Autour des sommes et produits d'éléments algébriques

1. Un argument non-constructif

Soit L/K une extension de corps. Si α, β sont deux éléments de L algébriques sur K alors $\alpha+\beta$, $\alpha\beta$ etc. appartiennent à $K(\alpha,\beta)$, qui est une extension finie de K par multiplicativité du degré. En effet, on a

$$[K(\alpha,\beta):K] = [K(\alpha)(\beta):K(\alpha)][K(\alpha):K]$$

et chacun des termes de droite est fini, le premier car comme β est algébrique sur K, il est algébrique sur $K(\alpha)$, et le second car α est algébrique sur K. Donc l'extension $K(\alpha,\beta)/K$ est finie, donc algébrique, donc les éléments $\alpha+\beta$, $\alpha\beta$ etc. sont algébriques sur K.

Cependant, cet argument nous dit seulement que $\alpha+\beta$ admet un polynôme annulateur à coefficients dans K, mais ne nous dit pas comment en trouver un.

2. Un exemple où l'on peut tâtonner

Pour des nombres algébriques de petit degré, on peut parfois s'en sortir même sans méthode systématique, simplement en calculant les puissances successives de l'élément $\alpha+\beta$ par exemple, et en cherchant des relations K-linéaires entre ces puissances.

Par exemple, pour trouver un polynôme annulateur à coefficients dans $\mathbf{Q}$ de $\sqrt{2}+\sqrt{3}$, on peut calculer

$$(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$$
$$(\sqrt{2}+\sqrt{3})^4 = (5+2\sqrt{6})^2 = 49+20\sqrt{6}$$

On voit qu'une combinaison linéaire de la première et de la deuxième équation permet de se débarrasser du $\sqrt{6}$: en effet

$$(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 = -1$$

ce qui montre que X^4-10X^2+1 est un polynôme annulateur de $\sqrt{2}+\sqrt{3}$ à coefficients dans $\mathbf{Q}$.

3. Calcul pratique de polynômes annulateurs à l'aide du théorème de Cayley-Hamilton

Cette méthode est tirée de l'exercice 1 de la feuille de TD de Jean-François Dat accessible ici : https://webusers.imj-prg.fr/~jean-francois.dat/enseignement/Galois/TD23.pdf

Soit L/K une extension de corps, et $\alpha \in L$ un élément algébrique sur K. L'application de L dans $\mathrm{End}_K(L)$ qui à x associe m_x (l'application linéaire de L dans L de multiplication par x) est un morphisme de K-algèbres, donc pour tout $f \in K[X]$, on a $f(m_x) = m_{f(x)}$. En particulier, si on prend pour f le polynôme caractéristique χ de m_α, on aura $\chi(m_\alpha)=0$ d'après le théorème de Cayley-Hamilton, et donc $m_{\chi(\alpha)}=0$. Or la multiplication par x est l'application linéaire nulle si et seulement si x est nul (cela vient aussi du fait qu'on a un morphisme d'algèbres, donc les inversibles de L sont envoyés sur les inversibles de $\mathrm{End}_K(L)$), donc $\chi(\alpha)=0$ et on a bien trouvé un polynôme annulateur de α à coefficients dans K.

Exemple 3.1. Déterminons un polynôme à coefficients rationnels qui s'annule en $\alpha := i+\sqrt{2}$. Pour cela, on se place dans $L = \mathbf{Q}(i,\sqrt{2})$, que l'on voit comme un $\mathbf{Q}$-espace vectoriel. On s'intéresse à l'application linéaire m_α de multiplication par α. Afin de calculer son polynôme caractéristique, on a besoin d'écrire la matrice de cette application linéaire dans une certaine base, et donc de trouver une base de $\mathbf{Q}(i,\sqrt{2})$ en tant que $\mathbf{Q}$-espace vectoriel. On sait que $(1,\sqrt{2})$ forme une base de $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$, et donc il nous reste à déterminer une base de $\mathbf{Q}(i,\sqrt{2})/\mathbf{Q}(\sqrt{2})$ pour conclure à l'aide du théorème de la base téléscopique. Or cette dernière extension est

de degré au plus 2 car i admet X^2+1 comme polynôme annulateur à coefficients dans $\mathbf{Q}(\sqrt{2})$. Comme i n'appartient pas à $\mathbf{Q}(\sqrt{2})$ (qui est contenu dans $\mathbf{R}$), on en déduit que $(1,i)$ est une base de $\mathbf{Q}(i,\sqrt{2})/\mathbf{Q}(\sqrt{2})$. D'après le théorème de la base téléscopique, une base de L sur $\mathbf{Q}$ est donc donnée par

$$\mathcal{B} = (1, \sqrt{2}, i, i\sqrt{2})$$

On calcule facilement

$$\mathrm{Mat}_{\mathcal{B}}(m_\alpha) = \begin{pmatrix} 0 & 2 & -1 & 0 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

puis son polynôme caractéristique $X^4 - 2X^2 + 9$, qui nous fournit un polynôme annulateur de $i + \sqrt{2}$.

