Equations algébriques résolubles par radicaux carrés

Les propositions suivantes, tirées de la théorie des équations algébriques, sont probablement connues du lecteur; nous allons pourtant les démontrer brièvement, afin de mieux faire percevoir l'ensemble des idées.

Si la grandeur à construire x ne dépend que d'expressions rationnelles et de racines carrées, elle est racine d'une équation irréductible $f(x) = 0$, dont le degré est toujours une puissance de 2.

1. Pour avoir une idée nette de la structure de la grandeur x, supposons qu'elle soit de la forme

$$x = \frac{\sqrt{a+\sqrt{c+ef}}+\sqrt{d+\sqrt{b}}}{\sqrt{a}+\sqrt{b}} + \frac{p+\sqrt{q}}{\sqrt{r}}$$

dans laquelle a, b, c, e, f, p, q, r sont des expressions rationnelles.

2. Le nombre des radicaux superposés figurant dans un terme de x s'appelle l'ordre de ce terme; l'expression précédente renferme des termes d'ordres $0, 1, 2$.

3. μ étant l'ordre maximum, aucun terme ne peut présenter plus de μ radicaux superposés.

4. L'expression

$$x = \sqrt{2}+\sqrt{3}+\sqrt{6}$$

semble renfermer trois termes différents du premier ordre; mais comme

$$\sqrt{6} = \sqrt{2}.\sqrt{3}$$

elle ne dépend en réalité que de deux termes distincts.

Nous supposerons que cette réduction a été faite dans tous les termes de x, de telle sorte que, parmi les différents termes d'ordre μ, aucun ne peut s'exprimer rationnellement en fonction des autres termes d'ordre μ ou d'ordre inférieur.

Nous ferons la même hypothèse sur les termes d'ordre $\mu - 1$ ou d'ordre inférieur; ces termes peuvent d'ailleurs se présenter explicitement ou implicitement. Cette hypothèse, évidemment très naturelle, est d'une grande importance pour les conclusions ultérieures.

5. *Forme normale de x.*

Si l'expression x est une somme de termes de dénominateurs différents, on les réduira au même dénominateur; x se présente alors sous la forme du quotient de deux fonctions entières.

Soit $\sqrt{Q}$ un des termes d'ordre μ; il ne peut figurer dans x que sous forme explicite, puisque μ est l'ordre maximum. D'autre part, les puissances de Q s'expriment en fonction de $\sqrt{Q}$ et de Q qui est un terme d'ordre inférieur à μ. La valeur de x peut donc se ramener à la forme

$$x = \frac{a+b\sqrt{Q}}{c+d\sqrt{Q}}$$

a, b, c, d ne contiennent plus que $(n-1)$ termes d'ordre μ et les termes d'ordre inférieur.

Multipliant les deux termes par $c - d\sqrt{Q}$, le dénominateur ne contient plus $\sqrt{Q}$; il vient

$$x = \frac{ac-bdQ+(bc-ad)\sqrt{Q}}{c^2-d^2Q} = \alpha + \beta\sqrt{Q}$$

α et β ne renferment plus que $(n-1)$ termes d'ordre μ.

Si on avait considéré un autre terme d'ordre μ, par exemple $\sqrt{Q_1}$, on aurait de même pu ramener la valeur de x à la forme

$$x = \alpha_1 + \beta_1\sqrt{Q_1}, \quad \text{etc.}$$

On peut donc transformer x de manière que cette expression ne renferme un terme donné d'ordre μ qu'à son numérateur et qu'elle ne le contienne que linéairement.

