Groupe de Galois d'un polynôme irréductible de degré 4 sur $\mathbb{Q}$: une simplification.

1) Introduction

La détermination du groupe de Galois d'un polynôme $P \in \mathbb{Q}[X]$ irréductible et de degré 4 est bien connue, le cas le plus délicat étant le cas où le polynôme résolvant (de Descartes) R de P a une et une seule racine rationnelle, cas où le groupe de Galois de P est alors, à isomorphisme près, $\mathbb{Z}/4\mathbb{Z}$ ou D_4 (groupe diédral d'ordre 8). "Anciennement", dans ce cas, on se contentait de conclure en donnant le critère suivant : si P est réductible sur $\mathbb{Q}(\sqrt{\Delta})$, Δ étant le discriminant de P, le groupe de Galois de P est $\mathbb{Z}/4\mathbb{Z}$, sinon c'est D_4 ([2] : appendix A).

Depuis, ce critère a été simplifié, mais parfois dans des cas particuliers, ou avec deux quantités à tester (carré ou pas). Je propose ici un critère simplifié valable pour tout polynôme P et avec une seule quantité à tester.

Par exemple pour $P(X) = X^4 + \frac{1}{3}X^2 + X - \frac{23}{36}$ (irréductible sur $\mathbb{Q}$: voir critère au 2)), son résolvant de Descartes étant $R(X) = (X - \frac{1}{3})(X^2 + X + 3)$, son groupe de galois est $\mathbb{Z}/4\mathbb{Z}$ ou D_4. Je laisse le lecteur voir si P est réductible ou pas sur $\mathbb{Q}(\sqrt{\Delta})$….

En fait, $\frac{1}{3}$(la seule racine rationnelle de R) $\times -11$(discriminant de $X^2 + X + 3$) n'est pas un carré dans $\mathbb{Q}$, donc P a pour groupe de Galois D_4.

Je donne une preuve de ce critère simplifié en explicitant les huit éléments possibles du groupe de Galois de P (dans ce cas) et je mets en évidence un élement de son corps de décomposition, qui selon qu'il est rationnel ou pas donne $\mathbb{Z}/4Z$ ou D_4 comme groupe de Galois.

Ce critère simplifié permet d'ailleurs de déterminer instantanément le groupe de Galois de tout polynôme bicarré $X^4 + pX^2 + r$ (irréductible) sans calculer Δ.

2) Liens entre $P \in \mathbb{Q}[X]$ de degré 4 et son résolvant R de Descartes : racines, irréductibilité, discriminant.

Dans tout ce qui suit je pose $P(X) = X^4 + pX^2 + qX + r \in \mathbb{Q}[X]$, unitaire ; tout polynôme de degré 4 unitaire peut se ramener par translation d'un rationnel sur X à un polynôme sans terme en X^3 : s'il est irréductible sur $\mathbb{Q}$, il reste irréductible, son discriminant reste inchangé, de même que son groupe de Galois.

Soit $R(X) = X^3 + 2pX^2 + (p^2 - 4r)X - q^2$ le polynôme résolvant de Descartes.

Ce polynôme résolvant résulte de la caractérisation suivante (facile à vérifier)

lorsque $q \neq 0$, alors

$P(X) = (X^2 + aX + b)(X^2 + cX + d)$ avec a, b, c, d dans $\mathbb{C}$

$\Leftrightarrow a \neq 0, R(a^2) = 0$ et $c = -a, b = \frac{1}{2}(p + a^2 - \frac{q}{a}), d = \frac{1}{2}(p + a^2 + \frac{q}{a})$

Note : si $a \in \mathbb{Q}$, alors b, c, d sont aussi dans $\mathbb{Q}$.

On en déduit tout de suite un critère d'irréductibilité de P lorsque $q \neq 0$:

P est irréductible sur $\mathbb{Q}$ $\Leftrightarrow$ P n'a pas de racine rationnelle et R n'a pas de racine qui soit le carré d'un rationnel.

(parceque, notamment, si $P = UV$ avec U, V dans $\mathbb{Q}[X]$ de degrés 2, on peut supposer U et V unitaires en les factorisant par leurs coefficients de tête dont le produit est 1).

On verra au 3) un critère particulier dans le cas $q = 0$.

Application au cas $P(X) = X^4 + \frac{1}{3}X^2 + X - \frac{23}{36}$.

Son résolvant R (voir introduction) n'a pas de racine qui soit le carré d'un rationnel ; montrons que P n'a pas de racine rationnelle.

Si $P(\frac{a}{b}) = 0$ avec $a, b > 0$ entiers premiers entre eux alors

$36a^4 + 12a^2b^2 + 36ab^3 - 23b^4 = 0$, donc a divise 23 et $a = \pm 1$ ou ± 23 ; 12 divisant $23b^4$, $2 \times 3 = 6$ divise b, d'où 6^3 divise $36a^4$ et a est pair ce qui est exclu et ainsi $\frac{a}{b}$ n'est pas racine de P.

Donc P est irréductible sur $\mathbb{Q}$.

Le passage des racines y_1, y_2, y_3 ($\in \mathbb{C}$) de R aux racines x_1, x_2, x_3, x_4 ($\in \mathbb{C}$) de P se fait ainsi :

que q soit nul ou pas, en choisissant, pour $i = 1, 2, 3$, a_i tel que $a_i^2 = y_i$ avec $a_1 a_2 a_3 = q$ (c'est possible car $y_1 y_2 y_3 = q^2$; **si** $q = 0$, **on prendra toujours** $y_1 = a_1 = 0$, y_2, y_3 étant alors les racines de $X^2 + 2pX + p^2 - 4r$), alors les racines de P sont

$x_1 = \frac{-a_1 + a_2 + a_3}{2}$; $x_2 = \frac{-a_1 - a_2 - a_3}{2}$; $x_3 = \frac{a_1 + a_2 - a_3}{2}$; $x_4 = \frac{a_1 - a_2 + a_3}{2}$.

En effet, pour $q \neq 0$,

en prenant $a = a_1$ on a $P(X) = (X^2 + aX + b)(X^2 + cX + d)$ avec $c = -a_1$,

$d = \frac{1}{2}(p + a_1^2 + \frac{q}{a_1})$, $b = \frac{1}{2}(p + a_1^2 - \frac{q}{a_1})$.

De $a^2 - 4b = y_1 - 2p - 2y_1 + \frac{2q}{a_1} = -y_1 - 2p + 2a_2a_3 = y_2 + y_3 + 2a_2a_3 = (a_2 + a_3)^2$ on déduit que les racines de $(X^2 + aX + b)$ sont $\frac{-a_1 \pm (a_2 + a_3)}{2}$.

De façon analogue, les racines de $(X^2 + cX + d)$ sont $\frac{a_1 \pm (a_2 - a_3)}{2}$.

Si $q = 0$, $a_2^2 + a_3^2 = -2p$ et $a_2^2 a_3^2 = p^2 - 4r$, d'où $4r = \frac{(a_2^2 - a_3^2)^2}{4}$ et

$P(X) = X^4 + pX^2 + r = (X^2 - \frac{a_2^2 + a_3^2}{4})^2 - \frac{a_2^2 a_3^2}{4} = (X^2 - (\frac{a_2 + a_3}{2})^2)(X^2 - (\frac{a_2 - a_3}{2})^2)$ et les quatre racines de P sont les quatre racines x_i obtenues dans le cas $q \neq 0$ en y faisant $a_1 = 0$.

Remarque 1 : ces formules prouvent que les racines de P s'obtiennent par radicaux à partir des coefficients de P.

Remarque 2 : $s_{1,2} = x_1x_2 + x_3x_4 = \frac{a_1^2 - (a_2 + a_3)^2}{4} + \frac{a_1^2 - (a_2 - a_3)^2}{4} = y_1 + p$ (puisque $\sum y_i = -2p$) et $t_{1,2} = (x_1 + x_2)(x_3 + x_4) = -a_1 \times a_1 = -y_1$.

De même, $s_{1,3} = y_2 + p, s_{1,4} = y_3 + p, t_{1,3} = -y_2, t_{1,4} = -y_3$.

