Extensions quadratiques itérées et calculatrices

Daniel PERRIN

1 Introduction

1.1 Les machines sont bêtes ?

Les calculatrices (par exemple la TI Voyage 200) ou les logiciels (par exemple *xcas*) qui font du calcul formel renvoient en général sans hésiter des formules du genre $\sqrt{9+4\sqrt{5}} = 2+\sqrt{5}$ lorsque la racine d'une quantité de $\mathbf{Q}(\sqrt{d})$ est encore dans ce corps. En revanche, avec l'expression $\sqrt{2+\sqrt{3}}$, la TI Voyage 200 répond sans hésitation : $\dfrac{\sqrt{2}+\sqrt{6}}{2}$ mais on a toutes les peines du monde à obtenir ce même résultat avec *xcas* ou d'autres logiciels de calcul formel. Ce texte a pour but de répondre à la suivante : quand la racine d'une expression quadratique (i.e. de $\mathbf{Q}(\sqrt{d})$, $d \in \mathbf{Q}$) est-elle dans ce corps, voire dans une extension biquadratique $\mathbf{Q}(\sqrt{d},\sqrt{e})$ avec $e \in \mathbf{Q}$?

1.2 Données et notations

On considère un entier [1] $d > 1$, sans facteur carré, et l'extension $K = \mathbf{Q}(\sqrt{d})$. On choisit $x = A+B\sqrt{d} \in K$, avec $B \neq 0$, et on considère sa racine [2] $y = \sqrt{x}$ et le corps $L := K(y) = \mathbf{Q}(y)$. Les questions initiales reviennent à préciser ce corps :

• Quand y est-il dans K (c'est le cas lorsque l'on a $x = 9+4\sqrt{5}$) ?

• Si y n'est pas dans K, l'extension L est de degré 4 sur $\mathbf{Q}$, quand est-elle de la forme $\mathbf{Q}(\sqrt{d},\sqrt{e})$, avec $e \in \mathbf{Q}$ (comme dans le cas de l'exemple initial) ? Il s'agit donc de savoir si l'extension L de degré 4 contient d'autres extensions de degré 2 que $\mathbf{Q}(\sqrt{d})$. On sait que ce genre de choses se comprend mieux en termes de théorie de Galois [3], ce qui mène à la question suivante :

1. On pourrait aussi bien prendre pour d un rationnel, $d = p/q$ mais on se ramène au cas entier en considérant $d' = q^2 d = pq$ car les extensions quadratiques associées à d et d' sont les mêmes.

2. Une de ses racines, l'autre étant $-y$.

3. On utilisera librement des résultats (faciles) de théorie de Galois. On renvoie à [DP] pour les notions de base sur les corps et à [ST] pour la théorie de Galois proprement dite.

• L'extension $L/\mathbf{Q}$ est-elle galoisienne ? Sinon, quelle est sa clôture normale M ? Quel est le groupe de Galois de l'extension $M/\mathbf{Q}$?

1.3 L'équation de y sur $\mathbf{Q}$

Pour déterminer la clôture normale de L sur $\mathbf{Q}$ il suffit de trouver le polynôme minimal de y sur $\mathbf{Q}$. Pour cela, on commence par calculer une équation de y sur $\mathbf{Q}$. On écrit $y^2 - A = B\sqrt{d}$, d'où $y^4 - 2Ay^2 + A^2 - dB^2 = 0$. On pose $p = 2A$ et $r = A^2 - dB^2$. On a une équation bicarrée $P(y) := y^4 - py^2 + r = 0$ de discriminant $\Delta = 4B^2d$.

1.1 *Remarques.* 1) Si on note $\overline{x}$ le conjugué de x, $\overline{x} = A - B\sqrt{d}$, les coefficients p et r sont respectivement la trace de x, $p = x + \overline{x}$ et sa norme $r = x\,\overline{x}$.

2) Comme les racines de $X^2 - pX + r = 0$ sont x et $\overline{x}$, les quatre racines de P sont $y, -y$ et $z, -z$ où z est une racine de $\overline{x} = A - B\sqrt{d}$.

3) Si P est irréductible, la clôture normale de L sur $\mathbf{Q}$ est le corps de décomposition $M = D_{\mathbf{Q}}(P) = \mathbf{Q}(y, z)$.

