1 Références

Par odre croissant de difficulté :

1. Xavier Gourdon, *Les maths en tête, Algèbre*
2. Serge Lang, *Cours d'algèbre*
3. Vinberg, *Algebra*
4. Cohn, *Algebra I*
5. Prasolov, *Polynomials*

Table des matières

cours du jeudi 12 octobre 2017

Introduction

1.1 Méthode de Cardan pour le degré 3

Pour résoudre $x^3+px+q=0$, on peut utiliser la méthode de Cardan qui est facile à retenir (ou à retrouver) :

On cherche une racine sous la forme $x=u+v$:

$$(u+v)^3+p(u+v)+q=0 \Leftrightarrow u^3+v^3+(u+v)(3uv+p)+q=0 \ .$$

Ça se simplifie si on impose $3uv=-p$:

$$u^3+v^3+q=0 \ .$$

Donc si u, v vérifient

$$\begin{cases} u^3+v^3=-q \\ uv=-p/3 \end{cases}$$

alors $u+v, ju+j^2v, j^2u+jv$ sont racines. Plus précisément :

$$X^3+pX+q=(X-(u+v))(X-(ju+j^2v))(X-(j^2u+jv))$$

où u^3, v^3 sont des racines de $T^2+qT-p^3/27$ telles que $uv=-p/3$.

1.2 Méthode d'Euler pour le degré 4

Pour résoudre $x^4 + px^2 + qx + r$ Euler procède ainsi :
On cherche une racine sous la forme $x = \sqrt{u} + \sqrt{v} + \sqrt{v}$.
Or,

$$x = \sqrt{u} + \sqrt{v} + \sqrt{v} \Rightarrow x^2 - u - v - w = 2(\sqrt{u}\sqrt{v} + \sqrt{u}\sqrt{w} + \sqrt{v}\sqrt{w})$$

$$\Rightarrow x^4 - 2(u+v+w)x^2 + (u+v+w)^2 = 4(uv+uw+vw) + 8(\sqrt{u}+\sqrt{v}+\sqrt{v})\sqrt{u}\sqrt{v}\sqrt{w}$$

Donc :

$$x^4 + px^2 + qx + r = (p + 2(u+v+w))x^2 + (q + 8\sqrt{u}\sqrt{v}\sqrt{w})x + r - (u+v+w)^2 + 4(uv+uw+vw).$$

Par conséquent :

$$x^4 + px^2 + qx + r = 0 \Longleftarrow \begin{cases} u + v + w = -p/2 \\ \sqrt{u}\sqrt{v}\sqrt{w} = -q/8 \\ -(u+v+w)^2 + 4(uv + uw + vw) = -r \end{cases}$$

$$\Longleftarrow \begin{cases} u + v + w = -p/2 \\ \sqrt{u}\sqrt{v}\sqrt{w} = -q/8 \\ (uv + uw + vw) = \frac{(p/2)^2 - r}{4} \end{cases}$$

Il suffit donc de trouver $(*)$ u, v, w trois racines du polynôme $T^3 + \frac{p}{2}T^2 + (\frac{(p/2)^2 - r}{4})T - \left(\frac{q}{8}\right)^2$ et trois racines carrées $\sqrt{u}$, $\sqrt{v}$, $\sqrt{w}$ telles que $\sqrt{u}\sqrt{v}\sqrt{w} = -q/8$.

On a ainsi résolu l'équation $x^4 + px^2 + qx + r = 0$ car on peut vérifier que si u, v, w et $\sqrt{u}$, $\sqrt{v}$, $\sqrt{w}$ vérifient $(*)$, alors :

$$x^4 + px^2 + qx + r =$$

$$(x - (\sqrt{u} + \sqrt{v} + \sqrt{w}))(x - (\sqrt{u} - \sqrt{v} - \sqrt{w}))(x - (-\sqrt{u} + \sqrt{v} - \sqrt{w}))(x - (-\sqrt{u} - \sqrt{v} + \sqrt{w})).$$

1.3 Méthodes de Lagrange

1.3.1 Degré 3

Soit $P(X) := X^3 + pX + q \in \mathbb{C}[X]$. On note r_1, r_2, r_3 ses racines.

