

Objectif : obtenir un polynôme générique galoisien de groupe de Galois C_4

Cherchons un élément d'ordre 4 dans $\text{PGL}_2(\mathbb{Q})$. Puisque $(1-i)^2 = -2i$ et $(1-i)^4 = -4$, la multiplication par $1-i$ dans le \mathbb{Q} -plan $\mathbb{Q}(i)$ a pour puissance quatrième une homothétie et donc définit un élément d'ordre 4 de $\text{PGL}_2(\mathbb{Q})$. L'élément $\sigma \in \text{PGL}_2(\mathbb{Q})$ associé à la multiplication par $1-i$ est :

$$\sigma = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \quad \sigma(x) = -\frac{x+1}{x-1}$$

Vérifions que c'est bien un élément d'ordre 4 de $\text{PGL}_2(\mathbb{Q})$:

$$\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ -2 & 0 \end{bmatrix} \quad \sigma^2(x) = -\frac{1}{x}$$

Voici les 4 itérés $\sigma^i(x)$ pour $i = 0, 1, 2, 3$:

$$x_1 = x, \quad x_2 = -\frac{x+1}{x-1}, \quad x_3 = -\frac{1}{x}, \quad x_4 = \frac{x-1}{x+1}$$

Notons $\mathbf{K} = \mathbf{L}^G$ où $\mathbf{L} = \mathbb{Q}(x)$ et $G = \langle \sigma \rangle$. Le polynôme minimal de x sur \mathbf{K} est :

$$F(X) = (X - x_1)(X - x_2)(X - x_3)(X - x_4) = X^4 - tX^3 - 6X^2 + tX + 1$$

où t est fraction rationnelle $x + \sigma(x) + \sigma^2(x) + \sigma^3(x)$:

$$t = x - \frac{x+1}{x-1} - \frac{1}{x} + \frac{x-1}{x+1} = \frac{x^2(x^2-1) - x(x+1)^2 - (x^2-1) + x(x-1)^2}{x(x^2-1)} = \frac{x^4 - 6x^2 + 1}{x(x^2-1)}$$

Cette fraction rationnelle mérite d'être encadrée :

$$t = \frac{x^4 - 6x^2 + 1}{x(x^2 - 1)}$$

Vu la construction de t , elle est bien invariante par $G = \langle \sigma \rangle$. Et d'ailleurs, dans l'encadré, on y voit l'égalité $x^4 - 6x^2 + 1 - t(x(x^2-1)) = 0$ i.e. le polynôme F . Redondance chère à C.Q.?

Bref, le polynôme $F_t(X) = X^4 - tX^3 - 6X^2 + tX + 1$ est irréductible sur le corps \mathbf{K} et son groupe de Galois est le groupe cyclique C_4 .

Et la fraction rationnelle t est de hauteur 4 et le quart de la moitié facile du théorème de Luröth nous dit que $\mathbf{K} = \mathbb{Q}(t)$: toute fraction rationnelle en x , σ -invariante, est une fraction rationnelle en t .

L'unique extension quadratique de $\mathbf{K} = \mathbb{Q}(t)$ contenue dans $\mathbf{L} = \mathbb{Q}(x)$ s'obtient comme points fixes de σ^2 . C'est donc $\mathbf{K}(x_1 + x_3) = \mathbf{K}(x - 1/x)$; pour éviter les jaloux, on peut faire aussi avec $x_2 + x_4$, qui est son $\mathbb{Q}(t)$ -conjugué, et qui engendre le même corps. Au cas où l'on aurait des doutes, on a $(x_1 + x_3)(x_2 + x_4) = -4$ et l'équation du second degré sur $\mathbb{Q}(t)$ vérifiée par $s \in \{x_1 + x_3, x_2 + x_4\}$ est

$$s^2 - ts - 4 = 0 \quad \text{de discriminant } t^2 + 16$$

Bref, l'unique extension quadratique peut être vue comme $\mathbf{K}(\sqrt{t^2 + 16}) = \mathbb{Q}(t, \sqrt{t^2 + 16})$

