contenant $\mathbf{Q}(a)$ et $\mathbf{Q}(b)$. L'hypothèse $[\mathbf{Q}(a,b):\mathbf{Q}] = [\mathbf{Q}(a):\mathbf{Q}][\mathbf{Q}(b):\mathbf{Q}]$ signifie que les extension $\mathbf{Q}(a)$ et $\mathbf{Q}(b)$ sont *linéairement disjointes* (on définit traditionnellement la disjonction linéaire par le fait qu'une base de $\mathbf{Q}(a)$ sur $\mathbf{Q}$ est libre sur $\mathbf{Q}(b)$, et vice versa).

Un résultat classique, le *théorème de l'élément primitif*, permet d'affirmer que $\mathbf{Q}(a,b)$ est une extension monogène de $\mathbf{Q}$, c'est-à-dire qu'il existe $c \in \mathbf{Q}(a,b)$ tel que $\mathbf{Q}(a,b) = \mathbf{Q}(c)$. La preuve usuelle de ce théorème montre que l'on peut prendre $c = a + \lambda b$, avec $\lambda \in \mathbf{Q}^*$ non précisé. Peut-on toujours choisir $\lambda = 1$? Le théorème 2 affirme que oui, sous la condition que $\mathbf{Q}(a)$ et $\mathbf{Q}(b)$ sont linéairement disjointes (par suite, dans ce cas, tout $\lambda \in \mathbf{Q}^*$ convient).

Si les degrés de a et b sont premiers entre eux, alors $\mathbf{Q}(a)$ et $\mathbf{Q}(b)$ sont nécessairement linéairement disjointes, puisque $[\mathbf{Q}(a,b):\mathbf{Q}]$ est divisible par $[\mathbf{Q}(a):\mathbf{Q}]$ et par $[\mathbf{Q}(b):\mathbf{Q}]$, donc par leur produit, et que l'on a toujours $[\mathbf{Q}(a,b):\mathbf{Q}] \leq [\mathbf{Q}(a):\mathbf{Q}][\mathbf{Q}(b):\mathbf{Q}]$. Nous voyons donc que le théorème 2 entraîne le théorème 1.

Dans la suite, nous donnons une preuve, due à Isaacs, du théorème 2. Elle fait appel aux groupes de Galois et à leurs représentations, et fournit à mon sens une jolie application de ces théories. L'un des attraits de la preuve est qu'à aucun moment elle ne fait appel à des calculs explicites sur les polynômes.

Démonstration du théorème 2. — Soit A (resp. B) l'ensemble des conjugués de a (resp. b), c'est-à-dire l'ensemble des racines du polynôme minimal de a (resp. b) sur $\mathbf{Q}$. Posons $m = \#A$ et $n = \#B$. Notons $\mathbf{Q}(A,B)$ l'extension engendrée par A et B. C'est une extension finie galoisienne de $\mathbf{Q}$. Nous noterons $G = \mathrm{Gal}(\mathbf{Q}(A,B)/\mathbf{Q})$ son groupe de Galois (qui n'est autre que le groupe des automorphismes de corps de $\mathbf{Q}(A,B)$). Par restriction, on a un morphisme surjectif $G \to \mathrm{Gal}(\mathbf{Q}(A)/\mathbf{Q})$ et il est connu que ce dernier groupe agit transitivement sur A. Par suite G agit transitivement sur A. Il en va de même pour l'action de G sur B.

***Lemme 1*.** — *L'action naturelle de G sur $A \times B$ est transitive.*

Démonstration. — Notons H le stabilisateur de a pour l'action de G sur A, et K le stabilisateur de b pour l'action de G sur B. Remarquons que $H = \mathrm{Gal}(\mathbf{Q}(A,B)/\mathbf{Q}(a))$ et $K = \mathrm{Gal}(\mathbf{Q}(A,B)/\mathbf{Q}(b))$. Le stabilisateur de (a,b) pour l'action de G sur $A \times B$ n'est autre que $H \cap K = \mathrm{Gal}(\mathbf{Q}(A,B)/\mathbf{Q}(a,b))$. Le cardinal de l'orbite $G \cdot (a,b)$ est égal à l'indice de $H \cap K$ dans G, qui est aussi le degré de l'extension $\mathbf{Q}(a,b)$ sur $\mathbf{Q}$. Par hypothèse, ce degré vaut $[\mathbf{Q}(a):\mathbf{Q}][\mathbf{Q}(b):\mathbf{Q}] = mn$. Ainsi $G \cdot (a,b) = A \times B$, de sorte que l'action est transitive. □

Rappelons qu'une représentation de G dans un $\mathbf{Q}$-espace vectoriel V de dimension finie est la donnée d'un morphisme de groupes $\rho : G \to \mathrm{GL}(V)$. Le caractère de (V, ρ) est la fonction $\chi_V : G \to \mathbf{Q}$ définie par $\chi_V(g) = \mathrm{Tr}\,\rho(g)$ pour tout $g \in G$. Si V et W sont deux représentations de G, on note $\mathrm{Hom}_G(V, W)$ l'espace vectoriel des applications linéaires de V dans W qui sont compatibles à l'action de G.

