Problème : On se pose la question de calculer le groupe de Galois (sur $\mathbb{Q}$, pour fixer les idées) d'une équation en t^2, c'est-à-dire du corps de décomposition d'un polynôme $P(t) = Q(t^2)$, en supposant au moins connu le groupe de Galois de $Q(u)$.

On supposera donc $Q \in \mathbb{Q}[u]$ irréductible, et on définit alors $P(t) = Q(t^2)$. On appellera ϑ_i (pour $i \in I$) les racines de Q et $L = \mathbb{Q}(\vartheta_i)$ le corps de décomposition de Q : pour chaque i on fixe ξ_i une racine carrée de ϑ_i, de sorte que $\Xi = \{\pm\xi_i\}$ est l'ensemble des racines de P et $E = \mathbb{Q}(\xi_i)$ en est le corps de décomposition. On suppose connu au moins $N = \mathrm{Gal}(L/\mathbb{Q})$, et on cherche à comprendre $G = \mathrm{Gal}(E/\mathbb{Q})$ dont N est le quotient par le sous-groupe distingué $H = \mathrm{Gal}(E/L)$:

$$1 \to H \to G \to N \to 1$$

Maintenant, tout élément $\tau \in H$ doit envoyer ξ_i sur $\pm\xi_i$ (i.e., sur $+\xi_i$ ou $-\xi_i$), donc une fois réalisé le choix des ξ_i on a un plongement $\Phi_H \colon H \hookrightarrow \{\pm1\}^I$ envoyant τ sur l'élément $\varepsilon \in \{\pm1\}^I$ tel que $\tau(\xi_i) = \varepsilon_i \xi_i$.

Cherchons à prolonger ce plongement Φ_H à un plongement de G dans un groupe « connu ». Pour cela, un élément $\sigma \in N$ peut se voir comme une permutation des ϑ_i, donc N opère (par automorphismes) sur $\{\pm1\}^I$ en envoyant (ε_i) sur $((\sigma * \varepsilon)_i) = (\varepsilon_{\sigma^{-1}(i)})$ (avec l'abus de notation consistant à écrire $\sigma^{-1}(i)$ pour le j tel que $\vartheta_j = \sigma^{-1}(\vartheta_i)$). Cette action incite à introduire le groupe

$$\mathfrak{G} = \{\pm1\}^I \rtimes N$$

(également noté $\{\pm1\} \wr I$) : en clair, il s'agit de l'ensemble des couples (ε, σ) où $\sigma \in N$ et $\varepsilon \in \{\pm1\}^I$, avec le produit $(\varepsilon', \sigma') \cdot (\varepsilon, \sigma) = (\varepsilon'(\sigma' * \varepsilon),\ \sigma'\sigma)$. Or à tout élément $\tilde\sigma \in G$ on peut associer un couple (ε, σ) de la façon suivante : premièrement, $\sigma \in N = \mathrm{Gal}(L/\mathbb{Q})$ est la restriction de $\tilde\sigma \in G = \mathrm{Gal}(E/\mathbb{Q})$ à L, deuxièmement, ε est choisi de sorte que $\tilde\sigma(\xi_i) = \varepsilon_{\sigma(i)}\, \xi_{\sigma(i)}$ (de nouveau, $\sigma(i)$ est un abus de notation pour le j tel que $\vartheta_j = \sigma(\vartheta_i)$). Appelons $\Phi \colon G \to \mathfrak{G}$ le morphisme en question : on voit facilement que

– Φ est un morphisme de groupes (en effet, si $\tilde\sigma, \tilde\sigma' \in G$ alors $\tilde\sigma'\tilde\sigma(\xi_i) = \varepsilon'_{\sigma'\sigma(i)}\varepsilon_{\sigma(i)}\xi_{\sigma'\sigma(i)} = \varepsilon''_{\sigma'\sigma(i)}\xi_{\sigma'\sigma(i)}$ si $\varepsilon''_j = \varepsilon'_j\varepsilon_{\sigma'^{-1}(j)}$ soit $\varepsilon'' = \varepsilon'\,(\sigma' * \varepsilon)$) ;
– ce morphisme est injectif (son noyau est l'ensemble des $\tilde\sigma \in G$ qui envoient chaque ξ_i sur lui-même) ;
– il prolonge $\Phi_H \colon H \hookrightarrow \{\pm1\}^I$ déjà défini (à condition d'identifier $\{\pm1\}^I$ à un sous-groupe de $\mathfrak{G}$ de la façon évidente).