Résumé :

$$\begin{array}{c} \mathbf{L} = \mathbb{Q}(x) \\ \left| \begin{array}{c} 2 \\ \mathbf{Q}(t, \sqrt{t^2 + 16}) = \mathbf{K}(x_1 + x_3) = \mathbf{K}(x_2 + x_4) = \mathbf{L}^{\sigma^2} \end{array} \right. \\ \left| \begin{array}{c} 2 \\ \mathbf{K} = \mathbb{Q}(t) = \mathbf{L}^\sigma \end{array} \right. \end{array}$$

Où l'on fait intervenir la D_4 -résolvante cubique

La D_4 -résolvante cubique d'un polynôme (unitaire) de degré 4 est un certain polynôme (unitaire) de degré 3 qui donne beaucoup de renseignements sur la nature du corps engendré par les 4 racines du polynôme de degré 4 de départ. Elle est liée aux 2-2-partitions de $\{1, 2, 3, 4\}$ qui sont au nombre de 3 :

$$\{\{1, 2\}, \{3, 4\}\}, \quad \{\{1, 3\}, \{2, 4\}\}, \quad \{\{1, 4\}, \{2, 3\}\}$$

Dans le groupe symétrique S_4 , le fixateur d'une quelconque 2-2-partition est un groupe diédral D_4 (d'ordre 8). Bref, il est classique d'introduire le polynôme

$$\left(X - (X_1X_2 + X_3X_4)\right) \left(X - (X_1X_3 + X_2X_4)\right) \left(X - (X_1X_4 + X_2X_3)\right)$$

dont les coefficients sont symétriques en (X_1, X_2, X_3, X_4) alors que les racines que l'on voit ne le sont. En passant, avec des notations que l'on peut deviner, on a :

$$\prod_{i < j} (X_i - X_j) = \pm \prod (Y_{ij, k\ell} - Y_{i'j', k'\ell'})$$

En conséquence, le discriminant du polynôme (unitaire) de degré 4 de départ, i.e. $\prod_{i < j} (x_i - x_j)^2$, est égal au discriminant de sa résolvante cubique diédrale.

En ce qui concerne $F_t(X) = X^4 - tX^3 - 6X^2 + tX + 1 = \prod_{i=1}^4 (X - x_i)$, on considère donc

$$R_t(X) = \left(X - (x_1x_2 + x_3x_4)\right) \left(X - (x_1x_3 + x_2x_4)\right) \left(X - (x_1x_4 + x_2x_3)\right)$$

Lorsque l'on croit à ce que l'on fait, on est capable d'obtenir l'expression en t suivante :

$$(\heartsuit) \quad R_t(X) = (X + 2) \times (X^2 + 4X - t^2 - 12)$$

Avec les choix faits, c'est $x_1x_3 + x_2x_4$ qui vaut -2 , pour la bonne (?) raison que $x_1x_3 = x_2x_4 = -1$. Pour le reste, cf la section "Croire à ce que l'on fait", plus loin.

Pour les connaisseurs de la D_4 -résolvante : le polynôme $R_t(X)$ possède une seule racine (à savoir -2) dans le corps de base $\mathbb{Q}(t)$, confirmant que le polynôme F_t est de groupe de Galois C_4 . La spécialisation devra être réalisée de sorte que le discriminant du trinôme ci-dessus $X^2 + 4X - t^2 - 12$ i.e. $4^2 + 4(t^2 + 12) = 4(t^2 + 16)$ ne soit point un carré.

La spécialisation en $t \in \mathbb{Z}$

A l'aide d'un système de Calcul Formel, on détermine

$$\text{disc}(F_t) \stackrel{\text{def}}{=} \prod_{i < j} (x_i - x_j)^2 = 4(t^2 + 16)^3 = \text{un carré} \times (t^2 + 16)$$

On va spécialiser en $t \in \mathbb{Z}$ en faisant en sorte que $t^2 + 16$ ne soit pas un carré. Cette dernière condition est toujours vérifiée sauf pour $t = 0, \pm 3$ (c'est le fameux $3^2 + 4^2 = 5^2$). A JUSTIFIER VRAIMENT : pour tout $t \in \mathbb{Z} \setminus \{0, \pm 3\}$, le polynôme $F_t(X)$ est irréductible de groupe de Galois C_4 .