4) Inversement, toute équation bicarrée de la forme $y^4 - py^2 + r = 0$ a des solutions du type précédent. En effet, le discriminant est $\Delta = p^2 - 4r$ et les racines sont de la forme $\pm\sqrt{\dfrac{p \pm \sqrt{\Delta}}{2}}$.

2 Le cas réductible

2.1 Les conditions

On traite d'abord le cas général d'un polynôme bicarré général :

2.1 Lemme. *Soient $p, q \in \mathbf{Q}$. Le polynôme $P(X) = X^4 - pX^2 + r$ est réductible sur $\mathbf{Q}$ dans les deux cas suivants :*

- *$\Delta = p^2 - 4r$ est un carré de $\mathbf{Q}$,*
- *r est un carré de $\mathbf{Q}$, $r = C^2$, et $p + 2C$ ou $p - 2C$ est un carré de $\mathbf{Q}$.*

Démonstration. 1) Supposons d'abord P réductible. Si P a une racine rationnelle y, on a $(y^2 - \frac{p}{2})^2 = \frac{1}{4}(p^2 - 4r)$, ce qui montre que $p^2 - 4r$ est un carré de $\mathbf{Q}$.

Si P est produit de deux polynômes de degré 2, on écrit :

$$X^4 - pX^2 + r = (X^2 + \alpha X + \beta)(X^2 + \gamma X + \delta)$$

avec $\alpha, \beta, \gamma, \delta \in \mathbf{Q}$. On a aussitôt $\gamma = -\alpha$ et $\alpha(\beta - \delta) = 0$. Le cas $\alpha = 0$ conduit à $\beta + \delta = -p$ et $\beta\delta = r$, ce qui impose que $p^2 - 4r$ est le carré de

$\beta - \delta$. Le cas $\beta = \delta$ donne $r = \beta^2$ et $\alpha^2 = p + 2\beta$, d'où le résultat avec $\beta = \pm C$.

Réciproquement, si on a $p^2 - 4r = \delta^2$ on a $P(X) = (X^2 - \frac{p}{2} + \frac{\delta}{2})(X^2 - \frac{p}{2} - \frac{\delta}{2})$ tandis que si l'on a $r = C^2$ et $p + 2\epsilon C = E^2$ avec $\epsilon = \pm 1$, on a $P(X) = (X^2 + EX + \epsilon C)(X^2 - EX + \epsilon C)$.

Dans le cas qui nous intéresse, on obtient :

2.2 Théorème. *Soient d un entier sans facteur carré, $A, B \in \mathbf{Q}$ avec $B \neq 0$, $p = 2A$, $r = A^2 - dB^2$.*

1) Le polynôme $P(X) = X^4 - pX^2 + r$ est réductible si et seulement si il existe $C, E \in \mathbf{Q}$ et $\epsilon = \pm 1$ tels que l'on ait $r = A^2 - dB^2 = C^2$ et $2(A + \epsilon C) = E^2$. Dans ce cas, les racines de P sont dans $\mathbf{Q}(\sqrt{d})$, ce sont $y = \frac{E}{2} + \frac{B}{E}\sqrt{d}$, $z = \frac{E}{2} - \frac{B}{E}\sqrt{d}$, $-y$ et $-z$. Les nombres y et $-y$ (resp. z et $-z$) sont les racines carrées de $x = A + B\sqrt{d}$ (resp. $\overline{x} = A - B\sqrt{d}$).

2) Inversement, si x ou $\overline{x}$ a une racine carrée dans $K = \mathbf{Q}(\sqrt{d})$, toutes les racines de x et $\overline{x}$ sont dans K et on a les conditions précédentes.

Démonstration. 1) Il est clair que le premier cas de 2.1 ne peut se produire [4] ici car $p^2 - 4r = 4dB^2$ n'est jamais un carré. On a donc $r = A^2 - dB^2 = C^2$ et $p + 2\epsilon C = 2A + 2\epsilon C = E^2$ avec $\epsilon = \pm 1$ et on a vu que l'équation qui donne y est :

$$y^4 - py^2 + r = (y^2 + Ey + \epsilon C)(y^2 - Ey + \epsilon C) = 0.$$

Les deux facteurs ont même discriminant :

$$E^2 - 4\epsilon C = 2(A - \epsilon C) = 2\frac{A^2 - C^2}{A + \epsilon C} = \frac{4dB^2}{E^2}$$

et les racines de l'équation sont $\eta\frac{E}{2} + \zeta\frac{B}{E}\sqrt{d}$ avec $\eta = \pm 1$ et $\zeta = \pm 1$. Le carré de cette quantité est $A + \eta\zeta B\sqrt{d}$: les racines avec $\zeta = \eta = 1$ et $\zeta = \eta = -1$ sont les racines carrées de $x = A + B\sqrt{d}$ et les autres sont les racines de $\overline{x} = A - B\sqrt{d}$.