On pose $a := r_1 + jr_2 + j^2 r_3$. Si on applique tous les $s \in \mathfrak{S}_3$ à a^3, on obtient seulement deux valeurs :

$$a^3 \text{ et } b^3$$

où $b = r_1 + j^2 r_2 + j r_3$.

Donc $(X - a^3)(X - b^3)$ s'exprime simplement en fonction de p, q.

Explicitement :

$$(X - a^3)(X - b^3) = X^2 + 27qX - 27p^3$$

Ce polynôme a pour discriminant $\Delta = 4.(27)^2((\frac{q}{2})^2 + (\frac{p}{3})^3)$.

Remarque : on a aussi $ab = -3p$.

On peut exprimer r_1, r_2, r_3 en fonction de a, b :

$$r_1 = \frac{a+b}{3},\ r_2 = \frac{j^2 a + jb}{3},\ r_3 = \frac{ja + j^2 b}{3},$$

Réciproquement, soient a, b des racines cubiques :

$$a := \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

$$b := \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

telles que $ab = -3p$.

Exercice : vérifier que c'est possible !

Alors si on pose :

$$r_1 = \frac{a+b}{3},\ r_2 = \frac{j^2 a + jb}{3},\ r_3 = \frac{ja + j^2 b}{3}$$

on a bien $(X - r_1)(X - r_2)(X - r_3) = X^3 + pX + q$.

On a donc bien résolu notre équation avec des radicaux.

Exemples :

i) l'unique racine réelle de $X^3 - X - 1$ est :

$$\sqrt[3]{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{23}{27}}} + \sqrt[3]{\frac{1}{2} - \frac{1}{2}\sqrt{\frac{23}{27}}}\ .$$

ii) $X^3 - 3X + 1$ a 3 racines réelles mais aucune n'est *résoluble par radicaux réels* : c'est le *casus irreducibilis*. Une des racines est :

$$2\cos\left(\frac{2\pi}{9}\right) = \sqrt[3]{j} + \sqrt[3]{j^2}\ .$$

où on pose $\sqrt[3]{re^{it}} := r^{\frac{1}{3}} e^{\frac{it}{3}}$ *si* $r > 0$ *et* $-\pi < t < \pi$.

Exercice : Montrer que $2\cos(2\pi/7) = -\frac{1}{3} + \frac{1}{3}\left(\sqrt[3]{\frac{7+21i\sqrt{3}}{2}} + \sqrt[3]{\frac{7-21i\sqrt{3}}{2}}\right)$ *(indication :* $1 + 2\cos(2\pi/7) + 2\cos(4\pi/7) + 2\cos(6\pi/7) = 0$ *et* $(2\cos 3t) = (2\cos t)^3 - 3(2\cos t)$*).*

1.3.2 Degré 4

Il y a aussi des formules avec des radicaux mais qui prennent beaucoup de places ...

Soient $p, q, r \in \mathbb{C}$.

On note r_1, r_2, r_3, r_4 les racines du polynôme $P := X^4 + pX^2 + qX + r$ *i.e.* :

$$P(X) = (X - r_1)(X - r_2)(X - r_3)(X - r_4) \ .$$

On pose $t_1 := (r_1+r_2)(r_3+r_4)$, $t_2 := (r_1+r_3)(r_2+r_4)$, $t_3 := (r_1+r_4)(r_2+r_3)$. On a alors :

$$R(X) := (X - t_1)(X - t_2)(X - t_3) = X^3 - 2pX^2 + (p^2 - 4r)X + q^2 \ .$$

Remarque : $(t_1-t_2)^2(t_2-t_3)^2(t_1-t_3)^2 = (r_1-r_2)^2(r_2-r_3)^2(r_3-r_4)^2(r_1-r_3)^2(r_2-r_4)^2(r_1-r_4)^2 = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3$.