4. Calcul pratique de polynômes annulateurs à l'aide de résultants

La référence principale pour cette partie est *Anneaux, corps, résultants* de Félix Ulmer. J'ai également emprunté un exemple au mémoire d'agrégation d'Antonin Riffaut https://perso.eleves.ens-rennes.fr/~ariffaut/Agregation/memoire_agregation.pdf

Rappelons quelques faits sur les résultants qui sont utiles pour le calcul de polynômes annulateurs. Étant donnés deux polynômes

$$f = \sum_{i=1}^{n} a_i Y^i \quad \text{et} \quad g := \sum_{i=1}^{m} b_i Y^i$$

à coefficients dans un anneau commutatif A, de degrés respectifs n et m, la matrice de Sylvester de f et g est une matrice dans $\mathrm{M}_{m+n}(A)$ (ses coefficients sont des a_i, des b_i, ou des zéros). Son déterminant est ce qu'on appelle le résultant de f et de g, noté $\mathrm{Res}_Y(f,g)$ (c'est donc un élément de A en tant que déterminant d'une matrice à coefficients dans A). On précise la variable Y car en pratique il faut imaginer que A sera de la forme $k[X_1,\dots,X_N]$. Le résultat essentiel pour nous sera le fait suivant, qui dit que $\mathrm{Res}_Y(f,g)$ (qui est, on le rappelle, un élément de A) appartient à l'idéal engendré par f et g dans $A[Y]$:

Lemme 4.1. *Avec les notations précédentes, il existe $u, v \in A[Y]$ tels que $\deg(u) < m$ et $\deg(v) < n$ et tels que*

$$\mathrm{Res}_Y(f,g) = uf + vg.$$

Ce lemme se démontre en faisant des opérations sur les lignes (ou les colonnes) de la matrice de Sylvester puis en développant le déterminant par rapport à la dernière ligne (ou la dernière colonne). Il faut souligner que le membre de gauche est une « constante » (c'est-à-dire un élément de A) alors que le membre de droite est formé de polynômes (c'est-à-dire d'éléments de $A[Y]$). On peut penser à l'égalité de ce lemme comme à une sorte de relation de Bézout entre f et g, sauf qu'elle est vraie dans le cadre général des anneaux commutatifs. Si A est supposé factoriel, alors en effet il y a un lien plus fort entre résultant et pgcd (le résultant est nul si et seulement si les polynômes ont un facteur commun), mais nous n'aurons pas besoin de ce fait pour le problème qui nous intéresse ici.

Soit L/K une extension de corps, et $\alpha, \beta \in L$, algébriques sur K. On note $f(Y)$ et $g(Y)$ leurs polynômes minimaux sur K. Ce sont des éléments de $K[Y]$. On introduit une seconde variable X, et on voit $f(X-Y)$ et $g(Y)$ comme deux éléments de $A[Y]$ avec $A = K[X]$. Alors

$$h := \mathrm{Res}_Y(f(X-Y), g(Y))$$

est un élément de $A = K[X]$ par définition du résultant, et nous allons expliquer pourquoi c'est un polynôme annulateur de $\alpha+\beta$. D'après le Lemme 4.1, il existe deux polynômes $u, v \in A[Y] = K[X,Y]$ tels que

$$h(X) = u(X,Y)f(X-Y) + v(X,Y)g(Y).$$

En évaluant en $\alpha+\beta$ la variable X on obtient

$$h(\alpha+\beta) = u(\alpha+\beta, Y)f(\alpha+\beta-Y) + v(\alpha+\beta, Y)g(Y)$$

Le membre de gauche est un élément de L, c'est l'évaluation en $\alpha+\beta$ du polynôme $h \in K[X]$. Par contre, le membre de droite est un élément de $L[Y]$, que l'on peut encore évaluer. Or si on évalue Y en β, on voit que $f(\alpha+\beta-\beta) = f(\alpha) = 0$ et $g(\beta) = 0$ par définition de f et g comme polynômes minimaux (annulateurs suffirait) de α et β. Donc $h(\alpha+\beta) = 0$, et c'est ce qu'on voulait : on a bien trouvé un polynôme annulateur de $\alpha+\beta$ à coefficients dans K.

Remarque 4.2. Attention, il pourrait arriver que h soit le polynôme nul... C'est notamment le cas lorsque f et g ne sont pas premiers entre eux, mais cette situation ne devrait pas se présenter sur des exemples simples.