Pour tout ensemble fini E, notons $\mathbf{Q}[E]$ le $\mathbf{Q}$-espace vectoriel abstrait de base E. Si G agit sur E, on étend par $\mathbf{Q}$-linéarité cette action à $\mathbf{Q}[E]$, ce qui fait de $\mathbf{Q}[E]$ une $\mathbf{Q}$-représentation, appelée *représentation de permutation* associée à E. Remarquons que le vecteur $e_E \in \mathbf{Q}[E]$ défini par $e_E = \sum_{x \in E}[x]$ est fixé par G. De plus, on a une décomposition en somme directe $\mathbf{Q}[E] = \mathbf{Q} \cdot e_E \oplus H_E$ où $H_E = \{\sum_{x \in E} \lambda_x [x] \in \mathbf{Q}[E]; \sum_{x \in E} \lambda_x = 0\}$ est stable par G. Enfin, nous noterons χ_E le caractère de $\mathbf{Q}[E]$: pour $g \in G$, on a $\chi_E(g) = \#\{x \in E; gx = x\}$.

Lemme 2. — *Le $\mathbf{Q}$-espace vectoriel $\mathrm{Hom}_G(\mathbf{Q}[A], \mathbf{Q}[B])$ est de dimension 1. Une base en est donnée par l'application linéaire $f : \mathbf{Q}[A] \to \mathbf{Q}[B]$ vérifiant $f(e_A) = e_B$ et $f|_{H_A} = 0$.*

Démonstration. — On vérifie que f est compatible à l'action de G. Comme f est non nulle, il vient $\dim_{\mathbf{Q}} \mathrm{Hom}_G(\mathbf{Q}[A], \mathbf{Q}[B]) \geq 1$.

D'autre part, on a

$$\begin{aligned}\dim_{\mathbf{Q}} \mathrm{Hom}_G(\mathbf{Q}[A], \mathbf{Q}[B]) &= \dim_{\mathbf{C}}(\mathrm{Hom}_G(\mathbf{Q}[A], \mathbf{Q}[B]) \otimes \mathbf{C}) \\ &\leq \dim_{\mathbf{C}} \mathrm{Hom}_G(\mathbf{C}[A], \mathbf{C}[B]).\end{aligned}$$

Il suffit donc de montrer $\dim_{\mathbf{C}} \mathrm{Hom}_G(\mathbf{C}[A], \mathbf{C}[B]) = 1$. Cette dimension peut se calculer à l'aide d'un produit scalaire [**2**, Chap XVIII, Thm 5.17], ce qui donne

$$\begin{aligned}\dim_{\mathbf{C}} \mathrm{Hom}_G(\mathbf{C}[A], \mathbf{C}[B]) &= \frac{1}{\#G} \sum_{g \in G} \chi_A(g)\chi_B(g^{-1}) \\ &= \frac{1}{\#G} \sum_{g \in G} \chi_A(g)\chi_B(g) \\ &= \frac{1}{\#G} \sum_{g \in G} \#\{(x, y) \in A \times B; g(x, y) = (x, y)\} \\ &= \frac{1}{\#G} \sum_{(x,y) \in A \times B} \#\{g \in G; g(x, y) = (x, y)\}.\end{aligned}$$

Puisque l'action de G sur $A \times B$ est transitive (lemme 1), la quantité $\#\{g \in G; g(x, y) = (x, y)\}$ est indépendante de (x, y) et vaut $\frac{\#G}{mn}$, ce qui permet de conclure. □

Notons C l'ensemble des conjugués de $a + b$. On sait que $\#C \leq mn$ et il s'agit de montrer l'égalité. Par l'absurde, supposons donc $\#C < mn$.