P et R ont le même discriminant $\Delta \in \mathbb{Q}$:

en effet, par définition, P et R étant unitaires,

$\Delta(P) = \prod_{1 \leq i < j \leq 4} (x_i - x_j)^2$ et $\Delta(R) = (y_1 - y_2)^2(y_1 - y_3)^2(y_2 - y_3)^2$

et, par exemple, $y_1 - y_2 = (a_1 - a_2)(a_1 + a_2) = (x_4 - x_1)(x_3 - x_2)$, donc $\Delta(P) = \Delta(R) = \Delta$.

Pour expliciter $\Delta = \Delta(R)$, on transforme R par translation sur X ($X \to X - \frac{2p}{3}$) en un polynôme de degré 3 sans terme en X^2, c'est-à-dire de la forme $X^3 + p'X + q'$ et, son discriminant étant conservé, $\Delta = -(4p'^3 + 27q'^2)$, soit :

$\Delta = 4(\frac{p^2}{3} + 4r)^3 - 27(\frac{2p^3}{27} - \frac{8pr}{3} + q^2)^2$
$\Delta = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3$; si $q = 0$, $\Delta = 16r(p^2 - 4r)^2$.

P étant irréductible sur $\mathbb{Q}$, ses racines sont distinctes, donc $\Delta = \Delta(P)$ est non nul, et comme $\Delta(P) = \Delta(R)$, R a aussi ses racines distinctes.

3) Détermination du groupe de Galois, sur $\mathbb{Q}$, de $P(X) = X^4 + pX^2 + qX + r$ irréductible.

Je noterai G le groupe de Galois de P sur $\mathbb{Q}$ et $\sqrt{\Delta}$ désignera toujours une racine 2ième de Δ (dans $\mathbb{C}$), même si $\Delta < 0$.

Si Δ n'est pas un carré dans $\mathbb{Q}$, le plus petit corps contenant $\mathbb{Q}$ et $\sqrt{\Delta}$ est $\mathbb{Q}(\sqrt{\Delta}) = \{u + v\sqrt{\Delta}\ ;\ (u,v) \in \mathbb{Q}^2\}$; $\sqrt{\Delta}$ étant algébrique sur $\mathbb{Q}$ (de degré 2) on peut noter $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}[\sqrt{\Delta}]$.

Dans les deux tableaux ci-dessous, lorsqu'on parle d'irréductibilité sans autre précision c'est sur $\mathbb{Q}$, et lorsqu'on parle de carré sans autre précision, c'est dans $\mathbb{Q}$.

P étant irréductible,

Cas	R (**résolvant** de P)	**Groupe de Galois** (G) **de** P ($\simeq$ pour isomorphe)
1	si R irréductible et Δ pas carré	$G \simeq S_4$
2	si R irréductible et Δ carré	$G \simeq A_4$
3	si $R = d°1 \times d°1 \times d°1$ $\Rightarrow \Delta$ est un carré	$G \simeq V_4 \simeq \{id; (12)(34); (13)(24); (14)(23)\} \subset A_4$ $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est le groupe de Klein
4	si $R = d°1 \times d°2$ (réduction en irréductibles) $\Rightarrow \Delta$ n'est pas un carré	si P est réductible sur $\mathbb{Q}(\sqrt{\Delta})$, $G \simeq \mathbb{Z}/4\mathbb{Z}$ (et $\Delta > 0$) sinon $G \simeq D_4$
4 **simplifié**	si $R(X) = (X - y_1)R_2(X)$ ($y_1 \in \mathbb{Q}, R_2$ irréductible sur $\mathbb{Q}$) on note δ le discriminant de R_2 $\Rightarrow \Delta$ et $\delta \neq$ carrés ; $\frac{\Delta}{\delta} =$ carré $y_1\delta = 2py_1^2 + (3p^2 + 4r)y_1 - 3q^2$ si $q \neq 0, y_1$ n'est pas un carré	si μ est un carré dans $\mathbb{Q}$, $G \simeq \mathbb{Z}/4\mathbb{Z}$ (et $\Delta > 0$) sinon $G \simeq D_4$ avec si $q = 0$, $\mu = r(p^2 - 4r)$ si $q \neq 0$, $\mu = y_1\delta$ (ou $\mu = y_1\Delta$)

La simplification du 4) remplace donc la recherche de l'irréductibilité de P sur $\mathbb{Q}(\sqrt{\Delta})$ par uniquement

si $q = 0$, l'examen de $r(p^2 - 4r)$

si $q \neq 0$, l'examen de $y_1\delta$ (ou de $y_1\Delta$ ... s'il a déjà été calculé).

On peut ainsi différencier très facilement les groupes D_4 et $\mathbb{Z}/4\mathbb{Z}$.

En outre, la détermination de Δ est nécessaire que lorsque R est irréductible.

Cette simplification de la différenciation entre $\mathbb{Z}/4\mathbb{Z}$ et D_4 est aussi faite dans les deux références suivantes :

[5] (théorème 6.15) : avec le même résolvant R, mais que pour le cas $p = 0$ (auquel cas $y_1\delta = 4ry_1 - 3q^2$)

[2] (voir table 8) : avec un autre résolvant que celui de Descartes, mais il y a deux quantités à tester.

Voir quelques exemples à l'annexe 3.

Remarque : si on connaît les racines de P, du tableau ci-dessus on déduit que Gal(P) est V_4 ou $\mathbb{Z}/4\mathbb{Z}$ ou D_4 si et seulement si une des trois expressions $(x_{i_1} + x_{i_2})(x_{i_3} + x_{i_4})$ est rationnelle, puisque d'après une remarque du 2), ces trois expressions sont les opposées des racines de R ; même résultat si on remplace $(x_{i_1} + x_{i_2})(x_{i_3} + x_{i_4})$ par $x_{i_1}x_{i_2} + x_{i_3}x_{i_4}$.

Application au cas particulier où P est bicarré ($q = 0$) : sans avoir à déterminer R, Δ, δ on obtient son groupe de Galois.

Cas bicarré : $P(X) = X^4 + pX^2 + r$ (irréductible)		
(P irréductible $\Leftrightarrow p^2 - 4r$ n'est pas un carré et $\nexists (a,b) \in \mathbb{Q}^2$ tel que $r = b^2$ et $2b - p = a^2$) (*)		
si r est un carré	Gal(P) $\simeq V_4$	$X^4 - 10X^2 + 4$; $X^4 + 1, X^4 + 9$ (**)
si $r \neq$ carré et $r(p^2 - 4r)$ carré	Gal(P) $\simeq \mathbb{Z}/4\mathbb{Z}$	$X^4 - 10X^2 + 5$
si $r \neq$ carré et $r(p^2 - 4r) \neq$ carré	Gal(P) $\simeq D_4$	$X^4 - 2X^2 - 1$, $X^4 + r$ et $r \neq$ carré (***)

En effet, puisque $q = 0$, $R(X) = X(X^2 + 2pX + p^2 - 4r) = XR_2(X)$ et le discriminant δ de R_2 est $\delta = 16r$, donc si r est un carré dans $\mathbb{Q}$, R_2 est réductible sur $\mathbb{Q}$ et c'est le cas 3), si r n'est pas un carré, c'est le cas 4).

(*) : voir annexe 1 pour la preuve ; la 2ième condition d'irréductibilité de P équivaut à $\nexists a \in \mathbb{Q}$ tel que $4r = (a^2 + p)^2$, (si $4r = (a^2 + p)^2$, $r = b^2$ avec $b = \frac{a^2 + p}{2}$ et $2b - p = a^2$) mais en pratique il est presque plus facile de voir si d'abord $r = b^2$, avec $b \in \mathbb{Q}$, et si oui, on regarde si $2b - p$ ou $-2b - p$ est un carré.
si $p = 0$, P irréductible $\Leftrightarrow -r \neq$ carré et $4r \neq a^4$ avec $a \in \mathbb{Q}$; ce résultat se généralise à $X^{2^n} + r$, voir [4].