On peut résumer cela par le diagramme commutatif :

$$\begin{array}{ccccccccc}
 & & & & & \overset{s}{\curvearrowleft} & & & \\
1 & \longrightarrow & \{\pm1\}^I & \longrightarrow & \mathfrak{G} & \longrightarrow & N & \longrightarrow & 1 \\
 & & \Big\uparrow{\scriptstyle \Phi_H} & & \Big\uparrow{\scriptstyle \Phi} & & \Big\| & & \\
1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & N & \longrightarrow & 1
\end{array}$$

dont les lignes sont exactes et celle d'en haut est scindée par la flèche $s \colon \sigma \mapsto ((+1), \sigma)$.

Moralité : On peut se permettre d'identifier G à son image (par Φ) dans $\mathfrak{G}$, ce dernier étant vu comme un groupe de couples formés d'une permutation σ des ϑ_i (figurant dans N, c'est-à-dire d'un automorphisme de L) et d'un choix de signes ε pour prolonger σ en $\tilde\sigma$; le groupe $\mathfrak{G}$ peut se comprendre comme le groupe le plus général possible dans la situation considérée (équation en t^2 sur une équation de groupe N).

Attention cependant : ce n'est pas parce que l'extension $1 \to \{\pm1\}^I \to \mathfrak{G} \to N \to 1$ est scindée (par construction !) et que Φ y plonge $1 \to H \to G \to N \to 1$ que cette

dernière est automatiquement scindée elle aussi (il n'y a pas de raison que l'image de N dans $\mathfrak{G}$ tombe dans G, et ce n'est pas le cas en général comme le montre l'exemple de $\mathbb{Q}(\sqrt{2\pm\sqrt{2}})$ pour lequel $G \cong \mathbb{Z}/4\mathbb{Z}$). En fait, la simple connaissance de H et de N ne permet pas de retrouver G, il y a en général plusieurs extensions possibles (les exemples $E = \mathbb{Q}(\sqrt{2\pm\sqrt{2}})$ et $E = \mathbb{Q}(\sqrt{2\pm\sqrt{3}})$ ont tous les deux un groupe de Galois extension du même sous-groupe $H \leq \{\pm 1\}^2$ (à savoir $\{(+1,+1),(-1,-1)\}$) par $N = \mathbb{Z}/2\mathbb{Z}$, et pourtant ils ne sont pas isomorphes) : en général, il va falloir retrouver non seulement H mais aussi quels éléments de $\mathfrak{G}$ appartiennent à G (au-dessus d'un élément donné de N) ; si l'on préfère, trouver G revient à trouver la section $N \to \mathfrak{G}/H$ définie par l'isomorphime $N \xrightarrow{\sim} G/H$ (le sous-groupe H est distingué dans $\mathfrak{G}$ puisqu'il est stable par conjugaison par tout élément de G mais aussi tout élément de $\{\pm 1\}^I$).

Il y a un cas particulièrement favorable : si $H = \{\pm 1\}^I$ tout entier alors certainement $G = \mathfrak{G}$ tout entier (ne serait-ce que pour des raisons de cardinal) et il est donc complètement compris. C'est le cas par exemple si H contient un élément qui réalise *un unique* changement de signe ($\xi_r \mapsto -\xi_r$ et $\xi_i \mapsto \xi_i$ pour tout $i \neq r$) : en effet, dans ce cas, comme l'action de N sur I est transitive (on a supposé Q irréductible), on peut réaliser n'importe quel changement de signe unique, donc n'importe quelle combinaison de changements de signes, i.e., $H = \{\pm 1\}^I$. Plus généralement, c'est le cas si H contient un élément ε tel que les $\sigma * \varepsilon$ engendrent $\{\pm 1\}^I$. (Noter qu'on n'a pas eu besoin de supposer P irréductible dans tout ça : on l'obtient automatiquement.)