2) Si $x = A + B\sqrt{d}$ est le carré de $y = a + b\sqrt{d}$ avec $a, b \in \mathbf{Q}$, on a $a^2 + db^2 = A$ et $2ab = B$ et on vérifie que $r = A^2 - dB^2$ est le carré de $C = a^2 - db^2$ et $2(A + C)$ le carré de $E = 2A$.

2.2 Construire des exemples

Pour construire des exemples de nombres $A + B\sqrt{d}$ dont les racines sont encore de cette forme, il y a un moyen bien simple : on part de la racine et

4. Comme x et $\overline{x}$ sont les racines de $X^2 - pX + r$, de discriminant $p^2 - 4r$, ce nombre est un carré si et seulement si x et $\overline{x}$ sont dans $\mathbf{Q}$, donc aussi $\sqrt{d}$, et ce cas a été écarté.

on l'élève au carré ! Par exemple, on part de $2+\sqrt{5}$ et son carré $9+4\sqrt{5}$ est un exemple comme souhaité.

2.3 *Exemples.* Le lecteur vérifiera que les nombres suivants sont des carrés dans $\mathbf{Q}(\sqrt{d})$: $349+156\sqrt{5}$, $1+\frac{4}{9}\sqrt{5}$, $\dfrac{1526873}{76176}-\dfrac{91\sqrt{17}}{138}$. Il vérifiera aussi que la calculatrice et l'ordinateur lui donnent le résultat sans faire de manières [5].

3 Le cas irréductible

3.1 La tour d'extensions quadratiques

On suppose désormais que $P = X^4 - pX + r$ est irréductible sur $\mathbf{Q}$. La racine y est alors de degré 4 sur $\mathbf{Q}$, donc n'est pas dans $K = \mathbf{Q}(\sqrt{d})$. On cherche cependant encore à écrire $x = A+B\sqrt{d}$ comme le carré de $y = a+b\sqrt{d}$ mais plus nécessairement avec a, b rationnels. Précisément, on cherche une extension N de $\mathbf{Q}$, ne contenant pas $\sqrt{d}$ (de sorte que $N(\sqrt{d})$ est de degré 2 sur K, avec $1, \sqrt{d}$ comme base) et telle que l'on ait $y = a + b\sqrt{d} \in N(\sqrt{d})$. Si N est de degré 2 sur $\mathbf{Q}$ on aura résolu le problème initial, comme dans le cas $x = 2 + \sqrt{3}$ où l'on a $N = \mathbf{Q}(\sqrt{2})$.

Comme $1, \sqrt{d}$ sont indépendants sur N, la relation $x = y^2$ est équivalente à $A = a^2 + db^2$ et $B = 2ab$. Comme B est non nul, donc aussi a, on peut tirer $b = B/2a$ et on obtient l'équation en $X = a^2$:

$$Q(X) := 4X^2 - 4AX + dB^2 = 0.$$

Le discriminant de cette équation est $4r = 4(A^2 - dB^2)$ et on en déduit : $a^2 = \dfrac{A \pm \sqrt{r}}{2}$.

Précisément, on choisit une des racines de r, que l'on note $\sqrt{r}$, et on pose $\alpha = \dfrac{A+\sqrt{r}}{2}$ et $\beta = \dfrac{A-\sqrt{r}}{2}$. On a ainsi $\alpha\beta = \dfrac{dB^2}{4}$. On choisit ensuite une racine de α, que l'on note $\sqrt{\alpha}$, et on définit $\sqrt{\beta}$ par la formule $2\sqrt{\alpha}\sqrt{\beta} = B\sqrt{d}$. On considère le corps $N = \mathbf{Q}(\sqrt{\alpha})$. Il est égal à $\mathbf{Q}(\sqrt{r}, \sqrt{\alpha})$ et $N(\sqrt{d})$ contient $\sqrt{\beta}$ et les racines y et $-y$ de x ainsi que z et $-z$ de $\overline{x}$:

$$y = \sqrt{\alpha} + \sqrt{\beta} = \sqrt{\alpha} + \frac{B\sqrt{d}}{2\sqrt{\alpha}} = \sqrt{\beta} + \frac{B\sqrt{d}}{2\sqrt{\beta}}, \quad z = \sqrt{\alpha} - \sqrt{\beta}.$$