Comme $r_1 + r_2 + r_3 + r_4 = 0$, on a aussi :

$$(r_1 + r_2)^2 = -t_1,\ (r_1 + r_3)^2 = -t_2,\ (r_1 + r_4)^2 = -t_3 \ .$$

On peut donc retrouver r_1, r_2, r_3, r_4 à partir de t_1, t_2, t_3.

On choisit des racines carrées des $-t_i$ de sorte que :

$$r_1 + r_2 = \sqrt{-t_1},\ r_1 + r_3 = \sqrt{-t_2},\ r_1 + r_4 = \sqrt{-t_3} \ .$$

Remarque : on a forcément $\sqrt{-t_1}\sqrt{-t_2}\sqrt{-t_3} = -q$.

On a alors :

$$r_1 = \frac{\sqrt{-t_1} + \sqrt{-t_2} + \sqrt{-t_3}}{2}$$
$$r_2 = \frac{\sqrt{-t_1} - \sqrt{-t_2} - \sqrt{-t_3}}{2}$$
$$r_3 = \frac{-\sqrt{-t_1} + \sqrt{-t_2} - \sqrt{-t_3}}{2}$$
$$r_4 = \frac{-\sqrt{-t_1} - \sqrt{-t_2} + \sqrt{-t_3}}{2} \ .$$

Réciproquement, si on note t_1, t_2, t_3 les racines du polynôme :

$$R(X) := X^3 - 2pX^2 + (p^2 - 4r)X + q^2$$

si on choisit trois racines carrées $\sqrt{-t_1}, \sqrt{-t_2}, \sqrt{-t_3}$ telles que $\sqrt{-t_1}\sqrt{-t_2}\sqrt{-t_3} = -q$, et si on pose :

$$r_1 := \frac{\sqrt{-t_1} + \sqrt{-t_2} + \sqrt{-t_3}}{2}$$

$$r_2 := \frac{\sqrt{-t_1} - \sqrt{-t_2} - \sqrt{-t_3}}{2}$$
$$r_3 := \frac{-\sqrt{-t_1} + \sqrt{-t_2} - \sqrt{-t_3}}{2}$$
$$r_4 := \frac{-\sqrt{-t_1} - \sqrt{-t_2} + \sqrt{-t_3}}{2},$$

alors :

$$X^4 + pX^2 + qX + r = (X - r_1)(X - r_2)(X - r_4)(X - r_4) \ .$$

On a donc résolu notre équation par des radicaux.

1.4 Degré ≥ 5

On a : $x^5 - 2 = (x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5)$ où $x_k = \sqrt[5]{2}(\cos(2k\pi/5) + i\sin(2k\pi/5)) = \sqrt[5]{2}\left(\frac{1+\sqrt{5}}{4} + \frac{\sqrt{-1}}{2}\sqrt{\frac{5-\sqrt{5}}{2}}\right)^k$. Donc $x^5 - 2 = 0$ est une équation « *résoluble par radicaux* ».

En revanche nous verrons plus tard que l'équation $x^5 - x - 1 = 0$ n'est pas résoluble par radicaux.

2 Polynômes et fonctions symétriques

2.1 polynômes symétriques

Soit K un corps. Si $s \in \mathfrak{S}_n$, si $P \in K[X_1, ..., X_n]$, on note $P^s(X_1, ..., X_n) := P(X_{s(1)}, ..., X_{s(n)})$. (*C'est une action à droite*). On note $K[X_1, ..., X_n]^{\mathfrak{S}_n}$ les polynômes invariants ou *polynômes symétriques*.

On note $\sigma_k(X_1, ..., X_n) := \sum_{1 \leq i_1 < ... < i_k \leq n} X_{i_1}...X_{i_k}$ les *polynômes symétriques élémentaires* . On peut aussi les définir aussi par l'égalité :

$$(T + X_1)....(T + X_n) = T^n\sigma_1 T^{n-1} + ... + \sigma_n$$

dans $K[X_1, ..., X_n][T]$.