Exemple 4.3. Pour déterminer un polynôme annulateur sur $\mathbf{Q}$ pour le nombre algébrique $\sqrt{2}+\sqrt[3]{3}$, on considère $f(Y) := Y^2 - 2$ (le polynôme minimal de $\sqrt{2}$ sur $\mathbf{Q}$) et $g(Y) := Y^3 - 3$ (celui de $\sqrt[3]{3}$). Alors $f(X-Y) = (X-Y)^2 - 2 = Y^2 - 2XY + X^2 - 2$. Donc (bon c'est là qu'on doit se souvenir de la définition de la matrice de Sylvester et qu'on ne peut pas se contenter de savoir qu'elle dépend des coefficients des polynômes)

$$h(X) = \mathrm{Res}_Y(f(X-Y), g(Y)) = \begin{vmatrix} X^2-2 & 0 & 0 & -3 & 0 \\ -2X & X^2-2 & 0 & 0 & -3 \\ 1 & -2X & X^2-2 & 0 & 0 \\ 0 & 1 & -2X & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{vmatrix}$$

Après calculs (cela se fait à la main, mais j'avoue avoir utilisé sage...) on obtient

$$h(X) = X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1$$

comme polynôme annulateur de $\sqrt{2} + \sqrt[3]{3}$.

Remarque 4.4. Si on voulait un polynôme annulateur de $\alpha\beta$ plutôt que de $\alpha+\beta$, on aurait envie de remplacer le $f(X-Y)$ de la définition de h par $f(X/Y)$. Le problème est que ce serait une fraction rationnelle, et non un polynôme. On compense cela en multipliant par Y^n. Un polynôme annulateur de $\alpha\beta$ est alors

$$\mathrm{Res}_Y(Y^n f(X/Y), g(Y)).$$

La preuve est la même que dans le cas additif.

5. Pour aller plus loin

Dans la section précédente, on a montré que le polynôme

$$h(X) = \mathrm{Res}_Y(f(X-Y), g(Y))$$

était un polynôme annulateur de $\alpha + \beta$. En fait, on peut même montrer que ses racines sont exactement les $\alpha_i + \beta_j$, où les α_i parcourent les racines de f et les β_j parcourent les racines de g.

Le résultat principal qui va nous servir à comprendre cela est le fait que le résultant, qui n'est défini qu'en termes des coefficients de f et g, « joue » en fait avec leurs racines dans un corps qui les contient.

Théorème 5.1. *Soit K un corps et L une extension de K dans laquelle f et g sont scindés :*

$$f = a_n \prod_{i=1}^{n} (Y - \alpha_i) \quad \text{et} \quad g = b_m \prod_{j=1}^{m} (Y - \beta_j) \quad \text{dans } L[Y].$$

Alors

$$\mathrm{Res}_Y(f,g) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m} (\alpha_i - \beta_j) = a_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_m^n \prod_{j=1}^{m} f(\beta_j).$$

On trouve ce résultat dans le livre de théorie de Galois de Gozard ou dans le livre *Anneaux, corps, résultants* de Félix Ulmer.

Puisque l'on va s'intéresser à des polynômes annulateurs, il ne faudra pas trop se préoccuper des coefficients dominants et des signes qui rendent les formules ci-dessus quelque peu effrayantes. Il ne faut pas trop non plus s'inquiéter du fait que le résultat est valable seulement sur un corps, alors qu'on utilise plutôt des résultants de polynômes à coefficients dans un anneau A de la forme $k[X_1, \ldots, X_N]$. En pratique, comme un tel anneau est intègre, on peut se placer dans son corps des fractions K, utiliser le théorème ci-dessus pour comprendre ce qu'il se passe quand on fait notre calcul de résultants en termes de racines de polynômes dans $\overline{K}$, puis se rappeler que les calculs ont en fait eu lieu dans A. *En tout cas tout ce qu'il faut retenir c'est que calculer le résultant de deux polynômes, c'est faire le produit des évaluations de l'un en en les racines de l'autre.*

Reprenons les notations précédentes : L/K une extension, $\alpha, \beta \in L$ algébriques sur K, de polynômes minimaux respectifs f et g. Alors on avait noté

$$h := \mathrm{Res}_Y(f(X-Y), g(Y)).$$

C'est un élément de $K[X]$ qui s'annule en $\alpha+\beta$, mais nous allons montrer un résultat plus précis.

