par Gérard Cohen-Zardi

Fonctions rationnelles des racines d'un polynôme

Deux premiers résultats sur les polynômes sont énoncés par Évariste Galois, l'un sur une propriété de divisibilité, et l'autre sur la construction d'une fonction rationnelle des racines. Les fonctions symétriques élémentaires sont introduites.

Galois commence par fourbir ses armes en lançant une première définition qu'il nous faut décrypter : *« Un polynôme sera dit irréductible quand il n'admet pas de diviseur rationnel. »* Il s'empresse de préciser le sens du mot « rationnel », aussi bien pour un polynôme que pour un nombre (voir en pages précédentes).

Un nombre est *rationnel* (au sens de Galois) s'il est dans le champ de rationalité actuel. Lorsqu'il considère l'équation d'inconnue x suivante,

$x_m + \alpha_{m-1}x_{m-1} + \alpha_{m-2}x_{m-2} + \ldots + \alpha_1 x + \alpha_0 = 0$,

il la suppose sans racines égales et la nomme *« la proposée »*.

Le polynôme est unitaire. Le champ de rationalité initial est $K = \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{m-1})$, c'est donc $\mathbb{Q}$ quand les coefficients $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{m-1}$ sont rationnels. Le champ de rationalité s'agrandit à mesure que l'on adjoint, comme dit Galois, une nouvelle quantité.

Nombre rationnel et polynôme rationnel

Un polynôme est considéré par Galois comme étant *rationnel* lorsque ses coefficients le sont (« *en notre sens* », dit Galois). Le sens du mot « rationnel », pour un nombre comme pour un polynôme, est relatif à un champ de rationalité donné (à mesure que l'on agrandit le champ de rationalité, des nombres et des polynômes, qui n'étaient pas rationnels, le deviennent). Galois fait même observer qu'*« un polynôme irréductible peut devenir réductible »*, car là encore la notion de réductibilité d'un polynôme (au sens de Galois) fait référence à un champ de rationalité.

Par exemple, le polynôme $X^2 - X - 1$ est rationnel et irréductible pour le champ de départ, qui est $K = \mathbb{Q}$. Mais quand on adjoint la quantité $\sqrt{5}$ le champ devient $K_1 = \mathbb{Q}(\sqrt{5})$ et notre polynôme se décompose

$$\left(X - \frac{1+\sqrt{5}}{2}\right)\left(X - \frac{1-\sqrt{5}}{2}\right),$$

Ces deux facteurs sont maintenant rationnels (au sens de Galois) sur le nouveau champ de rationalité K_1.

Galois écrit ensuite : « *Quand nous grouperons des substitutions, nous les ferons toutes provenir d'une même permutation. Mais on devra avoir les mêmes substitutions quelle que soit la permutation d'où l'on part. Ainsi, si dans un tel groupe nous avons les substitutions s et t on est sûr d'avoir la substitution st.* »

En effet, si $t = p_1 \to p_2$ et $s = p_1 \to p_3$, on peut faire partir s de p_2 et donc trouver une permutation p_4 dans la liste des permutations que l'on a groupées, de sorte que $s = p_2 \to p_4$. Ainsi $st = p_1 \to p_4$ est bien dans le groupe. Remarquons que si s est dans le groupe alors s^{-1} y est aussi, car $s^{-1} = p_3 \to p_1$ avec nos notations.

Nous sommes maintenant armés pour comprendre les deux lemmes énoncés par Galois. Voici le premier : **un polynôme rationnel irréductible ne peut avoir une racine commune avec un autre polynô-**

Racines communes et divisibilité

Expliquons le « *etc* » dans le premier lemme de Galois. Soient A et B les deux polynômes unitaires, B étant irréductible sur le champ de rationalité K, et soit Δ leur PGCD (qui est unitaire) dans C[X]. Si A et B sont dans K[X], ils sont aussi dans C[X] B est non nul. Dire que B divise A dans C[X] c'est dire qu'il existe Q dans C[X] tel que A = B Q. Mais Q s'obtient par division euclidienne de A par B, et cette opération ne fait pas « sortir » les coefficients calculés de K. Ainsi B divise aussi A dans K[X] et donne le même quotient. Donc Q appartient lui aussi à K[X].
De même, l'algorithme d'Euclide fournit explicitement les coefficients de D, qui sont tous dans K. Ainsi D est aussi le PGCD de A et B dans K[X].
Maintenant, B est irréductible et unitaire. Notons r une racine commune à A et B. Alors D est divisible par $X - r$ dans C[X] et est donc non constant. Comme D est dans K[X] et qu'il divise B, qui y est irréductible, il lui est égal (tous deux sont unitaires). B = D divise donc A dans K[X].