Proposition 2.1 $K[X_1, ..., X_n]^{\mathfrak{S}_n} = K[\sigma_1, ..., \sigma_n]$

Démonstration : Par récurrence sur le degré donné par l'ordre lexicographique $X_1 > ... > X_n$. *q.e.d.*

Remarque : c'est vrai si on remplace K par $\mathbb{Z}$!

Exercice : Si K est de caractéristique $\neq 2$, alors $K[X_1,...,X_n]^{A_n} = K[\sigma_1,...,\sigma_n] + \delta K[\sigma_1,...,\sigma_n]$ où $\delta := \prod_{1\leq i<j\leq n}(X_i - X_j)$

Solution : soit P tel que $^{\forall}\sigma$, $P^\sigma = \epsilon(\sigma)P$, alors P est divisible par δ (en effet, le monôme dominant de P est de la forme X^α avec $\alpha_1 > .... > \alpha_n$ qui est divisible par $X_1^{n-1}....X_{n-1}$, monôme dominant de δ donc

$$X^\alpha = X_1^{n-1}....X_{n-1}X^\beta$$

où $\beta_1 = \alpha_1 - (n-1) \geq \beta_2 = \alpha_2 - (n-2) \geq .... \geq \beta_n$. Mais alors, X^β est le terme dominant de $\sigma_1^{\beta_1-\beta_2}...\sigma_n^{\beta_n}$. Donc $P = \Delta\sigma_1^{\beta_1-\beta_2}...\sigma_n^{\beta_n} + Q$ où $Q^\sigma = \epsilon(\sigma)Q$ pour tout $\sigma \in \mathfrak{S}_n$ et $\deg Q < \deg P$. On peut raisonner par récurrence !.

Si $P^\sigma = P$ pour tout $\sigma \in A_n$, on vérifie facilement que si l'on pose $\tau = (12)$, transposition, alors $Q = P + P^\tau$ est symétrique et $R = P - P^\tau$ vérifie $R^\sigma = \epsilon(\sigma)R$ pour tout $\sigma \in \mathfrak{S}_n$. Il suffit pour conclure de remarquer que $P = \frac{1}{2}Q + \frac{1}{2}R$ ...

2.2 fonctions rationnelles symétriques

Soit K un corps.

Théorème 2.2 $K(X_1,...,X_n)^{\mathfrak{S}_n} = K(\sigma_1,...,\sigma_n)$

Démonstration : Inclusion non évidente : soit a/b une fraction rationnelle symétrique (où $a, b \in K[X_1,..,X_n]$). Posons $B = \prod_{\sigma\in\mathfrak{S}_n} b^\sigma$. Il est clair que B est un polynôme symétrique, que $a/b = \frac{Ba/b}{B}$ et que Ba/b est un polynôme symétrique ! *q.e.d.*

2.3 Relations coefficients racines

Proposition 2.3 (relations coefficients-racines) *Soit* $P(X) := X^n + a_1X^{n-1} + ... + a_n \in K[X]$. *On suppose que* P *a* n *racines* $x_1,...,x_n$ *dans une extension de* K i.e. *:*

$$P = (X - x_1)...(X - x_n) \ .$$

Alors $a_k = (-1)^k\sigma_k(x_1,...,x_n)$.

conséquence : si par exemple $P(X) = X^n + a_1X^{n-1} + ... + a_n \in \mathbb{Z}[X]$ si on note $r_1,...,r_n \in \mathbb{C}$ ses racines, alors tout polynôme $f \in \mathbb{Z}[X_1,...,X_n]$ symétrique vérifie $f(r_1,...,r_n) \in \mathbb{Z}$.