(**) $X^4 - 1 = (X^2 + 1)(X - 1)(X + 1)$ est réductible ($p^2 - 4r = -4r = 4$ est un carré) ; son corps de décomposition est celui de $X^2 + 1$, à savoir $\mathbb{Q}[i]$ et son groupe de Galois est $\mathbb{Z}/2\mathbb{Z}$.
(***) : on notera que pour $X^4 + r$, $\Delta = 256r^3$ peut être positif ou négatif ; par ailleurs, $X^4 + r$ est irréductible $\Leftrightarrow -r \neq$ carré et $4r \neq a^4$ avec $a \in \mathbb{Q}$ et dans ce cas si on a en outre $r \neq$ carré alors $X^4 + r$ a pour groupe de Galois D_4, puisqu'on a aussi $r(p^2 - 4r) = -4r^2 \neq$ carré. Par exemple $X^4 - 3$ a D_4 pour groupe de Galois : on verra une preuve directe à l'annexe 4.

preuve du 3)

Bien entendu une preuve directe de la simpification du cas 4) **peut se faire en partant de l'ancienne caractérisation** (**voir annexe 2**), **cela en n'utilisant aucun résultat de la théorie de Galois**!
Mais j'ai préféré présenter une preuve qui ne fait pas appel à l'ancienne caractérisation (et en rappelant comment on prouve les trois premiers cas).
La voici :

étape 0 : définitions,résultats (admis) sur Galois utilisés ici (voir [3]).

Soit $T \in \mathbb{Q}[X]$ de degré $n \geq 1$ et Gal(T) son groupe de Galois (sur $\mathbb{Q}$).
Ga1 : Le corps de décomposion de T est le plus petit corps N contenant $\mathbb{Q}$ et les racines (dans $\mathbb{C}$) de T.
Note : l'extension $\mathbb{Q} \subset N$ est alors normale, donc galoisienne car on est en caractéristique 0.
Ga2 : Gal(T) est l'ensemble des $\mathbb{Q}$ –automorphismes de N (c'est-à-dire les isomorphismes de $N \to N$ qui conservent les rationnels) ; son ordre est $[N : \mathbb{Q}]$, c'est-à-dire le degré de l'extension $\mathbb{Q} \subset N$, et si T a n racines distinctes ce groupe est isomorphe à un sous-groupe de S_n, cela parceque tout $\sigma \in$Gal(T) permute les racines z_i de T : $(\sigma(z_1), \sigma(z_2), \ldots, \sigma(z_n)) = (z_{s(1)}, z_{s(2)}, \ldots, z_{s(n)})$ avec $s \in S_n$.
Ga3 : Les seuls éléments de N invariants par tous les éléments de Gal(T) sont les rationnels.
Ga4 : Si T est irréductible sur $\mathbb{Q}$ et unitaire alors Gal(T) est isomorphe à un sous-groupe de A_n si et seulement si le discriminant de T est un carré dans $\mathbb{Q}$.
Ga5 : Si T est irréductible sur $\mathbb{Q}$, Gal(T) agit transitivement sur les n racines (elles sont distinctes) de T, c'est-à-dire $\forall\, z_i$ et z_j deux racines de T il existe $\sigma \in$Gal(T) tel que $\sigma(z_i) = z_j$, donc Gal(T) est isomorphe à un sous-groupe transitif de S_n (un sous-groupe U de S_n est transitif signifie que $\forall i \in \{1;2;\ldots;n\}, \forall j \in \{1;2;\ldots;n\}$ il existe $s \in U$ tel que $s(i) = j$).

étape 1 : le corps de décomposition de P est $N = \mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(a_2, a_3)$.

preuve : toute racine x_i de P est une demi-somme algébrique des a_j, donc $\mathbb{Q}(x_1, x_2, x_3, x_4) \subset \mathbb{Q}(a_1, a_2, a_3)$ et tout a_j est une somme de deux racines de P, donc $\mathbb{Q}(a_1, a_2, a_3) \subset \mathbb{Q}(x_1, x_2, x_3, x_4)$ et $\mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(a_1, a_2, a_3)$.
Mais $\mathbb{Q}(a_1, a_2, a_3) = \mathbb{Q}(a_2, a_3)$: si $q = 0$, parceque $a_1 = 0$ et si $q \neq 0$, parceque $a_1 = \frac{q}{a_2 a_3}$.

Par exemple si $P(X) = X^4 - 3$, ses racines sont $\pm\theta$ et $\pm i\theta$ avec $\theta = \sqrt{\sqrt{3}}$, donc $N = \mathbb{Q}(\theta, i\theta) = \mathbb{Q}(i, \theta)$; mais en utilisant $R(X) = X(X^2 + 12)$, on a $y_1 = 0, y_2 = 2i\sqrt{3}, y_3 = -2i\sqrt{3}$ et on peut prendre $a_2 = (1 + i)\theta, a_3 = (1 - i)\theta$, donc $i = \frac{a_2}{a_3}$, $\theta = \frac{a_2 - a_3}{2}$ et on retrouve $N = \mathbb{Q}(a_2, a_3) = \mathbb{Q}(i, \theta)$.

étape 2 :
Gal(P) est isomorphe ($\simeq$) à un des sous-groupes suivants de S_4 : $S_4, A_4, D_4, V_4 (\subset A_4), \mathbb{Z}/4\mathbb{Z}$
Si Gal(P) est d'ordre 4, $\Delta > 0$.

preuve : x_i étant une racine quelconque de P, $[N : \mathbb{Q}] = [N : \mathbb{Q}(x_i)][\mathbb{Q}(x_i) : \mathbb{Q}]$ (voir [1] pour multiplication des degrés), mais P étant irréductible sur $\mathbb{Q}$, $[\mathbb{Q}(x_i) : \mathbb{Q}] = 4$ et ainsi Gal(P) a pour ordre un multiple de 4, et P ayant quatre racines distinctes, d'après Ga2 de l'étape 0, Gal(P) est isomorphe à un sous-groupe de S_4 ; comme, à isomorphisme près, les seuls sous-groupes de S_4 d'ordre un multiple de 4 sont (voir [4]) $S_4, A_4, D_4, V_4, Z/4Z$, Gal(P) est isomorphe à un de ces cinq sous-groupes.
D'après Ga5 de l'étape 0, P étant irréductible sur $\mathbb{Q}$, Gal(P) agit transitivement sur les racines de P, donc, Gal(P) est isomorphe à un sous-groupe transitif de S_4 : $S_4, A_4, D_4, Z/4Z$ le sont.
En fait, tout sous-groupe de S_4 isomorphe à $\mathbb{Z}/4\mathbb{Z}$, donc cyclique d'ordre 4 (il y en a trois) est transitif, et donc tout sous-groupe de S_4 isomorphe à D_4 (il y en a trois) est aussi

transitif car un tel sous-groupe contient un sous-groupe cyclique d'ordre 4.
Par contre tout sous-groupe de S_4 isomorphe à V_4 (il y en a quatre) n'est pas transitif : seul $\{id;(12)(34);(13)(24);(14)(23)\}$ est transitif et il est dans A_4, les trois de la forme $\{id;(ab);(cd);(ab)(cd)\}$ ne le sont pas (aucun élément de ce groupe échange a et c).

Si l'ordre de Gal(P) est 4 alors $[N:\mathbb{Q}(x_i)]=1$, donc $N=\mathbb{Q}(x_i)$:

soit il existe une racine x_i de P qui est réelle et alors $N\subset\mathbb{R}$ et toutes ses racines sont réélles et $\Delta>0$

soit P n'a aucune racine réelle et ses racines sont conjuguées 2 à 2, (par exemple $x_2=\overline{x_1}, x_4=\overline{x_3}$) et à partir de $\Delta=\prod_{i<j}(x_i-x_j)^2$, on trouve $\Delta>0$.

étape 3 :
si R est irréductible alors, soit Δ est un carré et Gal(P) $\simeq A_4$, soit Δ n'est pas un carré et Gal(P) $\simeq S_4$

preuve : l'ordre de Gal(P) est $[N:\mathbb{Q}]=[\mathbb{Q}(a_2)(a_3):\mathbb{Q}(a_2)][\mathbb{Q}(a_2):\mathbb{Q}]$; or $[\mathbb{Q}(a_2):\mathbb{Q}]=[\mathbb{Q}(a_2):\mathbb{Q}(a_2^2)][\mathbb{Q}(a_2^2):\mathbb{Q}]$, et comme R est irréductible, $[\mathbb{Q}(a_2^2):\mathbb{Q}]=3$ et ainsi l'ordre de Gal(P) est un multiple de 3 ; comme cet ordre est aussi un multiple de 4 (étape 2), c'est un multiple de 12.
Donc Gal(P) est isomorphe à S_4 ou A_4 et Ga4 de l'étape 0 permet de conclure.