Remarquons d'ailleurs que, dans cette transformation, peuvent figurer les produits des termes d'ordre μ. En effet, α et β dépendent encore de $n-1$ termes d'ordre μ. On pourra donc faire en sorte que

$$x = \alpha_{11} + \alpha_{12}\sqrt{Q_1} \qquad \beta = \beta_{11} + \beta_{12}\sqrt{Q_1}$$

et par suite

$$x = \left(\alpha_{11} + \alpha_{12}\sqrt{Q_1}\right) + \left(\beta_{11} + \beta_{12}\sqrt{Q_1}\right)\sqrt{Q}$$

6. Nous procéderons d'une façon analogue pour les différents termes d'ordre $\mu-1$, qui se présentent explicitement dans Q, Q_1, etc.; chacune de ces quantités devient alors une fonction linéaire et entière par rapport au terme d'ordre $\mu-1$ considéré. Nous passons ensuite aux termes d'ordre inférieur, et nous finissons ainsi par mettre x et ses termes des divers ordres sous forme de fonctions rationnelles, linéaires et entières, par rapport aux radicaux qui y figurent *explicitement*. Nous dirons alors que x est mis sous la *forme normale*.

7. Soit m le nombre total des radicaux carrés indépendants (4) qui figurent dans cette forme normale. En attribuant le double signe à ces radicaux et les combinant de toutes les manières possibles, nous obtiendrons un système de 2^m valeurs,

$$x_1, x_2, \ldots, x_{2^m}$$

qui seront désignées par le nom de *valeurs conjuguées*. Nous allons chercher une équation admettant ces valeurs conjuguées comme racines.

8. Ces valeurs ne sont pas nécessairement toutes distinctes; car, si on a par exemple

$$x = \sqrt{a+\sqrt{b}} + \sqrt{a-\sqrt{b}}$$

cette expression ne change pas quand on change le signe de $\sqrt{b}$.

9. Formons le polynome

$$F(x) = (x-x_1)(x-x_2)\ldots(x-x_{2^m})$$

L'équation $F(x) = 0$ admet évidemment pour racines les différentes valeurs conjuguées; elle est du degré 2^m, mais peut admettre des racines multiples (8).

Les coefficients du polynome $F(x)$, ordonné par rapport à x, sont rationnels.

Changeons en effet le signe d'un des radicaux carrés, ce qui a pour effet

de permuter deux racines, x_λ et $x_{\lambda'}$ par exemple, puisque les racines de $F(x)$ sont précisément toutes les valeurs conjuguées. Comme ces racines n'entrent dans $F(x)$ que sous la forme du produit

$$(x-x_\lambda)(x-x_{\lambda'})$$

on ne fait que changer l'ordre des facteurs de $F(x)$; donc ce polynome ne change pas.

$F(x)$ reste donc invariable quand on change le signe de l'une quelconque des racines carrées; il ne contient donc que leurs carrés; il en résulte bien que ses coefficients sont rationnels.

10. *Lorsque l'une quelconque des valeurs conjuguées vérifie une équation à coefficients rationnels $f(x) = 0$, il en est de même de toutes les autres.*

$f(x)$ n'est pas nécessairement égal à $F(x)$, et peut admettre d'autres racines en dehors des x_i.

Soit $x_1 = \alpha + \beta\sqrt{Q}$ une des grandeurs conjuguées, $\sqrt{Q}$ un terme d'ordre μ; α et β dépendent encore des autres termes d'ordre μ et des termes d'ordre inférieur. Il existe alors une grandeur conjuguée

$$x_1' = \alpha - \beta\sqrt{Q}$$

Exprimons que x_1 satisfait à l'équation $f(x) = 0$. Mettons $f(x_1)$ par rapport à $\sqrt{Q}$ sous la forme normale

$$f(x_1) = A + B\sqrt{Q}$$

cette expression ne peut être nulle que sous les conditions simultanées

$$A = 0 \qquad B = 0$$

s'il en était autrement, on aurait

$$\sqrt{Q} = -\frac{A}{B}$$

on pourrait donc exprimer $\sqrt{Q}$ rationnellement en fonction des termes d'ordre μ et des termes d'ordre inférieur contenus dans A et B, ce qui est contraire à l'hypothèse de l'indépendance de toutes les racines carrées (4).