Exercice : $X^n - X - 1$ est irréductible sur $\mathbb{Q}$ pour tout $n \geq 2$. *Indications : Pour tout polynôme* $P \in \mathbb{C}[X]$, *on notera, chaque fois que cela a un sens :*

$$\mathscr{S}(P) := \sum_{z \text{ racine de P}} (z - \frac{1}{z}) \ .$$

Notons $F := X^n - X - 1$.

a) Montrer que F *a* n *racines distinctes et calculer* $\mathscr{S}(F)$.

b) Soit maintenant $D \in \mathbb{Q}[X]$ *est un diviseur unitaire de* F *(utiliser le contenu (défini plus loin ...).*

c) Montrer que $D \in \mathbb{Z}[X]$.

d) Montrer que $\mathscr{S}(D)$ *a un sens et que c'est un entier.*

e) Soit $z = re^{it}$ *(*$r > 0$ et $t \in \mathbb{R}$*) une racine de* D. *Montrer que :*

$$r^{2n} = r^2 + 1 + 2r\cos t$$

et en déduire que $r \neq 1$.

f) Montrer que $2Re(z - \frac{1}{z}) > \frac{1}{r^2} - 1$.

g) Soient $z_1, ..., z_d$ *les racines de* D. *Calculer* $\prod_{i=1}^{d} |z_i|$.

h) Montrer que $\mathscr{S}(D) \geq 1$.

Exercice :

a) soit $P(X) := X^3 + pX + q = (X - r_1)(X - r_2)(X - r_3)$. Montrer que $\Delta := (r_1 - r_2)^2(r_2 - r_3)^2(r_1 - r_3)^2 = -4p^3 - 27q^2$ [*] ;

b) soit $P(X) := X^3 + a_1X^2 + a_2X + a_3 = (X - r_1)(X - r_2)(X - r_3)$, alors $r_1 - r_2)^2(r_2 - r_3)^2(r_1 - r_3)^2 = a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2 + 18a_1a_2a_3$

c) soit $P(X) := X^4 + pX^2 + qX + r = (X - r_1)(X - r_2)(X - r_3)(X - r_4)$. Montrer que $(r_1 - r_2)^2(r_2 - r_3)^2(r_3 - r_4)^2(r_1 - r_3)^2(r_2 - r_4)^2(r_1 - r_4)^2 = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3$.

Définition 1 (Discriminant) *Soit* $P = (X - x_1)...(X - x_n)$ *un polynôme scindé sur* $\mathbb{C}$. *On pose*

$$\Delta(P) = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq i \neq j \leq n} (x_i - x_j)$$

le discriminant de P.

Remarque : si P est réel, alors $\Delta(P) \in \mathbb{R}$ et $\Delta > 0 \Leftrightarrow P$ a 3 racines réelles distinctes, $\Delta < 0 \Leftrightarrow P$ a 1 racine réelle et 2 racines réelles conjuguées non réelles et $\Delta = 0 \Leftrightarrow P$ a une racine réelle double ou triple.

Exercice :

$*$. Δ est symétrique donc est un polynôme en p, q ! De plus Δ est homogène de degré 6 en les r_i. Or p est homogène de degré 2 et q homogène de degré 3 en les r_i. Donc les seuls monômes en p, q qui apparaissent dans Δ sont p^3 et q^2. Pour trouver les bons coefficients on peut par exemple regarder les cas de $X^3 - 1$ et de $X^3 - X$ ...

a) $\Delta(P)$ est un polynôme à coefficients entiers en les coefficients de P !

b) $\Delta(P) = (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq i \leq n} P'(x_i)$.

c) $\Delta(P) = 0$ ou $1 \bmod 4$ si P est unitaire à coefficients entiers. *Indication : on pose* $\delta_1 = \prod_{1 \leq i < j \leq n}(x_i + x_j)$*, c'est symétrique en les racines donc c'est un entier et* $\Delta = \prod_{1 \leq i < j \leq n}(x_i - x_j)^2 = \prod_{1 \leq i < j \leq n}((x_i + x_j)^2 - 4x_i x_j) = \delta_1^2 + 4 \times$ *une fonction symétrique en les* x_i *c-à-d un entier.*

d) Soit $P_n = n!\left(\frac{X^n}{n!} + ... + 1\right)$. Alors $\Delta(P_n) = (-1)^{\frac{n(n-1)}{2}}(n!)^n$. *Indication :* $P_n' = nP_{n-1}$.