étape 4 :
si R est le produit de trois facteurs du 1er degré dans $\mathbb{Q}[X]$, alors $\Delta>0$ et Gal(P) $\simeq V_4\subset A_4$

preuve : R a donc trois racines rationnelles $y_i=a_i^2$ (donc $\Delta>0$) ainsi pour tout $\sigma\in$Gal(P), $\sigma(a_i^2)=a_i^2$ et $\sigma(a_i)=\pm a_i$.
N étant $\mathbb{Q}(a_2,a_3)$, un élément σ de Gal(P) est caractérisé par $\sigma(a_2)$ et $\sigma(a_3)$, ce qui donne au plus quatre possibilités pour σ : l'identité et trois qui sont d'ordre 2. Donc Gal(P) est d'ordre ≤ 4 ; mais d'après l'étape 2, Gal(P) est d'ordre ≥ 4, donc il est ici d'ordre 4 et comme toutes les possiblités $\sigma\neq id_N$ ci-dessus sont d'ordre 2, Gal(P) est isomorphe à un groupe de Klein, celui $\subset A_4$ (voir étape 2).

étape 5 si $R(X)=(X-y_1)R_2(X)$ avec $y_1\in\mathbb{Q}$ et $R_2\in\mathbb{Q}[X]$ irréductible ($\Leftrightarrow$ R a une et une seule racine rationnelle$\Leftrightarrow$ R réductible sur $\mathbb{Q}[X]$ et $\Delta\neq$ carré) alors en notant δ le discriminant de R_2, on a
si $q=0$, Gal(P) $\simeq\mathbb{Z}/4\mathbb{Z}$ si $r(p^2-4r)$ est un carré dans $\mathbb{Q}$, sinon Gal(P) $\simeq D_4$
si $q\neq 0$, Gal(P) $\simeq\mathbb{Z}/4\mathbb{Z}$ si $y_1\delta$ ou $y_1\Delta$ est un carré dans $\mathbb{Q}$, sinon Gal(P) $\simeq D_4$.

étape 5.1 : $\Delta=\mu^2\delta$ avec $\mu\in\mathbb{Q}^*$, $\delta=(y_2-y_3)^2$ et Δ et δ ne sont pas des carrés dans $\mathbb{Q}$; si $q\neq 0$, y_1 n'est pas un carré dans $\mathbb{Q}$ et $y_1\delta=2py_1^2+(3p^2+4r)y_1-3q^2$.

preuve : en posant $R_2(y_1)=\mu\in\mathbb{Q}^*$ ($y_1\in\mathbb{Q}, R_2\in\mathbb{Q}[X]$ est irréductible), on a alors $\Delta=((y_1-y_2)(y_1-y_3)(y_2-y_3))^2=\mu^2(y_2-y_3)^2$.
Mais le discriminant de $R_2(X)=X^2-(y_2+y_3)X+y_2y_3$ est $\delta=(y_2+y_3)^2-4y_2y_3=(y_2-y_3)^2$, qui n'est pas un carré dans $\mathbb{Q}$ (car R_2 est irréductible sur $\mathbb{Q}$), ce qui prouve que Δ aussi n'est pas un carré dans $\mathbb{Q}$.
Notons que si R est réductible sur $\mathbb{Q}[X]$ avec $\Delta\neq$ carré, R ne peut avoir trois racines rationnelles (sinon Δ serait un carré) et alors R s'écrit bien $R(X)=(X-y_1)R_2(X)$ avec R_2 irréductible.

Pour $q\neq 0$, $y_1\delta=y_1((-y_1-2p)^2-\frac{4q^2}{y_1})=2py_1^2+(3p^2+4r)y_1-3q^2$, puisque $R(y_1)=0$;
en fait l'égalité est vraie même si $q=0$ car alors $y_1=0$.
Enfin, P étant irréductible, si $q\neq 0$, d'après le critère d'irréductibilité donné au 2), y_1 n'est

pas un carré dans $\mathbb{Q}$.

étape 5.2 : Gal(P) est isomorphe à D_4 ou $\mathbb{Z}/4\mathbb{Z}$.

preuve : P étant irréductible et Δ n'étant pas un carré, d'après Ga4 de l'étape 0, Gal(P) n'est pas isomorphe à un sous-groupe de A_4, donc Gal(P) ne peut être isomorphe ni à A_4, ni à $V_4 \subset A_4$ (voir étape 2)).
Montrons que Gal(P) n'est pas isomorphe à S_4 : sinon il existe un élément σ de Gal(P) permutant les racines x_2 et x_3 de P , et conservant les deux autres ; or
$y_1 = -(x_1 + x_2)(x_3 + x_4)$ (voir une remarque du 2)), donc
$\sigma(y_1) = -(x_1 + x_3)(x_2 + x_4) = a_2^2 = y_2$ et comme $\sigma(y_1) = y_1$ (car $y_1 \in \mathbb{Q}$)
on arrive à $y_1 = y_2$, ce qui est une contradiction.

étape 5.3 : Détermination de Gal(P) selon que $\lambda = a_2 a_3(a_2^2 - a_3^2)$ est un carré ou pas.

preuve : le corps de décomposition de P étant $N = \mathbb{Q}(a_2, a_3)$ un élément σ de Gal(P) est caractérisé par $\sigma(a_2)$ et $\sigma(a_3)$.
Soit $\sigma \in$Gal(P).
σ étant un $\mathbb{Q}$ –automorphisme de N, et R étant dans $\mathbb{Q}[X]$ avec ses racines $a_i^2 \in N$, σ permute les racines de R. Comme $\sigma(a_1^2) = a_1^2$ (car $a_1^2 = y_1 \in \mathbb{Q}$) on a alors $\{\sigma(a_2^2); \sigma(a_3^2)\} = \{a_2^2; a_3^2\}$, donc $(\sigma(a_2), \sigma(a_3)) = (\pm a_2, \pm a_3)$ ou $(\pm a_3, \pm a_2)$.
$\sigma(a_2)$ étant choisi (quatre choix), il n'y a plus que deux choix pour $\sigma(a_3)$ et donc il y a au plus huit possibilités pour le couple $(\sigma(a_2), \sigma(a_3))$, donc au plus huit possibilités pour σ.
Rappelons que pour chacune de ces huit possibilités $\sigma(a_1)$ est défini : si $q = 0$, $\sigma(a_1) = \sigma(0) = 0$ (puisque $y_1 = a_1^2$ est la seule racine rationnelle de R qui est 0), si $q \neq 0$, $\sigma(a_1) = \dfrac{q}{\sigma(a_2)\sigma(a_3)} (= \pm a_1)$.
Voici sous forme de tableau les huit possibilités pour un élément σ de Gal(P), caractérisées chacune par l'image de a_2 et l'image de a_3 :

σ	$\sigma(a_1)$	$\sigma(a_2)$	$\sigma(a_3)$	ordre	permutation induite sur les x_i
σ_1	a_1	a_2	a_3	1 ($\sigma_1 = id_N$)	id
σ_2	a_1	$-a_2$	$-a_3$	2	$(x_1\ x_2)(x_3\ x_4)$
σ_3	$-a_1$	a_3	$-a_2$	4	$(x_1\ x_4\ x_2\ x_3)$
σ_4	$-a_1$	$-a_3$	a_2	4	$(x_1\ x_3\ x_2\ x_4)$
σ_5	a_1	a_3	a_2	2	$(x_3\ x_4)$
σ_6	a_1	$-a_3$	$-a_2$	2	$(x_1\ x_2)$
σ_7	$-a_1$	a_2	$-a_3$	2	$(x_1\ x_3)(x_2\ x_4)$
σ_8	$-a_1$	$-a_2$	a_3	2	$(x_1\ x_4)(x_2\ x_3)$

Note : si $q = 0$ alors $a_1 = 0$; pour les permutations induites sur les racines de P, se reporter au 2) où sont données les racines x_i de P en fonction des a_j : la colonne $\sigma(a_1)$ a été mise justement pour permettre de déterminer facilement ces permutations.
Les ordres s'obtiennent immédiatement par examen de ces permutations induites, lesquelles caractérisent aussi les σ_i ; par exemple $(x_1\ x_4\ x_2\ x_3)^2 = (x_1\ x_2)(x_3\ x_4)$ et $\sigma_3^2 = \sigma_2$.