Pour trouver des éléments de H, les techniques usuelles sont applicables : si toutes les racines de Q sont réelles, la conjugaison complexe réalise un élément de H dont le nombre de changements de signes est connu (c'est le nombre de racines négatives[1] de Q) ; de même, si Q est scindé à racines simples modulo un nombre premier ℓ, on obtient un élément de H qui réalise un nombre de changements de signes égal au nombre de racines de $\bar{Q}$ (la réduction modulo ℓ) qui sont des résidus quadratiques modulo ℓ.

On notera que dans le cas $N = \mathfrak{S}_d$ (avec $d = \deg Q = \#I$), la seule chose pertinente à retenir d'un élément de H est le *nombre* de changements de signes qu'il réalise, puisque ces changements de signes peuvent être reportés sur n'importe lesquels des ξ_i (comme $\mathfrak{S}_d$ opère d fois transitivement sur I).

Dans certains cas, au contraire, on cherche à prouver que H n'est pas $\{\pm 1\}^I$ tout entier. Ceci peut se produire, par exemple, si $\prod_{j\in J}\xi_j \in L$ pour un certain $J \subseteq I$, c'est-à-dire que $\prod_{j\in J}\vartheta_j$ est un carré dans L : alors manifestement $\prod_{j\in J}\varepsilon_j = +1$ pour tout $\varepsilon \in H$. En fait, en voyant $\{\pm 1\}^I$ comme $(\mathbb{Z}/2\mathbb{Z})^I$ et par de l'algèbre linéaire, montrer que H est plus petit que $(\mathbb{Z}/2\mathbb{Z})^I$ revient à montrer qu'il est contenu dans un hyperplan, noyau d'une certaine forme linéaire, c'est-à-dire justement qu'il existe une partie $J \subseteq I$ telle que tout $\varepsilon \in H$ réalise $\prod_{j\in J}\varepsilon_j = +1$, et ceci signifie précisément que $\prod_{j\in J}\vartheta_j$ est un carré dans L. Un cas particulier est celui où $J = I$ et où $\prod_{j\in I}\vartheta_j$ (soit $(-1)^d$ fois le coefficient constant de Q) est un carré dans L : dans ce cas, on sait d'emblée que H sera inclus dans $\{\varepsilon : \prod_{j\in I}\varepsilon_j = 1\}$; mais cela peut se produire pour deux raisons : soit $\prod_{j\in I}\vartheta_j$ est un carré dans $\mathbb{Q}$, auquel cas $\prod_{j\in I}\xi_j$ est invariant par G, donc tout $(\varepsilon,\sigma) \in G$ vérifie $\prod_{j\in I}\varepsilon_j = 1$ (on a donc bien $G = H \rtimes N$ dans ce cas) ; soit le produit $\prod_{j\in I}\xi_j$ appartient à L sans appartenir à $\mathbb{Q}$, auquel cas $\sigma \mapsto \prod_{j\in I}\varepsilon_j$, où $(\varepsilon,\sigma) \in G$, définit un morphisme $N \to \{\pm 1\}$ non trivial, qui dans le cas $N = \mathfrak{S}_d$ ne peut être que la signature (et ceci conduit à des situations où $1 \to H \to G \to N \to 1$ n'est pas scindé puisque l'image de N dans $\mathfrak{G}$ n'est pas dans G).

([1]) À ce sujet, pour calculer le nombre de racines de négatives d'un polynôme, l'algorithme de Sturm-Liouville est particulièrement adapté.

Quelques exemples

On va maintenant voir sur des exemples comment ces situations se produisent et par quelles méthodes on peut prouver quel est exactement le groupe de Galois.

• Commençons par une situation dans laquelle $G = \mathfrak{G}$ avec $N = \mathfrak{S}_d$. C'est le cas, par exemple, pour $P(t) = t^8 - 2t^6 - 8t^4 + 17t^2 - 5$: on vérifie que $Q(u) = u^4 - 2u^3 - 8u^2 + 17u - 5$ est irréductible avec pour groupe de Galois $N = \mathfrak{S}_4$ (c'est facile en réduisant modulo 2 et 3) ; or Q a toutes ses racines réelles et une seule est négative, donc la conjugaison complexe réalise un $\tau \in H$ qui opère un seul changement de signe. D'après ce qu'on a expliqué, ceci prouve que le groupe de Galois G de P est $\{\pm 1\}^4 \rtimes \mathfrak{S}_4$ (le plus gros possible pour une équation biquartique), d'ordre 384.

