Un théorème mythique

Gaëtan Bayle des Courchamps

19 mars 2002

Table des matières

1 Introduction

Cet article a pour but de présenter une démonstration élémentaire d'un théorème mythique : l'inexistence d'une formule générale qui permette de résoudre les équations algébriques de degré supérieur à 5 à l'aide de radicaux, conjugaisons, additions, soustractions, multiplications et divisions.

La démonstration proposée est adaptée de l'excellent livre "100 Great Problems of Elementary Mathematics" (traduction anglaise d'un bouquin de Heinrich Dörrie). Les notations ont été modernisées et quelques précisions ajoutées là où cela me semblait nécessaire (au prix d'un certain alourdissement des notations et de pas mal de notes de bas de page que l'on peut sauter en première lecture).

La démarche est assez simple : il suffit de donner un exemple d'équation polynomiale non-soluble par radicaux. Pour cela, on commence par montrer quelques propriétés que doit vérifier une équation polynomiale soluble par radicaux. On aboutit au théorème de Kronecker, qui énonce que si une équation polynomiale à coefficients rationnels, irréductible et de degré n premier impair, est résoluble par radicaux, alors elle a 1 ou n racines réelles. Il suffit alors d'exhiber une telle équation polynomiale irréductible, à coefficients rationnels et de degré 5, n'ayant ni 1 ni 5 racines réelles pour que le théorème d'Abel soit prouvé.

Les connaissance requises sont du niveau de première année de maths sup : nombres complexes, arithmétique élémentaire sur les entiers et sur les polynômes. Quelques résultats simples mais peut-être hors programme sur les polynômes symétriques (en particulier le théorème de Waring) sont rappelées en annexe.

2 Un peu de vocabulaire et de notations ...

Dans ce qui suit, on fait un usage intensif des notions et des notations ci-dessous.

Définition 2.1 (Nombre exprimable par radicaux) *Un nombre $x \in \mathbf{C}$ est dit exprimable par radicaux si et seulement si on peut l'obtenir en n'utilisant que des additions, soustractions, multiplications, divisions, extractions de racines et en partant de nombres rationnels.*

Exemple : $x = \sqrt[3]{\frac{4}{\sqrt{5}} + \sqrt[7]{\frac{2}{9} - 3}}$ est exprimable par radicaux.

Définition 2.2 (Polynôme réductible dans un corps) *Soit un corps $\mathbf{K}$ et soit P un polynôme à coefficients dans $\mathbf{K}$.*
On dit que P est réductible dans $\mathbf{K}$ si et seulement s'il existe deux polynômes A et B, à coefficients dans $\mathbf{K}$, tels que $P = AB$.

Définition 2.3 (Extension d'un sous-corps de C) *Si $\mathbf{K}$ est un sous-corps de $\mathbf{C}$ et si λ est un élément de $\mathbf{C}$, on note $\mathbf{K}(\lambda)$ le plus petit sous-corps de $\mathbf{C}$ (au sens de l'inclusion) qui contienne λ et tous les éléments de $\mathbf{K}$.*

Remarque : $\mathbf{K}(\lambda)$ existe, car toute intersection de sous-corps est un sous-corps.

Définition 2.4 (Notations utilisées) *Ici, les corps et anneaux sont notés par des majuscules en gras. Ainsi, on note :*
- $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{C}$ *les corps respectifs des réels, des rationnels, des complexes.*
- $\mathbf{N}$ *l'ensemble des entiers naturels.*
- $\mathbf{Z}$ *l'ensemble des entiers relatifs.*

On a aussi besoin de noter les extensions d'un corps ; si l'on appelle $\mathbf{K}$ un corps quelconque :
- $\mathbf{K}(\lambda)$ *: plus petit corps contenant tous les éléments du corps $\mathbf{K}$ et λ.*
- $\mathbf{K}(\lambda_1, \ldots, \lambda_n)$ *: plus petit corps contenant les éléments de $\mathbf{K}$ et λ_1, ..., λ_n.*

3 Quelques lemmes sur les polynômes irréductibles

Lemme 3.1 (Lemme d'Abel) *Soit $\mathbf{K}$ un sous-corps de $\mathbf{C}$, soit une constante $a \in \mathbf{K}$, et soit un nombre premier p. Si a n'est pas une puissance p-ième d'un élément de $\mathbf{K}$, alors le polynome $P(X) = X^p - a$ est irréductible dans $\mathbf{K}[X]$.*