me rationnel sans le diviser. *« Parce que,* dit-il, *leur PGCD est encore rationnel etc. »* (voir en encadré).
Voyons sans plus tarder le second lemme énoncé par Galois : **étant données les racines (distinctes) $x_1, x_2, x_3, \ldots, x_m$ de la proposée, on peut former une fonction rationnelle $\{(x_1, x_2, x_3, \ldots, x_m)$ de ces racines qui ne prend pas deux fois la même valeur quand on permute de toutes les façons possibles les *m* racines.**
On peut par exemple, nous dit Galois, prendre $\{(x_1, x_2, x_3, \ldots, x_m) = Ax_1 + Bx_2 + Cx_3 + \ldots$, A, B, $C\ldots$ étant des entiers convenablement choisis. Ce fait est acquis pour lui. En effet, considérons, pour chaque permutation $p = (x_1, x_2, x_3, \ldots, x_m)$, le polynôme $S_p = x_1X^{m-1} + x_2X^{m-2} + \ldots + x_{m-1}X + x_m$. De même, considérons, pour toute paire $\{p, p'\}$ de permutations des racines, le polynôme $D_{p,\,p'} = S_p - S_{p'}$. Ces polynômes $D_{p,\,p'}$, sont tous non nuls et en nombre fini. Leurs racines constituent un ensemble fini. L'ensemble des entiers non nuls étant infini, il existe un entier x qui n'est racine d'aucun de ces polynômes. Il suffit alors de prendre $A = x^{m-1}$, $B = x^{m-2}$, $C = x^{m-3}\ldots$
Ces deux résultats étant établis, Galois peut maintenant s'intéresser aux fonctions rationnelles des racines. Considérons le polynôme suivant :

$$H = (X - \{(x_1, x_2, x_3\ldots)(X - \{(x_1, x_3, x_2\ldots) \ldots (X - \{(x_1\ldots))$$

où l'on prend les valeurs de { pour x_1 restant en première place et en permutant les autres racines des $(m-1)!$ façons possibles. Ce polynôme H va alors s'écrire $H = F(X, a)$ avec $a = x_1$ et $F(X, a) = X^d + c_{d-1}(a)X_{d-1} + \ldots + c_1(a)X + c_0(a)$, où les c_k sont des polynômes rationnels (voir l'encadré en page précédente).
En fait, Galois désigne les racines par a, b, $c\ldots$ et pose V = $\{(a, b, c\ldots)$, valeur de { lorsque les racines sont prises dans l'ordre alphabétique. Le premier facteur de H est X – V, donc V est racine de H, ce qui fait que F(V, a) = 0. De là, il affirme : *« Je dis qu'on peut tirer la valeur de a. Il suffit pour cela de chercher la solution commune à cette équation et à la proposée. »*
L'équation dont il parle est F(V, z) = 0 d'inconnue z. Il affirme qu'aucune autre racine b, $c\ldots$ de la proposée ne vérifie cette équation. Car si l'on avait, par exemple, F(V, b) = 0, alors l'un des $\{(a, \ldots)$ serait égal à l'un des $\{(b, \ldots)$, *« ce qui est contre l'hypothèse »*, nous dit Galois. Explicitons cela.
Si, dans H, on fait $x_1 = b$ (au lieu de $x_1 = a$), on trouve alors :

$$\left(X - \varphi\left(b, a, c\ldots\right)\right)\left(X - \varphi\left(b, c, a\ldots\right)\right)\ldots\left(X - \varphi\left(b\ldots\right)\right) = F(X, b).$$

C'est le même F car on a juste échangé a et b. Donc, si F(V, b) = 0, V annulerait l'un des facteurs

et serait par conséquent égal à l'un des {(*b*, …) alors que V = {(*a*, *b*, *c*…). Donc seule la racine *a* de la proposée vérifie F(V, *z*) = 0.