Cela montre que $M = N(\sqrt{d})$ est le corps de décomposition de P et on a ainsi une tour de corps :

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt{r}) \subset N = \mathbf{Q}(\sqrt{r}, \sqrt{\alpha}) \subset M = N(\sqrt{d}) = \mathbf{Q}(\sqrt{r}, \sqrt{\alpha}, \sqrt{d}).$$

5. Avec une mention spéciale à la calculatrice qui simplifie les fractions !

On voit que M est au plus de degré 8 sur $\mathbf{Q}$ et il se pose maintenant plusieurs questions :

• L'extension N est-elle de degré 2 (ce qui répondrait positivement à la question initiale) ?

• Sinon, quel est le degré de $M/\mathbf{Q}$ et quel est son groupe de Galois ?

3.2 Le cas biquadratique

L'exemple initial est une illustration du théorème suivant :

3.1 Théorème. *On suppose que $r = A^2 - dB^2$ est un carré de $\mathbf{Q}$: $r = C^2$. Alors, $\alpha = \dfrac{A+C}{2}$ et $\beta = \dfrac{A-C}{2}$ sont dans $\mathbf{Q}$ et, si α et β ne sont pas des carrés de $\mathbf{Q}$, l'extension $N = \mathbf{Q}(\alpha)$ est de degré 2 et M est de la forme $\mathbf{Q}(\sqrt{d}, \sqrt{\alpha})$ (donc une extension* **biquadratique***). Son groupe de Galois est le groupe $\mathbf{V}_4$ de Klein. Les racines y et z de $x = A+B\sqrt{d}$ et de $\overline{x} = A-B\sqrt{d}$ sont dans M, donc de la forme $\lambda\sqrt{d}+\mu\sqrt{\alpha}$. Précisément, si l'on définit $\sqrt{\beta}$ par la formule $2\sqrt{\alpha}\sqrt{\beta} = B\sqrt{d}$, on a $y = \sqrt{\alpha} + \sqrt{\beta}$.*

Démonstration. Comme $\sqrt{r}$ est dans $\mathbf{Q}$, il est clair que M est égale à $\mathbf{Q}(\sqrt{d}, \sqrt{\alpha})$. Montrons que cette extension est bien de degré 4. Il suffit de voir que $\sqrt{\alpha}$ n'est pas dans $\mathbf{Q}(\sqrt{d})$. Sinon, on aurait $\alpha = (x + y\sqrt{d})^2$ d'où $xy = 0$ et $\alpha = x^2 + dy^2$. Autrement dit α ou α/d serait un carré de $\mathbf{Q}$. Mais, comme on a $\alpha\beta = \dfrac{dB^2}{4}$, α ou β serait un carré de $\mathbf{Q}$ et cela a été exclu. Le calcul du groupe de Galois est immédiat : un automorphisme de M envoie $\sqrt{d}$ sur $\pm\sqrt{d}$ et de même pour $\sqrt{\alpha}$.

3.2 *Exemple.* Dans le cas de l'exemple initial, $d = 3$, $A = 2$, $B = 1$, on a $r = 1$, $\alpha = \frac{3}{2}$ et $\beta = \frac{1}{2}$ et $y = \frac{\sqrt{3}}{\sqrt{2}} + \frac{\sqrt{2}}{2} = \frac{\sqrt{6}+\sqrt{2}}{2}$.

3.3 *Remarque.* Si α ou β est un carré de $\mathbf{Q}$ on est dans le cas réductible, voir 2.2.

3.3 Le cas général

Dans le cas général on a le résultat suivant (qui montre que le cas précédent est le seul à donner une extension biquadratique) :

3.4 Théorème. *On suppose que $r = A^2 - dB^2$ n'est pas un carré de $\mathbf{Q}$. Il y a deux cas.*

1) Si r/d est un carré de $\mathbf{Q}$, on a $\mathbf{Q}(\sqrt{r}) = \mathbf{Q}(\sqrt{d})$, le corps M est de degré 4 sur $\mathbf{Q}$, le groupe de Galois de M sur $\mathbf{Q}$ est $\mathbf{Z}/4\mathbf{Z}$. L'extension M n'est pas biquadratique (le seul sous-corps de degré 2 de M est $\mathbf{Q}(\sqrt{d})$).