Preuve : Supposons que $P(X)$ soit réductible dans $\mathbf{K}[X]$. Alors il existe deux polynômes $\psi(X)$ et $\varphi(X)$ de $\mathbf{K}[X]$, de degré au moins égal à un, tels que $X^p - a = \psi(X)\varphi(X)$. Soit r une racine p-ième de a, et soit ϵ la racine p-ième de l'unité $e^{\frac{2i\pi}{p}}$.
Alors les p racines de $X^p - a$ sont les $r\epsilon^i$ où $i = 0..(p-1)$, donc :

$$X^p - a = \prod_{i=0}^{p-1} \left(X - r\epsilon^i\right)$$

On a donc décomposé $P(X)$ en produit de polynômes irréductibles dans $\mathbf{C}[X]$. Donc $\psi(X)$ et $\varphi(X)$ s'expriment chacun comme produit d'un certain nombre de ces facteurs. Notons respectivement ψ_0 et φ_0 leur terme constant. En développant $\psi(X)$ et $\varphi(X)$, on s'aperçoit qu'il existe deux entiers positifs (μ, ν) et deux entiers (M, N) tels que :

$$\left\{ \begin{array}{lcl} \psi_0 & = & r^\mu \epsilon^M \\ \varphi_0 & = & r^\nu \epsilon^N \\ p & = & \mu + \nu \end{array} \right.$$

Comme p est premier, μ et ν sont premiers entre eux, donc il existe un couple (k, h) d'entiers tel que $h\mu + k\nu = 1$. Posons $K = \psi_0^h \varphi_0^k$. Alors :

$$\begin{array}{lcll} K^p & = & ((r^\mu \epsilon^M)^h (r^\nu \epsilon^N)^k)^p & \\ & = & (r^{h\mu+k\nu})^p \epsilon^{p(hM+kN)} & \\ & = & r^p & (\text{car } h\mu + k\nu = 1 \text{ et } \epsilon^p = 1) \\ K^p & = & a & (\text{par définition de } p) \end{array}$$

D'autre part, K appartient à $\mathbf{K}$, puisque ψ_0 et φ_0 sont des coefficients à valeurs dans $\mathbf{K}$. Donc a est puissance p-ième d'un élément de $\mathbf{K}$. Ceci contredit les hypothèses du théorème, donc $P(X)$ n'est en fait pas réductible dans $\mathbf{K}[X]$. CQFD. ∎

Théorème 3.2 (Théorème de Gauss) *Soit un polynôme unitaire (i.e. de coefficient dominant égal à un) P à coefficients dans $\mathbf{Z}$. Supposons qu'il existe deux polynômes unitaires ψ et φ, à coefficients dans $\mathbf{Q}$, tels que $P = \psi\varphi$.*
Alors tous les coefficients de ψ et de φ sont des entiers naturels.

Preuve : Soient m et n les degrés respectifs de ψ et de φ. Soient respectivement a_0 et b_0 les plus petits entiers naturels non-nuls tels que $a_0\psi$ et $b_0\varphi$ soient à coefficients entiers. Alors, en posant $\Psi = a_0\psi$ et $\Phi = b_0\varphi$, on peut écrire :

$$\begin{aligned}\Psi(X) &= \sum_{i=0}^{m} a_i X^i \\ \Phi(X) &= \sum_{j=0}^{n} b_j X^j\end{aligned}$$

Posons de plus : $Q = a_0 b_0 P = \Psi\Phi$.
Soit p un diviseur premier de $a_0 b_0$. Regroupons respectivement dans U et V les coefficients de Ψ et de Φ qui sont multiples de p. Regroupons de même dans u et v ceux qui ne sont pas multiples de p (donc premiers avec p, puisque p est premier). Alors :

$$\begin{aligned}Q &= (U+u)(V+v) \\ uv &= Q - UV - Uv - uV\end{aligned}$$

Par choix de a_0 et de b_0, les coefficients de Ψ et de Φ sont respectivement premiers dans leur ensemble : pour chacun de ces polynômes, il existe donc au moins un coefficient non multiple de p, et par conséquent premier avec p. Ceci fait que u et v sont non-nuls. Or leurs coefficients non-nuls de plus petit degré sont premiers avec p, donc le coefficient non-nul de plus petit degré du produit uv est premier avec p.
Or tous les coefficients du membre de droite sont multiples de p, ce qui est contradictoire puisque les deux membres sont censés être égaux.
Donc $a_0 b_0$ ne possède pas de diviseur premier, d'où $a_0 b_0 = 1$, ce qui implique $a_0 = b_0 = 1$.
En particulier, ψ et φ sont à coefficients entiers. CQFD. ∎

Théorème 3.3 (Théorème d'irréductibilité de Schœnemann) *Soit P un polynôme unitaire à coefficients dans $\mathbf{Z}$. S'il existe un nombre premier p tel que p divise tous les coefficients de P autres que le coefficient dominant, et tel que p^2 ne divise pas le coefficient de degré 0, alors P est irréductible dans $\mathbf{Q}[X]$.*