Notons $A + B$ l'ensemble des éléments de la forme $x + y$ avec $x \in A$ et $y \in B$. Pour tout $c \in C$, on a $c = g(a + b) = g(a) + g(b)$ avec $g \in G$, de sorte que $C \subset A + B$. Le lemme 1 montre l'inclusion réciproque, d'où $C = A + B$. Considérons l'application surjective $s : A \times B \to C$ qui à (x, y) associe $x + y$. Comme s ne peut être bijective, il existe deux éléments de $A \times B$ ayant même image par s, et comme s est compatible à l'action de G, on trouve finalement $(a', b') \in A \times B$ avec $(a', b') \neq (a, b)$, tel que $a + b = a' + b'$. Notons que l'élément $d = a' - a = b - b'$ est non nul.

Notons V_A (resp. V_B) le sous-$\mathbf{Q}$-espace vectoriel de $\mathbf{C}$ engendré par A (resp. B), et posons $U = V_A \cap V_B$. Les espaces V_A, V_B et U sont stables par G et définissent donc des représentations de G. Remarquons que U est non nul puisque $d \in U$.

Nous utiliserons les résultats suivants sur les $\mathbf{Q}$-représentations de G, pour lesquels nous renvoyons à [**2**, Chap XVIII, §1-2, Thm 2.3] (voir également [**3**, 6.1 et §12]).

(1) Deux $\mathbf{Q}$-représentations de dimension finie de G sont isomorphes si et seulement si leurs caractères sont égaux.

(2) Soit V une $\mathbf{Q}$-représentation de dimension finie de G. Si W est une sous-$\mathbf{Q}$-représentation de V, alors W possède un supplémentaire dans V qui est stable par G.

L'application naturelle « somme » définit des applications linéaires surjectives $\mathbf{Q}[A] \to V_A$ et $\mathbf{Q}[B] \to V_B$ compatibles à l'action de G. En notant N_A et N_B leurs noyaux respectifs, on obtient les suites exactes suivantes de représentations :

$$0 \to N_A \to \mathbf{Q}[A] \to V_A \to 0,$$
$$0 \to N_B \to \mathbf{Q}[B] \to V_B \to 0.$$

En considérant des bases dans lesquelles les matrices sont diagonales par blocs, on montre que $\chi_A = \chi_{N_A} + \chi_{V_A}$ et $\chi_B = \chi_{N_B} + \chi_{V_B}$. D'après le point (1) ci-dessus, il vient $\mathbf{Q}[A] \cong N_A \oplus V_A$ et $\mathbf{Q}[B] \cong N_B \oplus V_B$. Par suite U est isomorphe à la fois à une sous-représentation de $\mathbf{Q}[A]$ et à une sous-représentation de $\mathbf{Q}[B]$. D'après le point (2) ci-dessus, il existe des représentations U_A et U_B de G et des isomorphismes de représentations $\mathbf{Q}[A] \cong U \oplus U_A$ et $\mathbf{Q}[B] \cong U \oplus U_B$. L'application linéaire $\varphi : \mathbf{Q}[A] \to \mathbf{Q}[B]$ définie par $\varphi|_U = \mathrm{id}_U$ et $\varphi|_{U_A} = 0$ appartient à $\mathrm{Hom}_G(\mathbf{Q}[A], \mathbf{Q}[B])$. D'après le lemme 2, on a $\varphi = \mu f$ avec $\mu \in \mathbf{Q}^*$. En particulier $U \cong \mathrm{im}(\varphi) = \mathrm{im}(f) = \mathbf{Q} \cdot e_B$. Il suit que l'action de G sur U est triviale, et donc $U = \mathbf{Q}$.

Revenons aux nombres algébriques. D'après ce qui précède, $a' = a + d$ et $b' = b - d$ avec $d \in \mathbf{Q}^*$. Comme a' est un conjugué de a, il existe $g \in G$ tel que $a' = g(a)$. Alors $g^2(a) = g(a') = g(a) + g(d) = a' + d = a + 2d$ et par une récurrence immédiate, il vient $g^k(a) = a + kd$ pour tout $k \geq 1$, ce qui contredit le fait que les conjugués de a sont en nombre fini. □

Références

[1] I. M. Isaacs – « Degrees of sums in a separable field extension », *Proc. Amer. Math. Soc.* **25** (1970), p. 638–641.

[2] S. Lang – *Algebra*, 3e éd., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[3] J.-P. Serre – *Représentations linéaires des groupes finis*, 5e éd., Hermann, Paris, 1998.

François Brunault • *E-mail :* `brunault@umpa.ens-lyon.fr`, ÉNS Lyon, UMPA, 46 allée d'Italie, 69007 Lyon, France