Pourquoi alors peut-on exprimer a rationnellement en V ? Galois ne s'étend pas sur cette question, mais nous allons démontrer ce fait. Il s'agit donc de l'existence de deux polynômes *g* et *h* dans K[X] tels que $a = g(V)/h(V)$. Cela est équivalent (c'est sans doute clair dans la tête de Galois, même s'il n'en parle jamais) au fait qu'il existe un polynôme rationnel *f* (donc de K[X]) tel que $a = f(V)$. V est en effet racine d'un polynôme rationnel (que Galois introduit plus loin). Ce polynôme, que nous notons M, est le produit des (X – {(*p*)) pour *p* parcourant l'ensemble de toutes les permutations des racines. Le polynôme M est dans K[X] (car ses coefficients s'expriment symétriquement en fonctions rationnelles de toutes les racines de la proposée) et son degré est égal à *m*!.

Galois considère ensuite le facteur irréductible de M dans K[X] dont V est racine ; notons-le M_1.

Si l'on considère $g(V)/h(V)$, $h(V)$ étant non nul, *h* n'est pas multiple de M_1. Il est donc premier avec M_1. Le théorème de Bézout (que Galois connaît) stipule qu'il existe dans K[X] deux polynômes *u* et *v* tels que $u\,h + v\,M_1 = 1$. Il en résulte que $u(V)\,h(V) = 1$, car $M_1(V) = 0$. Ainsi, en posant $f = g\,u$, on a bien $f(V) = g(V)\,u(V) = g(V)/h(V)$

Galois affirme donc en fait que *a* est dans K(V), l'ensemble des fractions rationnelles. Or on sait que P(X) et F(V, X) sont dans K(V)[X], l'anneau des polynômes en l'indéterminée X dont les coefficients sont des éléments de K(V). Comme *a* est leur unique racine commune dans $\mathbb{C}$ et est racine simple de P, leur PGCD dans $\mathbb{C}[X]$ est $X - a$. Or leur PGCD est le même dans K(V)[X]. Il s'ensuit que *a* appartient à K(V). On peut donc exprimer *a* rationnellement en V.

Les fonctions symétriques des racines

Considérons un polynôme *P* de K[X] ayant *m* racines simples $x_1, x_2, x_3, \ldots, x_m$. Nous pouvons écrire $P = X^m + a_{m-1}X^{m-1} + \ldots + a_1X + a_0 = (X-x_1)(X-x_2)(X-x_3)\ldots(X-x_m)$. Notons $v_1, v_2 \ldots v_m$ les *fonctions symétriques élémentaires des racines* $x_1, x_2, \ldots, x_m$. Par définition, on a, pour tout indice *k* compris de 1 à *m*,

$$\sigma_k = \sum_{1 \le i_1 < i_2 < \ldots < i_k \le m} x_{i_1} x_{i_2} x_{i_3} \ldots x_{i_k}.$$

La fonction symétrique élémentaire v_k est donc la sommedes produits des racines prises *k* par *k* (la somme comporte $C_m^k = \frac{m!}{k!(m-k)!}$ termes).