Soit M un corps contenant les racines de f et de g. Dans $M[X]$, on peut écrire :

$$f(Y)=\prod_{i=1}^{n}(Y-\alpha_i) \quad \text{et} \quad g(Y)=\prod_{j=1}^{m}(Y-\beta_j).$$

Comme α et β sont racines respectives de f et g, on peut supposer que $\alpha=\alpha_1$ et que $\beta=\beta_1$. Notons que comme $f(X-Y)=\prod_{i=1}^{n}((X-\alpha_i)-Y)$, ce polynôme en Y est scindé sur le corps $M(X)$ et ses racines sont les $X-\alpha_i$. Ainsi, en appliquant le théorème ci-dessus on obtient que h est (au signe près) le produit des évaluations de $g(Y)$ en les racines de $f(X-Y)$, donc

$$h(X)=\pm\prod_{j=1}^{m}(X-(\alpha_i+\beta_j))$$

On a donc montré que les racines de h étaient en fait tous les éléments de la forme $\alpha_i+\beta_j$, où les α_i sont ce qu'on appelle les conjugués de α sur K (c'est-à-dire les racines de son polynôme minimal) et les β_j sont les conjugués de β sur K.

Exemple 5.2. Ce dernier résultat donne également une méthode pour construire des polynômes annulateurs lorsqu'on sait déterminer tous les conjugués des éléments algébriques considérés. Dans l'exemple de $\sqrt{2}+\sqrt{3}$, on sait que les conjugués de $\sqrt{2}$ sont $\sqrt{2}$ et $-\sqrt{2}$, et que les conjugués de $\sqrt{3}$ sont $\sqrt{3}$ et $-\sqrt{3}$, donc le polynôme

$$(X-(\sqrt{2}+\sqrt{3}))(X-(\sqrt{2}-\sqrt{3}))(X-(-\sqrt{2}+\sqrt{3}))(X-(-\sqrt{2}-\sqrt{3}))$$

sera, comme par magie, un polynôme à coefficients rationnels. Cela reste très proche d'une des grandes idées de la théorie de Galois, qui dit que les éléments du corps de base sont les éléments invariants par le groupe d'automorphismes. Ici, on ajoute au polynôme de degré 1

$$(X-(\sqrt{2}+\sqrt{3}))$$

tous les facteurs obtenus en faisant agir sur $\sqrt{2}$ (resp. $\sqrt{3}$) les automorphismes de $\mathbf{Q}(\sqrt{2})$ (resp. $\mathbf{Q}(\sqrt{3})$).

6. Calcul de polynômes annulateurs à l'aide du produit tensoriel d'applications linéaires

On présente cette méthode sous forme d'un exercice, inspiré du DM d'algèbre linéaire de Jérémy Leborgne.

Remarque 6.1. Dans l'exercice, on fait référence à l'utilisation du produit tensoriel pour munir proprement un K-espace vectoriel d'une structure de L-espace vectoriel, lorsque L est une extension de K. Cette prudence est nécessaire car lorsqu'on dit que $\alpha\in L$ est valeur propre d'un endomorphisme d'un K-espace vectoriel E, l'égalité

$$u(x)=\alpha x$$

n'a pas de sens tant que l'on a pas expliqué comment L agissait sur E. Bien sûr, même si cela peut-être jugé moins élégant, il est tout à fait correct de fixer une base $\mathcal{B}$ de E, et de voir la matrice $\mathrm{Mat}_{\mathcal{B}}(u)\in \mathrm{M}_n(K)$ comme un élément de $\mathrm{M}_n(L)$, pour laquelle cela a un sens de considérer des valeurs propres dans L et des vecteurs propres dans L^n.

Exercice.

1. Soit L/K une extension de corps et $\alpha\in L$. Montrer que α est algébrique sur K si et seulement si il existe un K-espace vectoriel E de dimension finie et un endomorphisme $u\in\mathcal{L}(E)$ tel que α soit racine de χ_u (i.e. tel que α soit une valeur propre de l'endomorphisme u_L obtenu à partir de u par extension des scalaires).
2. Soit E et E' deux K-espaces vectoriels de dimension finie, et $u\in\mathcal{L}(E)$, $v\in\mathcal{L}(E')$. Soit L/K une extension dans laquelle χ_u et χ_v sont scindés. On note u_L et v_L les endomorphismes des L-espaces vectoriels $E_L:=E\otimes_K L$ et $E'_L:=E'\otimes_K L$ obtenus par extension des scalaires. Montrer que si α est une valeur propre de u_L et β une valeur propre de v_L, alors $\alpha+\beta$ est valeur propre de $u_L\otimes \mathrm{Id}_{E'_L}+\mathrm{Id}_{E_L}\otimes v_L$ et que $\alpha\beta$ est valeur propre de $u_L\otimes v_L$.
3. En déduire que $\{x\in L \mid x \text{ est algébrique sur } K\}$ est un sous-corps de L.
4. Connaissant un polynôme annulateur de α et un polynôme annulateur de β, comment déterminer un polynôme annulateur de $\alpha+\beta$? de $\alpha\beta$?