Reste à faire le choix entre $\mathbb{Z}/4\mathbb{Z}$ et D_4.
Considérons $\lambda = a_2 a_3(a_2^2 - a_3^2)$: λ est évidemment dans N et est non nul (car R a ses

racines distinctes, donc $a_2^2 - a_3^2 \neq 0$, et y_1 est la seule racine rationnelle, donc les autres ne sont pas nulles et $a_2 a_3 \neq 0$).

Remarquons que $a_2^2 - a_3^2 = y_2 - y_3 \notin \mathbb{Q}$ (d'après l'étape 5.1, δ n'étant pas un carré dans $\mathbb{Q}$), de même $a_2 a_3 \notin \mathbb{Q}$ car si $q \neq 0$, $a_2 a_3 = \frac{q}{a_1}$ et $y_1 = a_1^2$ n'est pas un carré dans $\mathbb{Q}$ (étape 5.1)) et si $q = 0$, $(a_2 a_3)^2 = y_2 y_3 = p^2 - 4r$ qui n'est pas un carré car P est irréductible.

Cependant leur produit peut être dans $\mathbb{Q}$, cas de l'exemple $X^4 + 5X + 5$ ($R(X) = (X-5)(X^2+5X+5), a_2^2 a_3^2 = 5, a_2^2 - a_3^2 = \pm\sqrt{5}$) ou ne pas être dans $\mathbb{Q}$, cas de l'exemple de l'introduction.

Etant donné les valeurs des couples $(\sigma_i(a_2), \sigma_i(a_3))$, on voit tout de suite que $\sigma_i(\lambda) = \pm\lambda$.

Il est facile de vérifier que $\sigma_i(\lambda) = \lambda$ pour $i \in \{1;2;3;4\}$ et $\sigma_i(\lambda) = -\lambda$ pour $i \in \{5;6;7;8\}$.

D'où

si $\lambda \in \mathbb{Q}$, $\forall \sigma \in$Gal(P) on doit avoir $\sigma(\lambda) = \lambda$, donc Gal($P$) ne peut contenir que $\sigma_1, \sigma_2, \sigma_3, \sigma_4$, donc il est d'ordre ≤ 4 et comme (étape 5.2) Gal(P) $\simeq D_4$ ou $\mathbb{Z}/4Z$, c'est que Gal(P) est d'ordre 4 et Gal(P) $= \{\sigma_1;\sigma_2;\sigma_3;\sigma_4\}$ qui doit être isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

Effectivement on peut vérifier que Gal(P) est cyclique : $\sigma_3^2 = \sigma_2, \sigma_3^3 = \sigma_4, \sigma_3^4 = id_N$, σ_4 étant l'autre générateur.

si $\lambda \notin \mathbb{Q}$, Gal($P$) ne peut être cyclique d'ordre 4, car seuls σ_3 et σ_4 étant d'ordre 4, Gal(P) serait encore $\{\sigma_1;\sigma_2;\sigma_3;\sigma_4\}$ et alors λ serait conservé par tous les éléments de Gal(P) et serait dans $\mathbb{Q}$ (d'après Ga3, étape 0), ce qui contredit l'hypothèse ; donc Gal(P) est isomorphe à D_4 donc d'ordre 8 et Gal(P) $= \{\sigma_1;\sigma_2;\sigma_3;\sigma_4;\sigma_5;\sigma_6;\sigma_7;\sigma_8\}$ qui doit être isomorphe à D_4.

Effectivement, σ_5 est d'ordre 2, σ_3 est d'ordre 4 et $\sigma_5\sigma_3 = \sigma_7$ est d'ordre 2, donc σ_5 et σ_3 engendrent un groupe diédral d'indice 4.

On termine la démonstration :

si $q = 0$, $\lambda \in \mathbb{Q} \Leftrightarrow r(p^2 - 4r)$ est un carré dans $\mathbb{Q}$,

car le coefficient de X dans R donne $(a_2 a_3)^2 = p^2 - 4r$, le 2) et l'étape 5.1) donnent $\Delta = 16r(p^2-4r)^2$ et $(a_2^2 - a_3^2)^2 = \delta = \frac{\Delta}{\mu^2}$, d'où $\lambda^2 = (p^2-4r)\frac{\Delta}{\mu^2} = r(p^2-4r)\mu'^2$ avec $\mu' \in \mathbb{Q}^*$ puisque $\Delta = 16r(p^2-4r)^2$;

si $q \neq 0$, $\lambda \in \mathbb{Q} \Leftrightarrow y_1\delta$ est un carré dans $\mathbb{Q} \Leftrightarrow y_1\Delta$ est un carré dans $\mathbb{Q}$,

car $a_2 a_3 = \frac{q}{a_1}$ (voir le 2)) et d'après l'étape 5.1) $\lambda^2 = \frac{q^2}{y_1^2} y_1\delta = \frac{q^2}{(y_1\mu)^2} y_1\Delta$. □

Références :

[1] : Jean-Claude Carréga : Théorie des corps.

[2] : Keith Conrad (recherche sur Keith Conrad quartics et choisir Galois groups of cubics and quartic ; le fichier est cubicquartic.pdf)

[3] : Jean-Pierre Escofier : Théorie de Galois (beaucoup d'exercices corrigés).

[4] : Pascal Ortiz : Exercices (corrigés) d'algèbre.

[5] : Daniel Perrin (recherche sur Daniel Perrin Résolution par radicaux ; le fichier est radicaux.pdf).

Annexe 1

Critère d'irréductibilité sur $\mathbb{Q}$ de $P(X) = X^4 + pX^2 + r$.

Si $p^2 - 4r$ est un carré dans $\mathbb{Q}$, $P(X) = (X^2 + \frac{p}{2})^2 - \frac{p^2 - 4r}{4}$ est réductible sur $\mathbb{Q}$
si $r = b^2$ et $2b - p = a^2$ avec $(a,b) \in \mathbb{Q}^2$, alors $P(X) = (X^2 + aX + b)(X^2 - aX + b)$ et P est réductible sur $\mathbb{Q}$.
Réciproquement, si P est réductible sur $\mathbb{Q}$:
soit $P = UV$ avec $d°U = 1$ et P a une racine $e \in \mathbb{Q}$, donc $e^2 \in \mathbb{Q}$ est racine de $X^2 + pX + r$ et $p^2 - 4r$ est un carré dans $\mathbb{Q}$
soit $P = (X^2 + aX + b)(X^2 + a'X + b')$ (car si $P = UV$ avec U, V dans $\mathbb{Q}[X]$ de degrés 2, on peut supposer U et V unitaires en les factorisant par leurs coefficients de tête dont le produit est 1), d'où
$a' = -a,\ a(b' - b) = 0,\ b + b' - p = a^2,\ bb' = r$
soit $a = 0$ et $b + b' = p$, $bb' = r$ d'où b et b' sont racines rationnelles de $X^2 - pX + r$, donc à nouveau, $p^2 - 4r$ est un carré
soit $b = b'$ et $b^2 = r$ et $2b - p = a^2$.
Conclusion : P réductible sur $\mathbb{Q} \Leftrightarrow p^2 - 4r$ est un carré dans $\mathbb{Q}$ ou il existe $(a,b) \in \mathbb{Q}^2$ tel que $r = b^2$ et $2b - p = a^2$.

Annexe 2

Preuve de la simplification du cas 4

en supposant acquis la caractérisation du groupe de Galois en fonction de l'irréductibilité ou non de P sur $Q(\sqrt{\Delta})$.