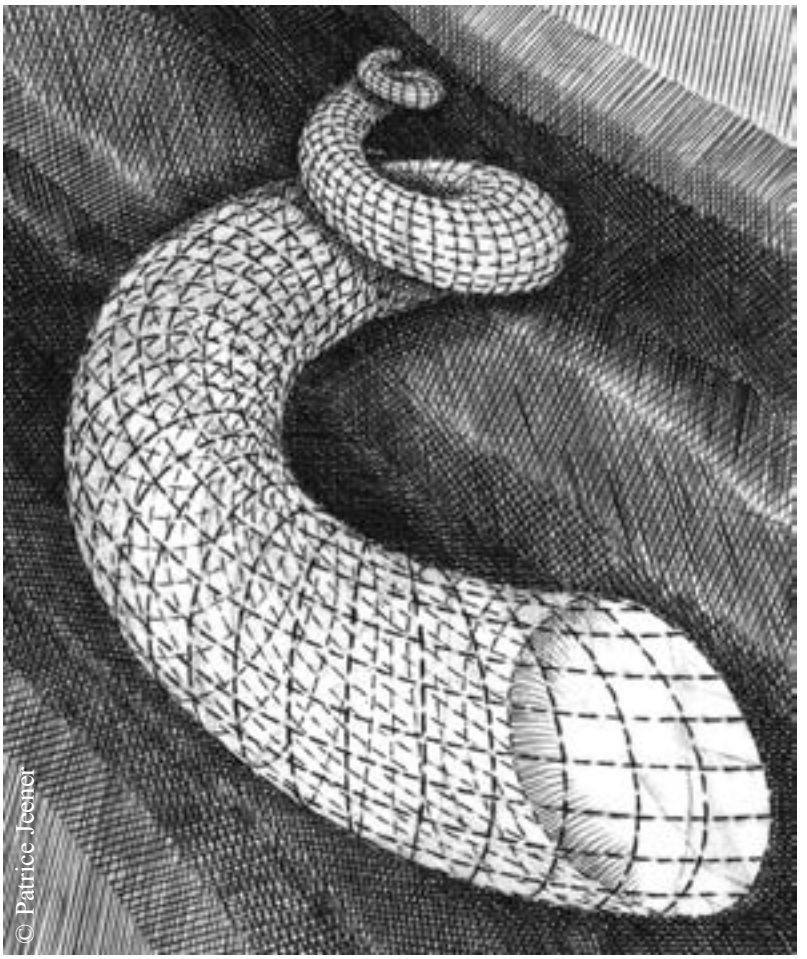
Pour $m = 3$, nous avons $v_1 = x_1 + x_2 + x_3$, $v_2 = x_1x_2 + x_1x_3 + x_2x_3$ et $v_3 = x_1x_2x_3$. On voit facilement que $v_k = (-1)^{m-k}a_{m-k}$ (relations entre coefficients et racines pour un polynôme unitaire). Les fonctions symétriques élémentaires des racines appartiennent donc au champ de rationalité $\mathbb{Q}(a_0, a_1, \ldots, a_{m-1})$.

Notons enfin $v'_1, v'_2, \ldots, v'_{m-1}$ les fonctions symétriques élémentaires des racines $x_2, x_3, \ldots, x_m$. On a clairement $v_1 = x_1 + x_2 + \ldots + x_m = x_1 + v'_1$, $v_2 = x_1\,v'_1 + v'_2$, etc., donc $v'_1 = v_1 - x_1$, $v'_2 = v_2 - x_1(v_1 - x_1)\ldots$ Les coefficients de *H* s'expriment au moyen de x_1 et symétriquement par rapport à $x_2, x_3, \ldots, x_m$. Donc ils s'expriment rationnellement à l'aide de x_1 et de $v'_1, v'_2, , v'_{m-1}$. Comme ces dernières s'expriment rationnellement à l'aide de x_1 et des $v_1, v_2, \ldots, v_m$ et que $v_1, v_2, \ldots, v_m$ sont dans le champ de rationalité, on a le résultat.

Il en est évidemment de même pour toutes les racines. Ceci fait que K(V) = K(x_1, x_2, x_3… x_m), car on savait déjà que K(V) est inclus dans K(x_1, x_2, x_3… x_m).

Galois a de plus montré que si W = {(x_1, x_2, x_3…) est l'une quelconque des racines de M_1, alors la racine x_1 s'exprime sous la forme f_1(W), f_1 étant un polynôme de K[X] qui ne dépend pas de la permutation p pour laquelle W = {(p). Évidemment il peut faire la même chose en fixant la racine x_2 à la deuxième place et en permutant les autres racines de toutes les manières possibles. Le même raisonnement donne alors $x_2 = f_2$(W) où f_2 est un polynôme de K[X] qui ne dépend toujours pas de p… et de même pour les autres racines.
Il obtient finalement m polynômes $f_1, f_2, f_3 \ldots f_m$ de K[X] qui vérifient, pour l'une quelconque des racines W de M_1 : W = {(p) si, et seulement si, p est la permutation f_1(W) f_2(W) f_3(W) … f_m(W). Galois note (W) la permutation p qui donne W par {, de sorte que cette équivalence s'écrit :
W = {(p) si, et seulement si, p = (W).
On en déduit en outre que toute fonction rationnelle des racines s'exprime sous la forme i(W), où i est dans K[X].

G.C.-Z.



Corne.
Gravure de Patrice Jeener, dans la série « Coquillages ».