Et d'ailleurs, cela fonctionne aussi sur \mathbb{F}_p ($p \neq 2$), à condition que $t^2 + 16$ ne soit pas un carré dans \mathbb{F}_p , fonctionne signifiant que sur \mathbb{F}_p , le polynôme $F_t(X) \in \mathbb{F}_p[X]$ est irréductible, de groupe de Galois C_4 .

Exercice : soit p un premier ≥ 3 ; montrer que l'ensemble des $t \in \mathbb{F}_p \setminus \{0\}$ tels que $F_t(X)$ soit irréductible dans $\mathbb{F}_p[X]$ est de cardinal :

$$\begin{cases} (p-1)/2 & \text{si } p \equiv 1 \pmod{4} \\ (p+1)/2 & \text{si } p \equiv 3 \pmod{4} \end{cases}$$

Croire à ce que l'on fait

On fixe un corps de base \mathbf{k} . Soit $y = u/v \in \mathbf{k}(x) \setminus \mathbf{k}$ une fraction rationnelle non constante de hauteur h ; étant donné $z \in \mathbf{k}(x)$, on veut tester si z appartient à $\mathbf{k}(y)$ et si oui exprimer z en fonction de y (comme une fraction rationnelle en y). Le quart de la moitié facile du théorème de Luröth nous informe que :

La $\mathbf{k}(y)$ -extension $\mathbf{k}(x)$ est isomorphe à la $\mathbf{k}(Y)$ -extension $\mathbf{k}(Y)[X]/\langle P \rangle$ où $P = u(X) - vg(X)$

avec bien sûr la correspondance :

$$x \leftrightarrow X \pmod{P}, \quad y \leftrightarrow Y$$

Encadrons cet isomorphisme d'extensions

$$(\star) \quad \boxed{\mathbf{k}(x)/\mathbf{k}(y) \quad \text{pareil que} \quad \frac{\mathbf{k}(Y)[X]}{\langle P \rangle} / \mathbf{k}(Y)}$$

Conséquence : étant donné $z \in \mathbf{k}(x)$, on peut l'écrire comme une combinaison linéaire, à coefficients dans $\mathbf{k}(y)$, de la base $1, x, x^2, \dots, x^{h-1}$ de $\mathbf{k}(x)/\mathbf{k}(y)$ où h est la hauteur de y . Alors z appartient à $\mathbf{k}(y)$ si et seulement si les coefficients de z sur x, \dots, x^{h-1} sont nuls ; dans ce cas, l'expression de z en fonction de y est donnée par le coefficient sur 1.

Pour vraiment assurer la chose, voilà ce qu'il faut réaliser : on prend $z = z_1(x)/z_2(x) \in \mathbf{k}(x)$ à gauche de (\star) où $z_i(x)$ est un polynôme en x . Pour le passer du côté droit de (\star) , il faut inverser $z_2(x)$, devenu $z_2(X)$. Sous-entendu, il faut l'inverser modulo P car on croit dur comme fer que P est irréductible dans $\mathbf{k}(Y)[X]$ puisqu'un jour on l'a montré. Coefficients de Bezout :

$$1 = Sz_2 + TP \quad \text{dans } \mathbf{k}(Y)[X] \quad \text{donc } S \text{ est l'inverse de } z_2(X) \text{ modulo } P$$

Bilan, z_1/z_2 est vu à droite comme $(z_1(X)S) \bmod P$ et le tour est joué.