Ce cas 4 est le cas où P est irréductible sur $\mathbb{Q}$, et la décomposition de R en irréductibles sur $\mathbb{Q}$ est $R(X) = (X - y_1)R_2(X)$, c'est-à-dire R **a une et une seule racine rationnelle** y_1, laquelle, si $q \neq 0$, **n'est pas un carré dans** $\mathbb{Q}$, car P est irréductible sur $\mathbb{Q}$: voir le critère d'irréductibilté d'un degré 4 au 2).

On note y_2, y_3 les racines de R_2 et δ son discriminant.

Δ n'étant pas un carré dans $\mathbb{Q}$ (preuve ci-dessous), $\mathbb{Q}(\sqrt{\Delta}) \neq \mathbb{Q} : \mathbb{Q}(\sqrt{\Delta}) = \{u + v\sqrt{\Delta}\ ; (u,v) \in \mathbb{Q}^2\}$.

La décomposition d'un élément de $\mathbb{Q}(\sqrt{\Delta})$ sous la forme $u + v\sqrt{\Delta}$ avec $(u,v) \in \mathbb{Q}^2$ est unique (preuve immédiate).

$\Delta = \mu^2\delta$ avec $\mu \in \mathbb{Q}^*$, $\delta = (y_2 - y_3)^2$, Δ, δ ne sont pas des carrés dans $\mathbb{Q}$

$y_1 = u + v\sqrt{\Delta}, y_2 = u - v\sqrt{\Delta}$ avec u et v dans $\mathbb{Q}$, $v \neq 0$.

En effet, en posant $R_2(y_1) = \mu \in \mathbb{Q}^*$ ($y_1 \in \mathbb{Q}, R_2 \in \mathbb{Q}[X]$ est irréductible), on a alors $\Delta = ((y_1 - y_2)(y_1 - y_3)(y_2 - y_3))^2 = \mu^2(y_2 - y_3)^2$.

Mais le discriminant de $R_2(X) = X^2 - (y_2 + y_3)X + y_2y_3$ est $\delta = (y_2 + y_3)^2 - 4y_2y_3 = (y_2 - y_3)^2$, qui n'est pas un carré dans $\mathbb{Q}$ (car R_2 est irréductible sur $\mathbb{Q}$), ce qui prouve que Δ aussi n'est pas un carré dans $\mathbb{Q}$.

On a $y_2 - y_3 = v\sqrt{\Delta}$ avec $v = \pm\frac{1}{\mu} \in \mathbb{Q}^*$, $y_2 + y_3 = y_1 - 2p = u \in \mathbb{Q}$ et, par ajout et différence, y_2 et y_3 sont dans $\mathbb{Q}(\sqrt{\Delta})$: $2y_2 = u + v\sqrt{\Delta}$ et $2y_3 = u - v\sqrt{\Delta}$.

Si P est réductible sur $\mathbb{Q}(\sqrt{\Delta})$,

sa décomposition en facteurs irréductibles est $(X^2 + \alpha X + \beta)(X^2 + \alpha' X + \beta')$ avec $\alpha, \beta, \alpha', \beta'$ dans $\mathbb{Q}(\sqrt{\Delta})$.

En effet si P avait une θ racine dans $\mathbb{Q}(\sqrt{\Delta})$, comme $[\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}] = 2$ (car $\sqrt{\Delta}$ est racine de $X^2 - \Delta$ irréductible sur $\mathbb{Q}$) le degré de θ sur $\mathbb{Q}$ serait un diviseur de 2, d'où une contradiction avec le fait que le polynôme minimal de θ sur $\mathbb{Q}$ est P qui est de degré 4.

Si $P(X) = (X^2 + \alpha X + \beta)(X^2 + \alpha' X + \beta')$ alors $\alpha + \alpha' = 0$, $-\alpha^2 + \beta + \beta' = p$, $\alpha(\beta' - \beta) = q$, $\beta\beta' = r$

Immédiat par identification.

Preuve du cas 4) simplifié dans le cas $q = 0$

On a (voir le 2)) $\Delta = 16r(p^2 - 4r)^2$, donc $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{r})$; rappelons que Δ n'étant pas un carré dans $\mathbb{Q}$, r n'est pas un carré.

Si P est réductible sur $\mathbb{Q}(\sqrt{\Delta})$, d'après ci-dessus, on a $P(X) = (X^2 + \alpha X + \beta)((X^2 - \alpha X + \beta')$ avec α, β, β' dans $\mathbb{Q}(\sqrt{\Delta})$ et $-\alpha^2 + \beta + \beta' = p$, $\alpha(\beta' - \beta) = q$, $\beta\beta' = r$.

Deux cas sont à envisager.

soit $\alpha = 0$: donc $P(X) = (X^2 + \beta)(X^2 + \beta')$ avec β, β' dans $\mathbb{Q}(\sqrt{r})$

$\beta = u + v\sqrt{r}$, $\beta' = u' + v'\sqrt{r}$ avec u, v, u', v' rationnels ; P étant irréductible sur $\mathbb{Q}$, v et

v' sont non nuls, car si l'un est nul, β ou β' est rationnel, donc β et β' sont rationnels (car $\beta\beta' = r \neq 0$) et P serait réductible sur $\mathbb{Q}$, ce qui est faux.

De $\beta + \beta' = p$ on tire $u + u' + (v + v')\sqrt{r} = p \in \mathbb{Q}$, donc $u + u' = p$ et $v + v' = 0$,

puis de $\beta\beta' = r$ on tire $uu' - rv^2 + v(u' - u)\sqrt{r} = r$, soit $uu' - rv^2 = r$ et $v(u' - u) = 0$,

d'où $u = u'$, $u^2 - rv^2 = r$, soit $\frac{p^2}{4} - r = rv^2$.

Donc $r(p^2 - 4r) = 4r^2v^2$ est un carré dans $\mathbb{Q}$.

Réciproquement si $r(p^2 - 4r) = \theta^2$ avec $\theta \in \mathbb{Q}$,

prenons $\beta = \frac{p}{2} + \frac{\theta\sqrt{r}}{2r}$ et $\beta' = \frac{p}{2} - \frac{\theta\sqrt{r}}{2r}$ (r est non nul, car $\Delta \neq 0$) :

ils sont bien dans $\mathbb{Q}(\sqrt{r})$ et on vérifie que $(X^2 + \beta)(X^2 + \beta') = P(X)$.

Donc si $\alpha = 0$, P est réductible sur $\mathbb{Q}(\sqrt{\Delta}) \Leftrightarrow r(p^2 - 4r)$ est un carré dans $\mathbb{Q}$.

soit $\beta' = \beta$: donc $P(X) = (X^2 + \alpha X + \beta)(X^2 - \alpha X + \beta)$ avec α, β dans $\mathbb{Q}(\sqrt{r})$

On pose cette fois $\beta = u + v\sqrt{r}$, $\alpha = u' + v'\sqrt{r}$ avec u, v, u', v' dans $\mathbb{Q}$.

De $\beta^2 = r$, on tire $u^2 + rv^2 = r$ et $uv = 0$:

$v = 0$ conduit à r est un carré dans $\mathbb{Q}$, ce qui est exclu : donc $u = 0$ et $v^2 = 1$.

Et de $-\alpha^2 + 2\beta = p$ on tire $2u - u'^2 - v'^2 r = p$ et $2v - 2u'v' = 0$.

D'où $u'^2 + v'^2 r = -p$, $u'^2 v'^2 = v^2 = 1$ et $u'^2 + \frac{r}{u'^2} = -p$, soit $P(u') = 0$.

Donc P a une racine rationnelle ce qui est impossible car il est irréductible sur $\mathbb{Q}$.

Donc si $\beta' = \beta$, P n'est pas réductible sur $\mathbb{Q}(\sqrt{\Delta})$.

Conclusion si $q = 0$:

P **est réductible sur** $\mathbb{Q}(\sqrt{\Delta}) \Leftrightarrow (p^2 - 4r)r$ **est un carré dans** $\mathbb{Q}$.

Dans ce cas on peut noter que la décomposition en facteurs irréductibles dans $\mathbb{Q}(\sqrt{\Delta})$ de $P(X)$ est $(X^2 + \beta)(X^2 + \beta')$.

Preuve du cas 4) simplifié dans le cas $q \neq 0$.