• Donnons un exemple où on a encore $G = \mathfrak{G}$ mais cette fois avec $N = \mathfrak{A}_d$: on prend $Q(u) = u^4 - 8u^3 + 7u^2 + 5u - 3$, dont le discriminant est $\Delta_Q = 589^2$ et dont les réductions modulo 2 (factorisable en degrés $1 + 3$) et 7 (factorisable en degrés $2 + 2$) montre qu'il a pour groupe de Galois $\mathfrak{A}_4$. Mais, de nouveau, Q a quatre racines réelles dont exactement une est négative, et ce qu'on a expliqué prouve qu'alors $G = \{\pm 1\}^4 \rtimes \mathfrak{A}_4$ comme groupe de Galois du polynôme $P(t) = t^8 - 8t^6 + 7t^4 + 5t^2 - 3$. Il a pour ordre 192.

• De même, considérons $Q(u) = u^4 - 8u^3 + 18u^2 - 8u - 2$. Ses racines sont $2 \pm \sqrt{3 \pm \sqrt{3}}$, et son groupe de Galois N est le groupe diédral du carré D_4 : pour s'en convaincre, on peut réduire modulo 7 (c'est irréductible donc on a trouvé un 4-cycle dans le groupe de Galois) et 11 (la réduction se fait en facteurs de degré $1 + 1 + 2$, ce qui donne une transposition), et comme N n'est manifestement pas $\mathfrak{S}_4$ tout entier (car tout élément fixant $\sqrt{3 + \sqrt{3}}$ fixe aussi $-\sqrt{3 + \sqrt{3}}$), c'est D_4. On pose $P(t) = Q(t^2) = t^8 - 8t^6 + 18t^4 - 8t^2 - 2$ comme d'habitude : puisque Q a quatre racines réelles dont exactement une est négative, on a $G = \{\pm 1\}^4 \rtimes D_4$, d'ordre 128.

• Passons maintenant à un exemple où H est plus petit, avec $N = \mathfrak{S}_d$. Soit $P(t) = t^8 - 4t^6 - 8t^4 + 11t^2 + 9$: de nouveau, le groupe de Galois de $Q(u) = u^4 - 4u^3 - 8u^2 + 11u + 9$ est $N = \mathfrak{S}_4$. Mais cette fois, le coefficient constant, $c_0 = 9$, c'est-à-dire $\prod_{j=1}^4 \vartheta_j$, est un carré, donc tout élément de H doit réaliser un nombre *pair* de changements de signes sur les ξ_i. Or Q a quatre racines réelles dont deux négatives : ceci prouve que la conjugaison complexe réalise deux changements de signes, et puisque $N = \mathfrak{S}_4$ (en particulier, il est 2-transitif) ces changements de signes peuvent être quelconques, et H est exactement le noyau — isomorphe à $\{\pm\}^3$ — de $\{\pm 1\}^4 \to \{\pm 1\}$ envoyant ε sur $\prod_{j=1}^4 \varepsilon_j$.

Puisque H est plus petit que $\{\pm 1\}^4$, il n'est pas trivial *a priori*, sur ce dernier exemple, que la suite exacte $1 \to H \to G \to N \to 1$ est scindée. En fait, elle l'est, c'est-à-dire que la surjection $G \to N$ admet une section : en effet, si $\sigma \in N$, on peut le relever en un élément de G qu'on voit comme $(\varepsilon, \sigma) \in \mathfrak{G}$, et nécessairement ε a un nombre pair de -1 vu que le produit de tous les ξ_i est un rationnel (3 ou -3 selon le choix des racines carrées, mais en tout cas invariant par l'action de G), donc ε appartient bien à H et on peut l'annuler, c'est-à-dire relever $\sigma \in N$ en $((+1), \sigma) \in \mathfrak{G}$ (le point subtil étant que ce $((+1), \sigma)$ appartient bien à G). On a donc prouvé ici que le groupe de Galois G de P était $H \rtimes \mathfrak{S}_4$ où $H \leq \{\pm 1\}^4$ est le sous-groupe des quadruplets ε dont un nombre pair vaut -1. Il a pour ordre 192.