Mais on a évidemment

$$f(x_1') = A - B\sqrt{Q}$$

si donc $f(x_1)$ est nul, il en est de même de $f(x_1')$. D'où cette première proposition :

Si la grandeur x_1 satisfait à l'équation $f(x)=0$, il en est de même de toutes les valeurs conjuguées qui se déduisent de x_1 par le changement de signe de l'un des termes d'ordre μ.

La démonstration se fait d'une manière analogue pour les autres valeurs conjuguées. Supposons par exemple (ce qui ne restreint pas la généralité du raisonnement) que l'expression x ne dépende que de deux termes d'ordre μ, $\sqrt{Q}$ et $\sqrt{Q'}$. $f(x_1)$ pourra être ramenée à la forme normale suivante :

$$f(x_1) = p + q\sqrt{Q} + r\sqrt{Q'} + s\sqrt{Q}\cdot\sqrt{Q'} = 0 \qquad (a)$$

Si x dépendait de plus de deux termes d'ordre μ il faudrait adjoindre à l'expression précédente un plus grand nombre de termes de structure analogue.

L'équation (a) n'est possible que si l'on a séparément

$$p=0 \qquad q=0 \qquad r=0 \qquad s=0 \qquad (b)$$

sans quoi $\sqrt{Q}$ et $\sqrt{Q'}$ seraient liés par une relation rationnelle, ce qui est contraire à l'hypothèse (4).

Soient maintenant $\sqrt{R}$ et $\sqrt{R'}$ les termes d'ordre $\mu-1$ dont dépend x_1 ; ils figurent dans p, q, r, s; on pourra donc mettre ces quantités sous la forme normale par rapport à $\sqrt{R}$ et $\sqrt{R'}$ (en supposant qu'il n'y en ait que deux). On obtient ainsi des équations de la forme

$$p = k_1 + l_1\sqrt{R} + m_1\sqrt{R'} + n_1\sqrt{RR'} = 0 \qquad (c)$$

et d'autres équations analogues pour q, r, s.

L'hypothèse, déjà plusieurs fois utilisée, de l'indépendance des radicaux, nous donne de suite les conditions

$$k_1=0, \quad l_1=0, \quad m_1=0, \quad n_1=0, \quad \text{etc.}$$

Il en résulte que les équations (c) et par suite aussi $f(x)=0$, sont vérifiées, lorsque, au lieu de x_1, on emploie les valeurs conjuguées qui s'en déduisent par les changements de signe de $\sqrt{R}$ et $\sqrt{R'}$. Donc :

L'équation $f(x)=0$ est aussi vérifiée par toutes les valeurs conjuguées

qui se déduisent de x_1 en changeant le signe de l'un des termes d'ordre $\mu-1$.

Le même procédé de démonstration s'applique évidemment aux termes d'ordre $\mu-2$, $\mu-3$, etc., ce qui prouve entièrement la proposition énoncée.

11. Nous venons de considérer deux équations

$$F(x)=0 \quad \text{et} \quad f(x)=0$$

à coefficients rationnels, admettant toutes deux comme racines les quantités x_i.

$F(x)$ est du degré 2^m, et peut avoir des racines multiples; $f(x)$ peut avoir d'autres racines que les x_i.

Soit $\varphi(x)=0$ l'équation de moindre degré, à coefficients rationnels, admettant la racine x_1 et par suite toutes les quantités x_i(10).