On va montrer que P est réductible sur $\mathbb{Q}(\sqrt{\Delta}) \Leftrightarrow y_1\Delta$ est un carré dans $\mathbb{Q}^* \Leftrightarrow y_1\Delta$ est un carré dans $\mathbb{Q}^*$, cela en établissant que les cinq propositions suivantes sont équivalentes :

(**p1**) : P est réductible sur $\mathbb{Q}(\sqrt{\Delta})$

(**p2**) : une racine de R est un carré dans $\mathbb{Q}(\sqrt{\Delta})$

(**p3**) : y_1 est un carré dans $\mathbb{Q}(\sqrt{\Delta})$

(**p4**) : $y_1\Delta$ est un carré dans $\mathbb{Q}^*$

(**p5**) : $y_1\delta$ est un carré dans $\mathbb{Q}^*$

en effet

p1⇒p2 :

P étant réductible sur $\mathbb{Q}(\sqrt{\Delta})$, $P(X) = (X^2 + \alpha X + \beta)(X^2 + \alpha' X + \beta')$ avec $\alpha, \beta, \alpha', \beta'$ dans $\mathbb{Q}(\sqrt{\Delta})$.

Puisque $\alpha + \alpha' = 0$, on a $\alpha(\beta' - \beta) = q \neq 0$, $\alpha \neq 0$ et $\beta \neq \beta'$.

De $\beta + \beta' = p + \alpha^2$ et $\beta' - \beta = \frac{q}{\alpha}$ on tire $2\beta' = \alpha^2 + p + \frac{q}{\alpha}$ et $2\beta = \alpha^2 + p - \frac{q}{\alpha}$.

Comme $\beta\beta' = r$, on obtient $(\alpha^2 + p)^2 - \frac{q^2}{\alpha^2} = 4r \Leftrightarrow R(\alpha^2) = 0$, c'est-à-dire R a une racine qui est un carré dans $\mathbb{Q}(\sqrt{\Delta})$.

(Evidemment c'est le calcul qui permet d'arriver à la définition de R : voir début du 2)).

p2⇒p1 :

soit $\alpha \in \mathbb{Q}(\sqrt{\Delta})$ avec $R(\alpha^2) = 0$, comme $q \neq 0$, α est non nul et d'après le calcul précédent on a $(\alpha^2 + p)^2 - \frac{q^2}{\alpha^2} = 4r$, soit en posant $2\beta' = \alpha^2 + p + \frac{q}{\alpha}$ et $2\beta = \alpha^2 + p - \frac{q}{\alpha}$, $4\beta\beta' = 4r$ et ainsi $P(X) = (X^2 + \alpha X + \beta)(X^2 - \alpha X + \beta')$ et P est bien réductible sur $\mathbb{Q}(\sqrt{\Delta})$.

p2⇒p3 :

soit y_1 est un carré dans $\mathbb{Q}(\sqrt{\Delta})$,
soit c'est une des deux autres racines de R qui est un carré dans $\mathbb{Q}(\sqrt{\Delta})$; quitte à renuméroter ces deux autres racines, on peut supposer que c'est y_2 qui est un carré dans $\mathbb{Q}(\sqrt{\Delta})$, et comme $y_2 = u + v\sqrt{\Delta}, y_3 = u - v\sqrt{\Delta}$, avec u, v dans $\mathbb{Q}$ et $v \neq 0$, on a alors $y_2 = (s + t\sqrt{\Delta})^2$ avec s, t dans $\mathbb{Q}$, d'où $u = s^2 + t^2\Delta$ et $v = 2st$ ce qui donne $y_3 = (s - t\sqrt{\Delta})^2$, c'est-à-dire que dans ce cas y_2 et y_3 sont des carrés dans $\mathbb{Q}(\sqrt{\Delta})$, or $y_1 y_2 y_3 = q^2$, donc y_1 est aussi un carré dans $\mathbb{Q}(\sqrt{\Delta})$.

p3⇒p2 :

trivial, puisque y_1 est une racine de R.

p3⇒p4 :

on a $y_1 = (s + t\sqrt{\Delta})^2$ avec s, t dans $\mathbb{Q}$, donc puisque $y_1 \in \mathbb{Q}$, $y_1 = s^2 + t^2\Delta$ et $st = 0$, d'où, puisque $t \neq 0$ (car y_1 n'est pas un carré dans $\mathbb{Q}$, voir étape 5.1) de la preuve du 3)), on a $s = 0$, soit $y_1 = t^2\Delta$, et $y_1\Delta$ est un carré dans $\mathbb{Q}^*$ (y_1 et Δ sont dans $\mathbb{Q}^*$).

p4⇒p3 :

puisque $y_1\Delta = \theta^2$ avec θ dans $\mathbb{Q}^*$(car y_1, Δ sont dans $\mathbb{Q}^*$) on a $y_1 = (\frac{\theta}{\Delta}\sqrt{\Delta})^2$ qui est bien un carré dans $\mathbb{Q}(\sqrt{\Delta})$.

p4⇔p5 :

puisque $\Delta = \mu^2\delta$ avec $\mu \in \mathbb{Q}^*$.

Conclusion si $q \neq 0$: **P est réductible sur $\mathbb{Q}(\sqrt{\Delta}) \Leftrightarrow y_1\Delta$ est un carré dans $\mathbb{Q}^* \Leftrightarrow y_1\delta$ est un carré dans $\mathbb{Q}^*$.** □

Annexe 3

Quelques exemples.

Pour prouver l'irréductibilité sur $\mathbb{Q}$ de $P \in \mathbb{Q}[X]$ de degré 4 on pourra appliquer le critère déduit du résolvant R (voir le 2)) ou le critère propre au cas bicarré (voir le 3)).
Cependant, on pourra penser au critère d'Eisenstein (voir [1]) car il peut donner la réponse très rapidement.

Exemple 1 :
$Gal(X^4 - X - 1) = S_4$; $(R(X) = X^3 + 4X - 1$; $\Delta = -283)$.

Exemple 2 :
$Gal(X^4 + 8X + 12) = A_4$; $(R(X) = X^3 - 48X - 64$; $\Delta = 3^4 \times 2^{12})$.

Exemple 3 :
$P(X) = X^4 + \frac{1}{2}X^2 + 2X + \frac{17}{16}$:
$R(X) = X^3 + X^2 - 4X - 4 = (X+1)(X-2)(X+2)$.
Donc $Gal(P) = V_4$…sous réserve que $P(X) = X^4 + \frac{1}{2}X^2 + 2X + \frac{17}{16}$ soit irréductible sur $\mathbb{Q}$.
R n'ayant pas de racine qui soit le carré d'un rationnel, P ne peut être le produit de deux seconds degrés, il reste donc à montrer que P n'a pas de racine rationnelle (voir critère donné au 2)).
Soient a et $b > 0$ deux entiers premiers entre eux :
$P(\frac{a}{b}) = 0 \Leftrightarrow 16a^4 + 8a^2b^2 + 32ab^3 + 17b^4 = 0$, donc $a < 0$, a divise 17, b^2 divise 16, et nécessairement $a = -1$ ou -17 et $b = 2$ ou 4. On vérifie alors qu'aucune de ces quatre possibilités pour $\frac{a}{b}$ n'est racine de P ce qui prouve que P est bien irréductible sur $\mathbb{Q}$.
Remarque : pour fabriquer de tels exemples, on peut commencer par choisir p, q, r tels que R ait deux racines rationnelles dont aucune est un carré.
Par exemple on cherche p, q, r tels que $R(-1) = R(2) = 0$, ce qui donne $4r = 3 + 2p + p^2, q^2 = 2 + 4p$; la troisième racine (forcément rationnelle) de R est alors $-\frac{q^2}{2}$ qui n'est jamais un carré dans $\mathbb{Q}$ (pour $q \neq 0$).
Il reste à trouver q de telle sorte que le P obtenu soit sans racine rationnelle : par exemple $q = 2$ donne $p = \frac{1}{2}$ et $r = \frac{17}{16}$.