• Pour comparer, donnons un exemple où l'extension $1 \to H \to G \to N \to 1$ n'est pas scindée[2] : on prendra $P(t) = t^8 + 6t^6 - 2t^2 - 3$. Le groupe de Galois de $Q(u) = u^4 + 6u^3 - 2u - 3$ est $\mathfrak{S}_4$. Modulo 103, la réduction $\bar{Q}$ du polynôme Q est scindée, ses racines sont 20, 34, 53

([2]) L'exemple le plus simple, déjà signalé, est $t^4 - 4t^2 + 2$ (racines $\pm\sqrt{2 \pm \sqrt{2}}$) avec groupe $G = C_4 = \mathbb{Z}/4\mathbb{Z}$: on a $H = \{\pm 1\}$ l'unique sous-groupe d'indice 2 dans C_4 (changement de signe simultané sur $\sqrt{2 + \sqrt{2}}$ et $\sqrt{2 - \sqrt{2}}$) et $N = \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = C_2$, et l'extension $1 \to H \to G \to N \to 1$ n'est visiblement pas scindée.

et 93, et comme exactement deux de ces nombres sont des carrés (dans $\mathbb{Z}/103\mathbb{Z}$), il y a dans H un élément réalisant deux changements signes, donc, par le même raisonnement qu'avant ($\mathfrak{S}_4$ opère deux fois transitivement) n'importe quels deux changements de signes donc tout nombre pair de changements de signes.

La différence avec le cas précédent et que cette fois $c_0 = \prod_{j=1}^4 \vartheta_j = -3$ n'est pas un carré dans $\mathbb{Q}$: mais $c_0\Delta_Q = 936^2$, où Δ_Q désigne le discriminant de Q, en est un. Donc $\prod_{j=1}^4 \xi_j$ est un multiple rationnel de $\sqrt{\Delta_Q}$ (et notamment il appartient à L). Ainsi, si $\sigma \in N = \mathfrak{S}_4$ est une permutation *paire* (de sorte que $\sigma(\sqrt{\Delta_Q}) = \sqrt{\Delta_Q}$), on a $\tilde\sigma(\prod_j \xi_j) = \prod_j \xi_j$ pour tout prolongement $\tilde\sigma$ de σ à G, c'est-à-dire que tout couple $(\varepsilon, \sigma) \in \mathfrak{G}$ qui appartient à G doit avoir un nombre *pair* de -1 dans ε et (comme précédemment) on en conclut que $((+1), \sigma) \in G$; en revanche, si σ est *impaire*, on a $\tilde\sigma(\prod_j \xi_j) = -\prod_j \xi_j$, c'est-à-dire que tout couple (ε, σ) appartenant à G doit cette fois avoir un nombre *impair* de -1 dans ε. Comme on sait qu'on a au moins $(\#H)(\#N) \geq 8 \times 24 = 192$ éléments dans G et qu'on vient d'expliquer qu'il y en a au plus $\frac{1}{2}16 \times 24 = 192$, c'est le nombre précis. On a donc prouvé que G était le sous-groupe de $\{\pm1\}^4 \rtimes \mathfrak{S}_4$ formé des couples (ε, σ) pour lesquels la parité (=signature) de σ est égale à la parité du nombre de -1 dans ε. Et la suite $1 \to H \to G \to N \to 1$ n'est pas scindée : par exemple parce que chacun des huit antécédents d'un 4-cycle dans $N = \mathfrak{S}_4$ est d'ordre 8 dans G.

(On vient de donner trois exemples, $t^8 - 8t^6 + 7t^4 + 5t^2 - 3$, $t^8 - 4t^6 - 8t^4 + 11t^2 + 9$ et $t^8 + 6t^6 - 2t^2 - 3$, d'équations biquartiques dont le groupe de Galois est d'ordre 192, à savoir dans $\{\pm1\}^4 \rtimes \mathfrak{S}_4$ les sous-groupes correspondant aux conditions que la seconde coordonnée soit paire, que la première le soit, ou que les deux aient même parité. Certainement ils sont différents en tant que sous-groupes (d'indice 2) de $\{\pm1\}^4 \rtimes \mathfrak{S}_4$. Mais on peut se demander s'ils sont isomorphes en tant que groupes abstraits... il n'en est rien : dans le premier cas il y a un sous-groupe distingué d'ordre 16, à savoir $\{\pm1\}^4 \cong (\mathbb{Z}/2\mathbb{Z})^4$, alors que les deux autres ne l'ont pas ; dans le second cas il y a trois sous-groupes distingués isomorphes à $(\mathbb{Z}/2\mathbb{Z})^3$ alors que le troisième cas n'en a qu'un — en revanche il a deux sous-groupes distingués isomorphes au groupe des quaternions.)