2) Si r/d n'est pas un carré de $\mathbf{Q}$, le corps N est de degré[6] *4 sur $\mathbf{Q}$, le corps M est de degré 8 sur $\mathbf{Q}$ et le groupe de Galois de M sur $\mathbf{Q}$ est isomorphe au groupe diédral $\mathbf{D}_4$.*

Démonstration. 1) On a $r = ds^2$ avec $s \in \mathbf{Q}$. On prendra par exemple $\sqrt{r} = s\sqrt{d}$. On voit alors qu'on a $\mathbf{Q}(\sqrt{r}) = \mathbf{Q}(\sqrt{d})$ et il en résulte que M est égal à $N = \mathbf{Q}(\sqrt{\alpha})$. Comme r n'est pas un carré de $\mathbf{Q}$, il résulte de 2.2 que y n'est pas dans $\mathbf{Q}(\sqrt{d})$, de sorte que M est de degré 4 sur $\mathbf{Q}$. Calculons le groupe de Galois G de M sur $\mathbf{Q}$. Il est de cardinal $4 = [M : \mathbf{Q}]$, donc isomorphe à $\mathbf{V}_4$ (dont tous les éléments non nuls sont d'ordre 2) ou $\mathbf{Z}/4\mathbf{Z}$. Si σ est dans G on note d'abord qu'on a $\sigma(r) = r$, donc $\sigma(\sqrt{r}) = \epsilon\sqrt{r}$ avec $\epsilon = \pm 1$. Avec $\sqrt{r} = s\sqrt{d}$ on en déduit qu'on a $\sigma(\sqrt{d}) = \epsilon\sqrt{d}$ avec le même signe. Comme on a $\alpha = \dfrac{A + \sqrt{r}}{2}$, on a alors $\sigma(\alpha) = \alpha$ ou β selon que ϵ vaut 1 ou -1 et on en déduit $\sigma(\sqrt{\alpha}) = \pm\sqrt{\alpha}$ ou $\pm\sqrt{\beta}$. Considérons σ tel que $\sigma(\sqrt{\alpha}) = \sqrt{\beta}$ (donc $\epsilon = -1$). On a alors $\sigma^2(\sqrt{\alpha}) = \sigma(\sqrt{\beta})$ et avec la formule $2\alpha\beta = B\sqrt{d}$ on voit que $\sigma^2(\sqrt{\alpha})$ vaut $-\sqrt{\alpha}$. Cela montre que σ n'est pas d'ordre 2, donc que G est le groupe cyclique. Comme ce groupe n'a qu'un sous-groupe d'ordre 2, il n'y a pas d'autre extension de degré 2 que $\mathbf{Q}(\sqrt{d})$ et M n'est pas biquadratique.

2) Montrons que M est de degré 8. On note déjà que $\sqrt{r}$ n'est pas dans $\mathbf{Q}(\sqrt{d})$. Sinon, on aurait $\sqrt{r} = a + b\sqrt{d}$ et on voit aussitôt que cela implique que r ou r/d est un carré de $\mathbf{Q}$ et cela a été exclu. Cela montre que M est de degré multiple de 4. Si c'était 4, comme l'extension admet deux extensions de degré 2, $\mathbf{Q}(\sqrt{d})$ et $\mathbf{Q}(\sqrt{r})$ distinctes, c'est que l'extension est biquadratique avec comme groupe de Galois $G = \mathbf{V}_4$. On considère alors $\sqrt{\alpha} \in M$. Ses conjugués sont $\pm\sqrt{\alpha}$ et $\pm\sqrt{\beta}$. Soit σ l'élément de G qui envoie $\sqrt{\alpha}$ sur $\sqrt{\beta}$. Comme σ est d'ordre 2, l'élément $y = \sqrt{\alpha} + \sqrt{\beta}$ est invariant par σ, donc dans une extension de degré 2 de $\mathbf{Q}$. Mais c'est absurde car le polynôme minimal de y est P qui est irréductible.

On en déduit que $N = \mathbf{Q}(\sqrt{\alpha})$ n'est pas une extension galoisienne de $\mathbf{Q}$. Sinon, elle contiendrait le conjugué $\sqrt{\beta}$, donc aussi $\sqrt{d}$ et, comme on a $M = N(\sqrt{d})$ on aurait $M = N$ et M serait de degré 4.