----- Extrait de LurothViteFait.magma -----

```
// Quart de la moitié de la partie facile du théorème de Luröth
// La k(y)-extension k(x)/k(y) est isomorphe à la k(Y)-extension k(Y)[X]/<u(X) - v(X)Y>

LurothBasisComponents := fonction(y, z)
// y=u/v et z = z1/z2 deux fractions rationnelles dans k(x) avec y non constante
// Retourne l'expression de z sur la k(y)-base (1, x, , .., x^{h-1}) où h est la hauteur de y
// Petit micmac polynomial cher à magma
// kx = k(x)
kx := Parent(y) ;
// Récupérer le corps de base k
k := BaseRing(kx) ;
// kY = k(Y)
kY<Y> := FunctionField(k) ;
// kYX = k(Y)[X]
kYX<X> := PolynomialRing(kY) ;
// k[x] -> k(Y)[X]   x --> X
xToX := hom < IntegerRing(kx) -> kYX | X > ;
// Dans l'autre sens : k(Y)[X] -> k(x),   Y --> y, X --> x
Y2yX2x := hom < kYX -> kx | hom < BaseRing(kYX) -> kx | y >, x> where x is kx.1 ;

// P = u(X) - v(X)*Y
P := u - v*Y where u is xToX(Numerator(y)) where v is xToX(Denominator(y)) ;

z1 := xToX(Numerator(z)) ;   z2 := xToX(Denominator(z)) ;
// Coefficients de Bezout
pgcd, a, b := XGCD(z2, P) ;
assert pgcd eq 1   and   1 eq a*z2 + b*P ;
// 1 = a*z2 mod P => a est l'inverse de z2 modulo P
result := (a*z1) mod P ;
assert Y2yX2x(result) eq z ;
return result, Y2yX2x ;
end fonction ;
```

----- La calculette en action -----

```
> y := (x^2 + x - 1) / (x + 3) ;
> z := (y - 1) / (y^3 + y + 2) ;
> z ;
(x^4 + 6*x^3 + 5*x^2 - 24*x - 36)/(x^6 + 3*x^5 + x^4 + 4*x^3 + 32*x^2 + 60*x + 44)
> E := LurothBasisComponents(y, z) ;
> E ;
(Y - 1)/(Y^3 + Y + 2)
```

Ainsi l'auteur s'aide d'une calculette pour déterminer :

$$x_1x_2 + x_3x_4 = \frac{-x^4 - 2x^3 - 2x^2 + 2x - 1}{x^3 - x}, \quad x_1x_4 + x_2x_3 = \frac{x^4 - 2x^3 + 2x^2 + 2x + 1}{x^3 - x}$$

puis le produit :

$$(\text{produit}) \quad (x_1x_2 + x_3x_4)(x_1x_4 + x_2x_3) = \frac{-x^8 - 14x^4 - 1}{x^6 - 2x^4 + x^2}$$

Mais maintenant, la calculette doit être aidée par l’auteur en ce qui concerne le fait d’obtenir, puisque l’on croit que c’est dans $\mathbb{Q}(t)$, l’expression du produit en fonction de la fraction rationnelle t suivante :

$$t = \frac{x^4 - 6x^2 + 1}{x(x^2 - 1)}$$

Toujours avec sa calculette, l’auteur détermine les coefficients de Bezout évoqués quelques lignes auparavant. Et obtient :

$$\frac{-x^8 - 14x^4 - 1}{x^6 - 2x^4 + x^2} = -t^2 - 12$$

C’est cela qui apparaît dans (♥) page précédente.

Une introduction aux résolvants d’une action transitive

EN-COURS

Pour $\sigma \in S_n$ et $F = F(X_1, \dots, X_n) \in \mathbf{k}[X_1, \dots, X_n]$, je note ${}^\sigma F$ le polynôme $F(X_{\sigma(1)}, \dots, X_{\sigma(n)})$. Soit H un sous-groupe du groupe symétrique S_n . Un résolvant $\theta \in \mathbf{k}[X_1, \dots, X_n]$ pour ce sous-groupe H est un polynôme tel que :

$$H = \{\sigma \in S_n \mid {}^\sigma \theta = \theta\}$$

Soit par exemple, la représentation “habituelle” du groupe diédral D_4 dans S_4 , i.e.