2. *Propriétés de l'équation $\varphi(x)=0$.*

1. $\varphi(x)=0$ *est une équation irréductible.*
   Cela veut dire que son premier membre ne peut être mis sous forme d'un produit de deux polynomes à coefficients rationnels.
   Si on avait en effet
   $$\varphi(x)=\psi(x)\chi(x)$$
   la condition $\varphi(x_1)=0$ entraînerait
   $$\psi(x_1)=0 \quad \text{ou} \quad \chi(x_1)=0$$
   Mais, d'après (10), si x_1 satisfait à l'équation à coefficients rationnels $\psi(x)=0$, il en est de même de toutes les valeurs conjuguées x_i; $\varphi(x)=0$ ne serait donc pas l'équation du moindre degré ayant les x_i pour racines.
2. $\varphi(x)=0$ *n'a pas de racines multiples.*
   Car si elle en avait, son premier membre $\varphi(x)$ pourrait se décomposer en facteurs rationnels d'après les méthodes connues de l'Algèbre[1]; donc $\varphi(x)=0$ ne serait pas irréductible.
3. $\varphi(x)=0$ *n'admet pas d'autres racines que les quantités x_i.*
   S'il en était autrement, $F(x)$ et $\varphi(x)$ admettraient un plus grand

[1]Théorie des Racines égales.

commun diviseur, qu'on sait calculer rationnellement. On pourrait donc décomposer $\varphi(x)$ en facteurs rationnels, ce qui est impossible, puisque $\varphi(x)$ est irréductible.

4. Soit M le nombre des x_i qui ont des valeurs distinctes, et soient

$$x_1, x_2, \ldots, x_M$$

ces quantités; on aura

$$\varphi(x) = C(x - x_1)(x - x_2) \ldots (x - x_M)$$

En effet, l'équation $\varphi(x) = 0$ admet pour racines les quantités $x_1, \ldots, x_M$; elle n'admet pas de racines multiples; le polynome $\varphi(x)$ est donc déterminé à un facteur constant près, dont la valeur n'importe pas pour l'équation.

$$\varphi(x) = 0$$

5. *$\varphi(x) = 0$ est la seule équation irréductible à coefficients rationnels admettant les x_i pour racines.*
Car si $f(x) = 0$ était une autre équation rationelle irréductible admettant comme racine x_1 et par suite toutes les quantités x_i, $f(x)$ devrait être divisible par $\varphi(x)$ et par suite ne serait pas irréductible.

13. Comparons maintenant $F(x)$ et $\varphi(x)$. – Ces deux polynomes ont pour seules racines les x_i, et, en outre, $\varphi(x)$ n'admet pas de racines multiples. $F(x)$ est donc divisible par $\varphi(x)$:

$$F(x) = F_1(x) \cdot \varphi(x)$$

$F_1(x)$ a nécessairement ses coefficients rationnels, comme étant le quotient de la division de $F(x)$ par $\varphi(x)$. Si ce n'est pas une constante, ce polynome admet des racines appartenant à $F(x)$; en admettant au moins une, il les admettra toutes (10). Donc $F_1(x)$ est aussi divisible par $\varphi(x)$, et

$$F_1(x) = F_2(x) \cdot \varphi(x)$$

Si $F_2(x)$ n'est pas une constante, le même raisonnement est encore applicable. Le degré des polynomes quotient s'abaisse à chaque opération; par suite au bout d'un nombre limité de divisions on tombe sur une égalité de la forme

$$F_{n-1}(x) = C.\varphi(x)$$

Multipliant toutes les égalités obtenues membre à membre, il vient

$$F(x) = C.[\varphi(x)]^n$$

Donc :

Le polynome $F(x)$ est une puissance du polynome de degré minimm $\varphi(x)$, abstraction faite d'une certaine constante.

14. Nous pouvons maintenant nous rendre compte du degré de $\varphi(x)$. $F(x)$ est du degré 2^m; c'est de plus la n^e puissance de $\varphi(x)$, lequel est du degré M; il en résulte que

$$2^m = n.M$$

Donc M est une puissance de 2; remarquons qu'il en est de même de n. D'où ce théorème :

Le degré de l'équation irréductible à coefficients rationnels, à laquelle satisfait une expression ne dépendant que de radicaux carrés, est une puissance de 2.

15. Comme, d'autre part, il n'existe qu'une seule équation irréductible à coefficients rationnels, vérifiée par tous les x_i, il en résulte la réciproque suivante :

Si une équation irréductible n'est pas du degré 2^h, elle ne peut certainement pas être résolue par radicaux carrés.