Il reste à montrer que le groupe de Galois est le groupe diédral. Comme l'extension N n'est pas galoisienne, c'est que le sous-groupe $\mathrm{Gal}(M, N)$ n'est pas distingué dans G. Or, parmi les groupes d'ordre 8, $\mathbf{D}_4$ est le seul à avoir des sous-groupes non distingués ! (Les autres sont soit abéliens, soit le groupe des quaternions $\mathbf{H}_8$ dont tous les sous-groupes sont distingués.)

6. Mais n'est pas une extension galoisienne de $\mathbf{Q}$, donc pas biquadratique.

3.5 *Remarque.* De manière élémentaire, la différence entre les deux cas du théorème est la suivante : y et z ne sont pas dans $\mathbf{Q}(\sqrt{d})$, mais, dans le premier cas, leur produit s'y trouve, alors que ce n'est pas vrai dans le second cas.

3.6 *Exemples.* 1) Si l'on prend $x = 5 + \sqrt{5}$ on a $d = 5$ et $r = 20$. On est dans le cas examiné au point 1). L'extension $\mathbf{Q}\left(\sqrt{5+\sqrt{5}}\right)$ est de degré 4, galoisienne, de groupe de Galois $\mathbf{Z}/4\mathbf{Z}$, donc n'est pas biquadratique.

2) Dans le cas générique, on a une extension de degré 8. C'est le cas, par exemple, avec $x = 1 + \sqrt{5}$ (ici on a $r = -4$) ou encore $x = 4 + \sqrt{5}$ ($r = 11$).

3.4 Bilan

Le théorème suivant résume la situation :

3.7 Théorème. *Soit d un entier sans facteur carré, A, B des rationnels avec $B \neq 0$, $x = A + B\sqrt{d}$, $\overline{x} = A - B\sqrt{d}$. On note y et $-y$ (resp. z et $-z$) les racines carrées de x (resp. $\overline{x}$). On pose $r = A^2 - dB^2$. On a les alternatives suivantes :*

1) Le nombre r est un carré de $\mathbf{Q}$, $r = C^2$, ainsi que l'un des nombres $2(A + \epsilon C)$ avec $\epsilon = \pm 1$. Alors, y et z sont dans $\mathbf{Q}(\sqrt{d})$.

2) Le nombre r est un carré de $\mathbf{Q}$, $r = C^2$, mais les nombres $2(A + \epsilon C)$ avec $\epsilon = \pm 1$ ne sont pas des carrés. Alors y et z sont dans l'extension biquadratique $\mathbf{Q}(\sqrt{d}, \sqrt{r})$.

3) a) Le nombre r n'est pas un carré de $\mathbf{Q}$, mais r/d est un carré de $\mathbf{Q}$. Alors, y et z sont dans une extension galoisienne de degré 4, de groupe de Galois $\mathbf{Z}/4\mathbf{Z}$, donc non biquadratique.

b) Ni r, ni r/d ne sont des carrés de $\mathbf{Q}$. L'extension engendrée par y et z est galoisienne de degré 8 de groupe de Galois $\mathbf{D}_4$.

3.5 Un algorithme

le théorème précédent montre que, pour calculer la racine carrée y de $x = A + B\sqrt{d}$ en repérant éventuellement si elle se dans $\mathbf{Q}(\sqrt{d})$ ou dans une extension biquadratique $\mathbf{Q}(\sqrt{d}, \sqrt{r})$, l'algorithme, finalement assez simple, est le suivant :

1) On calcule $r = A^2 - dB^2$. Si r n'est pas un carré dans $\mathbf{Q}$, on renvoie $y = \sqrt{A + B\sqrt{d}}$.

2) Si r est un carré de $\mathbf{Q}$, $r = C^2$, on regarde $2(A + \epsilon C)$ avec $\epsilon = \pm 1$.

2.1) Si ces nombres ne sont pas des carrés de $\mathbf{Q}$, on renvoie

$$y = \sqrt{\frac{A+C}{2}} + \sqrt{\frac{A-C}{2}},$$

où les racines sont choisies de sorte que leur double produit soit égal à $B\sqrt{d}$.

2.2) Si $2(A+\epsilon C)$ est le carré de $E \in \mathbf{Q}$, on renvoie $y = \frac{E}{2} + \frac{B}{E}\sqrt{d}$.