$$D_4 = \langle (1234), (24) \rangle \subset S_4, \quad \begin{array}{c} 2 \swarrow \quad \nwarrow 1 \\ 3 \quad \quad 4 \end{array}$$

On peut prendre comme D_4 -résolvant $X_1X_3 + X_2X_4$ et l’action de S_4 sur l’ensemble des classes à gauche $(S_4/D_4)_g$ (de cardinal 3) peut-être perçue comme l’action de S_4 sur les 3 polynômes :

$$X_1X_3 + X_2X_4, \quad X_1X_2 + X_3X_4, \quad X_1X_4 + X_2X_3$$

Un exemple de résolvant pour le groupe cyclique $C_4 = \langle (1, 2, 3, 4) \rangle$:

$$X_1X_2^2 + X_2X_3^2 + X_3X_4^2 + X_4X_1^2$$

L’action de S_4 sur l’ensemble des classes à gauche $(S_4/C_4)_g$ (de cardinal 6) peut-être perçue comme l’action de S_4 sur 6 polynômes de type ${}^\tau (X_1X_2^2 + X_2X_3^2 + X_3X_4^2 + X_4X_1^2)$, τ décrivant un système de représentants de $(S_4/C_4)_g$.

Une table indiquant le type des orbites sur l’ensemble $(S_4/D_4)_g$ (de cardinal 3) des 5 (à conjugaison près) sous-groupes transitifs de S_4 , le type étant la suite des cardinaux des orbites rangée par ordre croissant par exemple. Ainsi 1+2 signifie 2 orbites, une de cardinal 1, l’autre de cardinal 2. Puis le type des orbites de l’action transitive de S_4 sur $(S_4/C_4)_g$, de cardinal 6.

	C_4	$V \simeq C_2 \times C_2$	D_4	$A_4(+)$	S_4
ordre	4	4	8	12	24
$(S_4/D_4)_g$ -type	1+2	1+1+1	1+2	3	3
$(S_4/C_4)_g$ -type	1+1+4	2+2+2	2+4	6	6

FIN-EN-COURS

Le polynôme $F_t(X^2)$ de groupe de Galois $C_2^3 \rtimes C_4$

Ici, on reste en terrain générique, en particulier x est une indéterminée sur \mathbb{Q} . Je dis que x n’est pas un carré dans l’anneau principal $\mathbb{Q}[x]$ donc pas non plus un carré dans son corps des fractions $\mathbb{Q}(x)$. En conséquence, le polynôme $F_t(X^2)$ est irréductible sur $\mathbb{Q}(t)$. On note \mathbf{L}' un corps de décomposition de $F_t(X^2)$ sur $\mathbb{Q}(t)$; comme le polynôme $F(tX^2)$ qui intervient est un polynôme en X^2 (de degré 8), ses racines vont deux par deux $\pm y_i$ et on peut utiliser une numérotation de sorte que $y_i^2 = x_i$. On a

$(y_1 y_2 y_3 y_4)^2 = x_1 x_2 x_3 x_4 = 1$ donc $y_1 y_2 y_3 y_4 = \pm 1$. Quitte à remplacer y_4 par $-y_4$, on peut supposer $y_1 y_2 y_3 y_4 = 1$. On dispose donc d'un schéma :

$$\begin{array}{c} \mathbf{L}' = \mathbb{Q}(y_1, y_2, y_3, y_4) \\ | \\ \mathbf{L} = \mathbb{Q}(x) \\ \text{galoisienne} \left| \langle \sigma \rangle \text{ d'ordre } 4 \right. \\ \mathbf{K} = \mathbb{Q}(t) \end{array}$$