Exemple 4 :
$P(X) = X^4 + 5X + 5$: il est irréductible sur $\mathbb{Q}$ (Eisenstein, voir [1]) et
$R(X) = X^3 - 20X - 25 = (X-5)(X^2 + 5X + 5)$, donc on est dans le cas 4).
La seule racine rationnelle de R est $y_1 = 5$ (qui n'est pas effectivement un carré) ; comme le discriminant de $X^2 + 5X + 5$ est $\delta = 5$, $y_1\delta = 5^2$ est le carré d'un rationnel, donc le groupe de Galois de P est $\mathbb{Z}/4\mathbb{Z}$; on n'a pas eu besoin de calculer $\Delta = -27q^4 + 256r^3 = 5 \times 55^2$

Exemple 5 :
$P(X) = X^4 + 3X + 3$: il est irréductible (Eisenstein) et
$R(X) = X^3 - 12X - 9 = (X+3)(X^2 - 3X - 3)$, donc on est dans le cas 4).

La seule racine rationnelle de R est $y_1 = -3$ (qui n'est pas effectivement un carré) ; comme le discriminant de $X^2 - 3X - 3$ est $\delta = 21$, $y_1\delta = -63$ n'est pas le carré d'un rationnel, donc le groupe de Galois de P est D_4 ; là aussi il est inutile de calculer Δ ($= 21 \times 15^2$).

Exemple 6 :

$P(X) = X^4 + 3X^2 - 2X + 2$.

Pour l'irréductibilité de P, le critère donné au 2) nécessite le calcul de $R(X) = X^3 + 6X^2 + X - 4 = (X + 1)(X^2 + 5X - 4)$ (décomposition en irréductibles sur $\mathbb{Q}$) : R n'a pas de racine qui soit le carré d'un rationnel et comme P n'a pas de racine rationnelle ($\frac{a}{b}$ racine de R avec a et $b > 0$ entiers premiers entre eux implique a divise 2 et $b = 1$ donc $\frac{a}{b} = \pm 2$, et aucune de ces possibilités est racine de R), P est irréductible sur $\mathbb{Q}$.

Et puisque $y_1\delta = -1 \times (25 + 16)$ n'est pas un carré dans $\mathbb{Q}$, le groupe de Galois de P est D_4.

Remarque ... pour les curieux :

la méthode de Descartes pour factoriser P donne, en prenant $a = i$,

$P(X) = (X^2 + iX + 1 - i)(X^2 - iX + 1 + i)$.

Pour en déduire les racines, on remarquera que les racines carrées de $-5 + 4i$ sont $\pm\left(\sqrt{\frac{-5 + \sqrt{41}}{2}} + i\sqrt{\frac{5 + \sqrt{41}}{2}}\right)$.

Annexe 4

Détermination explicite du groupe de GALOIS DE X^4-3.

D'après le tableau du 2) sur la classification des groupes de Galois d'un polynôme bicarré, on a vu que X^4-3 a pour groupe de Galois D_4.

On va retrouver ce résultat en partant de la définition d'un groupe de Galois .... et sans passer par les racines du résolvant de Descartes comme dans la preuve du 3).

Le groupe de Galois d'un polynôme $P \in \mathbb{Q}[X]$ est par définition le groupe G des $\mathbb{Q}$ –automorphismes de son corps N de décomposition, lequel est la plus petite extension de $\mathbb{Q}$ contenant toutes les racines (dans $\mathbb{C}$) de P.

On admettra que l'ordre du groupe G est le degré de l'extension $\mathbb{Q} \subset N$, soit $[N:\mathbb{Q}]$ (ce sera le seul résultat sur Galois à admettre ici).

Pour $P(X)=X^4-3$, ses racines sont $\pm\theta$ et $\pm i\theta$ avec $\theta=\sqrt{\sqrt{3}}$; donc son corps de décomposition est $N=\mathbb{Q}(i,\theta)$, plus petit corps contenant $\mathbb{Q}$, i et θ.

La multiplication des degrés donne $[\mathbb{Q}(i,\theta):\mathbb{Q}]=[Q(\theta)(i):\mathbb{Q}(\theta)][\mathbb{Q}(\theta):\mathbb{Q}]$.

$X^2+1 \in Q(\theta)[X]$ et X^2+1 est irréductible sur $\mathbb{Q}(\theta) \subset \mathbb{R}$, donc $[Q(\theta)(i):\mathbb{Q}(\theta)]=2$, et P étant irréductible sur $\mathbb{Q}$, $[\mathbb{Q}(\theta):\mathbb{Q}]=4$, ainsi G est un groupe d'ordre 8.

Mais il y a cinq sortes de groupes d'ordre 8 : $\mathbb{Z}/8Z$, $\mathbb{Z}/4Z\times\mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, D_4, H_8 (groupe des quaternions) : pour savoir lequel est G, on va commencer par expliciter les huit éléments de G.

Un élément σ de G étant un $\mathbb{Q}$ –automorphisme de N, si $x \in N$ alors $P(x) \in N$ et $\sigma(P(x))=P(\sigma(x))$; d'où si e est une racine de P, alors $0=\sigma(0)=\sigma(P(e))=P(\sigma(e))$ et $\sigma(e)$ est une racine de P.

Un élément σ de G est caractérisé par $\sigma(i)$ et $\sigma(\theta)$:

comme i est racine de X^2+1, $\sigma(i)$ aussi, donc $\sigma(i)=\pm i$

comme θ est racine de P, $\sigma(\theta)$ aussi et $\sigma(\theta) \in \{\theta,-\theta,i\theta,-i\theta\}$,

ce qui donne au plus 8 possibilités pour σ.

G étant d'ordre 8, ses 8 éléments σ_i, pour $i=1,2,\ldots,8$ sont exactement ceux correspondants aux 8 possibilités ci-dessus :

σ_1	$\sigma_1(i)=i$ $\sigma_1(\theta)=\theta$	$\sigma_1=id_N$	σ_5	$\sigma_5(i)=-i$ $\sigma_5(\theta)=\theta$	$\sigma_5^2=id_N$
σ_2	$\sigma_2(i)=i$ $\sigma_1(\theta)=-\theta$	$\sigma_2^2=\sigma_2\circ\sigma_2=id_N$	σ_6	$\sigma_6(i)=-i$ $\sigma_6(\theta)=-\theta$	$\sigma_6^2=id_N$
σ_3	$\sigma_3(i)=i$ $\sigma_3(\theta)=i\theta$	$\sigma_3^2=\sigma_2,\sigma_3^3=\sigma_4,\sigma_3^4=id_N$	σ_7	$\sigma_7(i)=-i$ $\sigma_7(\theta)=i\theta$	$\sigma_7^2=id_N$
σ_4	$\sigma_4(i)=i$ $\sigma_4(\theta)=-i\theta$	$\sigma_4^2=\sigma_2,\sigma_4^3=\sigma_3,\sigma_4^4=id_N$	σ_8	$\sigma_8(i)=-i$ $\sigma_8(\theta)=-i\theta$	$\sigma_8^2=id_N$

Par exemple $\sigma_4^2(\theta)=\sigma_4(-i\theta)=-\sigma_4(i)\sigma_4(\theta)=-i\times(-i\theta)=-\theta=\sigma_2(\theta)$, et comme $\sigma_4^2(i)=i=\sigma_2(i)$, c'est que $\sigma_4^2=\sigma_2$

On constate que G a cinq éléments d'ordre 2 et deux d'ordre 4, ce qui peut faire penser au groupe D_4 lequel posséde justemment $4+1=5$ éléments d'ordre 2.

σ_3 est d'ordre 4, σ_5 d'ordre 2 et $\sigma_3\sigma_5=\sigma_7$ (vérification laissée au lecteur) est d'ordre 2, donc par définition même d'un groupe diédral, G est le groupe diédral D_4 engendré par σ_3 et σ_5.

On peut vérifier (résultat général sur groupe diédral) que
$G=\{id_{\mathbb{Q}};\sigma_3;\sigma_3^2;\sigma_3^3;\sigma_5;\sigma_5\sigma_3;\sigma_5\sigma_3^2;\sigma_5\sigma_3^3\}$, cela parce que $\sigma_5\sigma_3=\sigma_8$, $\sigma_5\sigma_3^2=\sigma_6$, $\sigma_5\sigma_3^3=\sigma_7$ et évidemment G n'est pas commutatif car par exemple $\sigma_5\sigma_3\neq\sigma_3\sigma_5$.