4 Construire des exemples : un peu d'arithmétique

On a vu ci-dessus comment construire des exemples de x dont la racine soit dans $\mathbf{Q}(\sqrt{d})$ et à l'opposé, un choix aléatoire de x mène en général à une extension de degré 8. En revanche il est intéressant de savoir fabriquer des exemples donnant les cas intermédiaires (groupes de Galois égaux à $\mathbf{V}_4$ ou $\mathbf{Z}/4\mathbf{Z}$). Notre but étant de produire des exemples, nous ne chercherons pas à traiter le cas général et nous ferons souvent des hypothèses simplificatrices (par exemple le tait que d est un nombre premier).

4.1 Des exemples biquadratiques

4.1.1 Le cas $d > 2$

On a vu qu'on a de tels exemples lorsque $r = A^2 - dB^2$ est un carré de $\mathbf{Q}$: $A^2 - dB^2 = C^2$ (et lorsque $2(A \pm C)$ n'en est pas un). Voici, en tous cas, un résultat :

4.1 Proposition. *Soit d un nombre premier impair, $A, B \in \mathbf{Z}$ des entiers premiers entre eux, $x = A + B\sqrt{d}$. Alors, $y = \sqrt{x}$ est dans une extension biquadratique (et pas dans $\mathbf{Q}(\sqrt{d})$) si et seulement si il existe des entiers B_1, B_2, impairs, premiers entre eux, tels que $A = \frac{dB_1^2 + B_2^2}{2}$ et $B = B_1B_2$.*

Démonstration. On vérifie d'abord que si A et B sont de cette forme ils conviennent (on a $C = \frac{dB_1^2 - B_2^2}{2}$ donc $2(A+C) = 2dB_1^2$ et $2(A-C) = 2B_2^2$ et, comme on a $d \neq 2$, ces quantités ne sont pas des carrés).

Inversement, si on a A, B avec $A^2 - dB^2 = C^2$, on peut supposer $C \in \mathbf{N}$ et on écrit alors $A^2 - C^2 = dB^2 = (A-C)(A+C)$. Comme d est premier, il divise $A-C$ ou $A+C$. Par ailleurs, on vérifie facilement que A et C sont premiers entre eux, de sorte que le *pgcd* de $A-C$ et $A+C$ est égal à 1 ou 2.

Supposons d'abord que ce *pgcd* est 1. Alors, les facteurs de B figurant dans ces nombres sont premiers entre eux, autrement dit, on a $B = B_1B_2$, avec B_1, B_2 premiers entre eux, tels que B_1^2 divise $A-C$ et B_2^2 divise $A+C$. On a donc $A-C = dB_1^2$ et $A+C = B_2^2$ ou $A-C = B_1^2$ et $A+C = dB_2^2$, et, dans les deux cas, on a la forme annoncée pour A.

Supposons ensuite qu'on a $pgcd(A-C, A+C) = 2$. Un raisonnement analogue donne $B = B_1B_2$ et $A = dB_1^2 + B_2^2$, mais on a alors $A - C = 4B_2^2$, qui est un carré, contrairement à l'hypothèse que y n'est pas dans $\mathbf{Q}(\sqrt{d})$.

4.2 *Exemples.* Avec $d = 3$ et $B_1 = B_2 = 1$ on obtient l'exemple initial $2+\sqrt{3}$. Avec $d = 5$, $B_1 = 1$ et $B_2 = 3$ on trouve $7 + 3\sqrt{5}$.

4.1.2 Le cas $d = 2$

On a vu que la preuve précédente ne fonctionne pas pour $d = 2$, de fait il n'y a pas de vrais exemples biquadratiques dans ce cas :

4.3 Proposition. *Soient A, B, C des entiers solutions de $A^2 = C^2 + 2B^2$. On suppose que A, B, C n'ont pas de diviseur commun non trivial. Alors, la racine carrée de $x = A + B\sqrt{2}$ est dans $\mathbf{Q}(\sqrt{2})$.*

Démonstration. On peut montrer ce résultat en raisonnant comme ci-dessus avec $(A-C)(A+C) = 2B^2$. On peut aussi faire cela de manière plus savante en travaillant dans l'anneau principal $R = \mathbf{Z}[i\sqrt{2}]$. On écrit $C^2 + dB^2 = (C + iB\sqrt{d})(C - iB\sqrt{d}) = z\overline{z}$. Le lemme crucial est le suivant :

4.4 Lemme. *Les nombres $z, \overline{z}$ sont premiers entre eux dans R.*

Démonstration. Un éventuel facteur commun diviserait leur somme et leur différence $2C$ et $2iB\sqrt{2}$. Comme B, C sont premiers entre eux (sinon ils auraient un facteur commun avec A aussi), le seul facteur possible est $i\sqrt{2}$. Cela implique que C est pair, donc A, donc B et c'est absurde.