• Pour donner un exemple avec H encore plus petit, prenons $P(t) = t^8+5t^6+7t^4+4t^2-4$: cette fois, $Q(u) = u^4 + 5u^3 + 7u^2 + 4u - 4$, qui a encore groupe de Galois $N = \mathfrak{S}_4$, est scindé modulo 113 et $P(t)$ s'y factorise comme produit de quatre facteurs quadratiques. Donc il y a un élément (-1) (constamment égal à -1) dans H. En fait, il s'avère que H est effectivement réduit à $\{\pm1\}$, c'est-à-dire que chaque produit $\xi_r\xi_s$ avec $r \neq s$ appartient en fait à $L = \mathbb{Q}(\vartheta_i)$. Une façon de le montrer serait de constater que le polynôme $R(t) = \prod_{\pm,\pm,\pm}^{i<j<k} (t \pm \xi_i \pm \xi_j \pm \xi_k)$ dont les racines sont tous les $\pm\xi_i \pm \xi_j \pm \xi_k$ pour une certaine combinaison de signes et $\{\xi_i, \xi_j, \xi_k\}$ une partie à trois éléments de $\{\xi_n\}$ (ce polynôme est donc de degré 32, c'est-à-dire en fait de degré 16 en l'indéterminée t^2), qui est à coefficients entiers puisque ce sont des polynômes totalement symétriques à coefficients entiers des racines de P, est séparable, et admet un facteur $R_0(t) = t^8 + 15t^6 + 30t^4 - 233t^2 - 49$ de degré 8. Considérons l'ensemble $\mathscr{R}$ des ensembles de trois racines de P dont la somme est racine de R_0 : ce facteur nous donne donc une partie $\mathscr{R}$ de cardinal 8 de l'ensemble des parties à trois éléments de $\Xi = \{\pm\xi_n\}$, qui est invariante sous l'action de G : donc, donné trois indices $i < j < k$ (il y a quatre choix possibles de tels indices, et ils sont interchangeables par l'action de $N = \mathfrak{S}_4$), il existe exactement deux choix (opposés) des signes pour que $\{\pm\xi_i, \pm\xi_j, \pm\xi_k\} \in \mathscr{R}$; or dans ces conditions, H ne peut pas être plus que $\{\pm1\}$, puisque l'action de H (comme de n'importe quoi dans G) doit préserver $\mathscr{R}$. Soit en calculant précisément (numériquement, par exemple) quels triplets appartiennent à $\mathscr{R}$, soit en étudiant les sous-groupes transitifs d'ordre 48 de $\mathfrak{S}_8$ et en excluant la possibilité $\{\pm1\} \times \mathfrak{S}_4$

(car $c_0 = \prod_{j=1}^4 \vartheta_j = -4$ n'est pas un carré dans $\mathbb{Q}$), on peut prouver que dans ce cas $G = GL_2(\mathbb{F}_3)$ agissant sur Ξ comme $\mathbb{F}_3^2$, la relation ternaire $\mathscr{R}$ est donnée par $\{\alpha, \beta, \gamma\} \in \mathscr{R}$ lorsque $\alpha + \beta + \gamma = 0$ dans $\mathbb{F}_3^2$, et la suite exacte non scindée $1 \to H \to G \to N \to 1$ est simplement $1 \to \{\pm 1\} \to GL_2(\mathbb{F}_3) \to PGL_2(\mathbb{F}_3) \to 1$.