Pour $\tau \in \text{Gal}(\mathbf{L}'/\mathbf{L})$, on a $\tau(y_i) = \pm y_i$ donc $\tau^2(y_i) = y_i$ puis $\tau^2 = \text{Id}_{\mathbf{L}'}$. Par conséquent, le groupe $\text{Gal}(\mathbf{L}'/\mathbf{L})$ est commutatif, d'exposant 2, donc un produit de groupes cycliques $C_2 \simeq \{\pm 1\}$. Le morphisme suivant de groupes :

$$\text{Gal}(\mathbf{L}'/\mathbf{L}) \ni \tau \mapsto \left(\frac{\tau(y_1)}{y_1}, \frac{\tau(y_2)}{y_2}, \frac{\tau(y_3)}{y_3}, \frac{\tau(y_4)}{y_4} \right) \in \{-1, 1\}^4$$

est injectif (facile). **TODO** Il faut montrer que son image est le sous-groupe formé des $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$ de produit 1, donc un groupe isomorphe à C_2^3 **END-TODO**. Ceci revient à montrer que pour i, j, k distincts, x_i n'est pas un carré dans $\mathbb{Q}(y_j, y_k)$.

Une fois ce **TODO** assuré, en utilisant le fait que \mathbf{L}/\mathbf{K} est galoisienne qui impacte sur le fait que $\text{Gal}(\mathbf{L}'/\mathbf{L})$ est un sous-groupe distingué de $\text{Gal}(\mathbf{L}'/\mathbf{K})$, on obtient que le groupe de Galois convoité est un certain produit semi-direct :

$$\text{Gal}(\mathbf{L}'/\mathbf{K}) = \text{Gal}(\mathbf{L}'/\mathbf{L}) \rtimes C_4 \simeq C_2^3 \rtimes C_4$$

Pour les détails, voir ce qui suit qui présente un contexte un peu plus général. **Il est erroné**. J'aurais mieux fait de continuer à travailler dans le cas particulier !

Ici, on oublie le terrain des homographies (ansi que le coup de σ d'ordre 4) et on se met dans le contexte plus général qui suit.

$$\begin{array}{c} \mathbf{L}' \\ | \\ \mathbf{L} \\ \text{galoisienne} \left| \langle \sigma \rangle \right. \\ \mathbf{K} \end{array}$$

Extension \mathbf{L}'/\mathbf{K} galoisienne, donc \mathbf{L}'/\mathbf{L} aussi
sous-extension \mathbf{L}/\mathbf{K} galoisienne cyclique

Soit $\tilde{\sigma}$ un prolongement à \mathbf{L}' de σ (j'ai souligné "un" car il n'est pas unique). Alors

$$\text{Gal}(\mathbf{L}'/\mathbf{L}) \cap \langle \tilde{\sigma} \rangle = \{\text{Id}_{\mathbf{L}'}\}$$

FAUX : c'est cette intersection qui est problématique; en utilisant ce genre d'âneries, je vais finir par montrer que le groupe quaternionien \mathbb{Q}_8 est un produit semi-direct non trivial. **A REVOIR**.

Le sous-groupe $\text{Gal}(\mathbf{L}'/\mathbf{L})$ étant un sous-groupe distingué de $\text{Gal}(\mathbf{L}'/\mathbf{K})$, il est légitime d'écrire un produit :

$$(\star) \quad \text{Gal}(\mathbf{L}'/\mathbf{L}) \cdot \langle \tilde{\sigma} \rangle \subseteq \text{Gal}(\mathbf{L}'/\mathbf{K})$$

Mais du point de vue des cardinaux :

$$\#\text{Gal}(\mathbf{L}'/\mathbf{L}) = [\mathbf{L}' : \mathbf{L}], \quad \#\langle \tilde{\sigma} \rangle \geq \#\langle \sigma \rangle = [\mathbf{L} : \mathbf{K}]$$

Donc d'une part, l'inclusion dans (\star) est une égalité et d'autre part, $\langle \tilde{\sigma} \rangle$ est un groupe cyclique de même ordre que $\langle \sigma \rangle$. Bilan : un produit semi-direct :

$$\text{Gal}(\mathbf{L}'/\mathbf{K}) = \text{Gal}(\mathbf{L}'/\mathbf{L}) \rtimes \langle \tilde{\sigma} \rangle \simeq \text{Gal}(\mathbf{L}'/\mathbf{L}) \rtimes \langle \sigma \rangle$$