Il résulte de ce lemme en décomposant en produit de facteurs premiers que z et $\overline{z}$ sont des carrés (au signe près). Si l'on écrit $z = (\alpha + i\beta\sqrt{2})^2$, on trouve $A = \alpha^2 + 2\beta^2$, $B = 2\alpha\beta$, $C = \alpha^2 - 2\beta^2$ et $x = (\alpha + \beta\sqrt{2})^2$. Cela correspond au cas où $2(A + C) = 4\alpha^2$ est un carré.

4.5 *Remarque.* Bien entendu, on peut obtenir une racine qui habite une extension biquadratique en mettant un facteur, par exemple $x = 9 + 6\sqrt{2}$, mais c'est triché.

4.2 Des exemples avec groupe de Galois $\mathbf{Z}/4\mathbf{Z}$

Rappelons, voir 3.4, que le corps de décomposition M du polynôme P est de degré 4 avec le groupe de Galois cyclique si et seulement si $r = A^2 - dB^2$ n'est pas un carré de $\mathbf{Q}$ mais que r/d en est un. De tels exemples n'existent pas toujours. Précisément, on a la proposition suivante :

4.6 Proposition. *On reprend les notations de 1.2.*

1) Si le le corps de décomposition $M = D_{\mathbf{Q}}(P)$ est de degré 4 avec groupe de Galois $\mathbf{Z}/4\mathbf{Z}$ l'entier d est somme de deux carrés[7]*, $d = p^2 + q^2$.*

2) On suppose que d est somme de deux carrés (par exemple un nombre premier congru à 1 modulo 4), $d = p^2 + q^2$. Soient u, v deux entiers. On obtient un exemple $x = A + B\sqrt{d}$ tel que le corps M soit de degré 4 avec un groupe de Galois cyclique en posant $A = d(u^2 + v^2)$ et $B = p(u^2 - v^2) + 2quv$ ou les formules analogues obtenues en échangeant les rôles de p, q ou de u, v ou en les changeant de signe.

Démonstration. 1) Dire que r/d est un carré revient à dire que rd en est un et on a donc $rd = dA^2 - d^2B^2 = C^2$. Quitte à réduire au même dénominateur on peut supposer A, B, C entiers et C est alors multiple de d (car d est sans facteur carré). On pose $C = dC'$ et on a $A^2 - dB^2 = dC'^2$, ce qui montre que A est multiple de d, $A = dA'$. En définitive, il reste $B^2 + C'^2 = dA'^2$. Cela impose déjà que d est somme de deux carrés en vertu de [DP] *loc. cit.*

2) On reprend l'égalité $dA'^2 = B^2 + C'^2$. Il s'agit de décomposer[8] dA'^2 en somme de deux carrés à partir des décompositions $d = p^2 + q^2$ et $A' = u^2 + v^2$. La méthode est bien connue et consiste à faire le produit des nombres complexes $(p \pm iq)(u \pm iv)(u \pm iv)$. On obtient le résultat annoncé avec la partie réelle de la variante $(p - iq)(u + iv)^2$.

4.7 *Exemple.* Avec $d = 5 = 1^2 + 2^2$, et $A' = 1^2 + 0^2$ on obtient les deux exemples $5 + \sqrt{5}$ et $5 + 2\sqrt{5}$. Avec $A' = 13 = 3^2 + 2^2$ on obtient les solutions $65 + 22\sqrt{5}$, $65 + 19\sqrt{5}$, $65 + 2\sqrt{5}$ et $65 + 29\sqrt{5}$, plus les variantes obtenues en changeant les signes.

5 Références

[DP] PERRIN Daniel, *Cours d'Algèbre*, Ellipses, 1996.

[ST] STEWART Ian, *Galois theory*, Chapmann & Hall, 1973.

7. Donc, comme il est sans facteur carré, d est produit de nombres premiers $\equiv 1 \pmod 4$ et éventuellement de 2 (voir par exemple [DP] Ch. II, §6, th. 6.9).

8. En évitant la décomposition triviale $dA'^2 = A'^2p^2 + A'^2q^2$ qui donne A, B non premiers entre eux.