• Le groupe de Galois N de $Q(u) = u^4 - 7u^3 + 5u^2 + 2u - 2$ est D_4 (groupe diédral du carré), et ses racines sont $\frac{1}{4}(7 \pm \sqrt{17} \pm' \sqrt{90 \pm 22\sqrt{17}})$ (où les deux signes devant $\sqrt{17}$ sont les mêmes). En posant $P(t) = Q(t^2)$, on est de nouveau dans une situation où $c_0\Delta_Q = (665\,856)^2$ est un carré dans $\mathbb{Q}$: on ne va pouvoir réaliser que des éléments $(\varepsilon, \sigma) \in \mathfrak{G}$ pour lesquels ε a un nombre de -1 de la même parité que la permutation σ ; seulement, cette fois, σ vit dans $N = D_4$, qui n'opère pas deux fois transitivement sur $\Theta = \{\theta_n\}$, donc pour s'assurer qu'on réalise bien tous ces éléments il ne suffit plus de trouver un seul élément réalisant deux changements de signe quelconques... Par exemple, modulo 43, la réduction $\bar{Q}$ de Q est scindée et $\bar{P}$ donne un élément de H réalisant deux changements de signes, mais il faut encore constater que les deux changements de signes se font sur des ξ_i tels que les ϑ_i correspondants soient « adjacents » pour la structure de carré impliquée par $N = D_4$ (si on préfère, ils correspondent à des choix différents du signe $\pm\sqrt{17}$) : une fois cette observation faite, on obtient n'importe quels deux changements de signes « adjacents » donc aussi deux changements de signes « opposés », donc on a bien H d'indice 2 dans $\{\pm 1\}^4$ égal aux ε comportant un nombre pair de signes -1, et G est le sous-groupe d'indice 2 de $\{\pm 1\}^4 \rtimes D_4$ égal aux couples (ε, σ) pour lesquels ε a un nombre de -1 de la même parité que la permutation σ. L'ordre de G est 64.

• Pour finir, soit $Q(u) = u^4 - 6u^3 + 2u - 1$, dont le groupe de Galois est de nouveau D_4 et dont les racines sont $\frac{1}{2}(3 \pm \sqrt{5} \pm' \sqrt{22 \pm 10\sqrt{5}})$. La constatation intéressante est que, si $\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4$ sont dans l'ordre « adjacentes » pour la structure diédrale (c'est-à-dire que ϑ_1, ϑ_3 d'une part, et ϑ_2, ϑ_4 de l'autre, font les mêmes choix de signe dans $\pm\sqrt{5}$) alors $\vartheta_1\vartheta_3$ est le carré de $\frac{1}{2}(2\vartheta_2^3 - 11\vartheta_2^2 - 6\vartheta_2 + 3) = -2 \pm \sqrt{5} \in L$ (et bien sûr aussi de la même expression avec ϑ_4 à la place de ϑ_2). Ceci prouve que si ξ_i est (pour chaque i) une racine de ϑ_i, alors $\xi_1\xi_3 \in L$ et bien sûr aussi $\xi_2\xi_4 \in L$: donc H a quatre éléments, on peut effectuer des changements de signes sur ξ_1 et ξ_3 simultanément, et/ou sur ξ_2 et ξ_4 simultanément. Mais même une fois connu le sous-groupe $H \leq \{\pm 1\}^4$, il reste (à conjugaison près) quatre sous-groupes (par ailleurs abstraitement deux à deux non isomorphes) G, d'ordre 32, de $\mathfrak{G}$ qui réalisent une extension $1 \to H \to G \to D_4 \to 1$. On peut trouver auquel d'entre eux on a affaire en constatant, par exemple, que le $\sigma \in N = D_4$ qui échange ϑ_2 et ϑ_4 en laissant ϑ_1, ϑ_3 fixes se relève en un $\tilde{\sigma} \in G$ qui échange ξ_1 et ξ_4 tout en échangeant ξ_3 et $-\xi_3$ (dans les autres extensions de H par D_4 dans $\mathfrak{G}$ les relèvements de σ réaliseraient par exemple des cycles $\xi_2 \mapsto \xi_4 \mapsto -\xi_2 \mapsto -\xi_4$ ou bien laisseraient ξ_1, ξ_3 tous deux fixes) ; or, de fait, $\tilde{\sigma}$ est réalisé par la conjugaison complexe (si on appelle $\vartheta_1 = \frac{1}{2}(3 + \sqrt{5} + \sqrt{22 + 10\sqrt{5}})$).