Preuve : Supposons qu'il existe deux polynômes A et B de $\mathbf{Q}[X]$, de degré au moins 1, tels que $P = AB$. Comme P est unitaire, on peut prendre A et B unitaires aussi. Comme de plus P est à coefficients entiers, le théorème de Gauss montré ci-dessus permet alors de dire que A et B sont à coefficients entiers. Appelons n, ν et μ les degrés respectifs de P, A et B ; notons respectivement $(c_i)_{i=0\ldots n}$, $(a_j)_{j=0\ldots\nu}$ et $(b_k)_{k=0\ldots\mu}$ les coefficients de P, A et B. Complétons les suites a et b par des 0 en posant $a_j = 0$ pour $\nu < j < n$ et $b_k = 0$ pour $\mu < k < n$. Alors :

$$\forall i \in \{0 \ldots n\}, c_i = \sum_{j=0}^{i} a_j b_{n-j}$$

Pour $i = 0$, on a $c_0 = a_0 b_0$. Par hypothèse, p est premier et divise c_0, mais p^2 ne divise pas c_0, donc p divise un seul des coefficients a_0 ou b_0. Pour fixer les idées, disons que p divise a_0. Alors p ne divise pas b_0, donc p est premier avec b_0.
A présent, soit i un nombre compris entre 1 et ν. Supposons que, pour tout $0 \leq k \leq i-1$, p divise a_k. On peut écrire :

$$a_i b_0 = c_i - \sum_{j=0}^{i-1} a_j b_{n-j}$$

Alors tous les termes de la somme sont multiples de p. De plus, puisque A et B sont tous deux de degré au moins 1, on a $\nu < n$ donc $i < n$ et c_i est multiple de p. Donc le membre de droite est multiple de p. Or b_0 est premier avec p, donc a_i est multiple de p.
Donc, par récurrence sur i compris entre 0 et ν, a_ν est multiple de p.

Or $c_n = a_\nu b_\mu$ (les termes nuls disparaissent), donc c_n doit être multiple de p. C'est impossible par hypothèse ($c_n = 1$) donc finalement P n'est pas réductible dans $\mathbf{Q}[X]$. CQFD. ∎
Remarque : On peut remplacer l'hypothèse "P unitaire" par "p ne divise pas le coefficient dominant de P", mais la démonstration devient alors plus technique (on ne peut plus recourir au théorème de Gauss).

Théorème 3.4 (Théorème d'irréductibilité d'Abel) *Soit* $\mathbf{K}$ *un corps, et soir un polynôme* P *irréductible dans* $\mathbf{K}[X]$*. Alors tous les polynômes de* $\mathbf{K}[X]$ *qui possèdent une racine en commun avec* P *sont multiples de* P*.*

Preuve : Soit Q un polynôme de $\mathbf{K}[X]$ possédant une racine en commun avec P. Soit A le plus grand commun diviseur de P et de Q. Alors A est au moins de degré 1 (puisqu'il y a une racine commune). D'autre part, l'algorithme d'Euclide nous garantit que A est un élément de $\mathbf{K}[X]$ et qu'il existe un polynôme B de $\mathbf{K}[X]$ tel que $P = AB$.
A est au moins de degré 1, donc B est différent de P. Si le degré de B était non-nul, P serait réductible dans $\mathbf{K}[X]$ (puisque $P = AB$), ce qui est exclu par hypothèse, donc le degré de B est 0. Donc A est multiple de P. Or Q est multiple de A (par définition de A), donc Q est aussi multiple de P. CQFD. ∎

Lemme 3.5 (Adjonction d'un nombre algébrique à un corps) *Soit* $\mathbf{K}$ *un sous-corps de* $\mathbf{C}$*, soit un polynôme* P *irréductible, de degré* n *dans* $\mathbf{K}[X]$ *possédant une racine* $\alpha \in \mathbf{C}$ *n'appartenant pas à* $\mathbf{K}$*.*
Alors, si l'on note $\mathbf{K}(\alpha)$ *le plus petit sous-corps de* $\mathbf{C}$ *qui contienne* $\mathbf{K}$ *et* α*,* $\mathbf{K}(\alpha)$ *est l'ensemble des valeurs prises par* $Q(\alpha)$*, où* Q *décrit l'ensemble des polynômes de degré au plus* $n-1$ *à coefficients dans* $\mathbf{K}$*.*
De plus, pour tout x *de* $\mathbf{K}(\alpha)$*, il existe un unique polynôme* $Q \in \mathbf{K}[X]$ *de degré au plus* $n-1$ *tel que* $x = Q(\alpha)$*.*

Remarque : Ici, on peut remplacer $\mathbf{C}$ par n'importe quel corps commutatif.
Preuve : Notons $\mathbf{K}_{n-1}[X]$ l'ensemble des polynômes à coefficients dans $\mathbf{K}$ et de degré au plus $n-1$. Notons $\mathbf{K}_{n-1}(\alpha)$ l'ensemble des valeurs prises par $Q(\alpha)$ quand Q décrit $\mathbf{K}_{n-1}[X]$ et prouvons que c'est un sous-corps de $\mathbf{C}$

- $\mathbf{K}_{n-1}[x]$ est stable par addition, donc $\mathbf{K}_{n-1}(\alpha)$ aussi.
- Soient deux polynômes U et V de $\mathbf{K}_{n-1}[X]$. Soient Q et R le quotient et le reste de la division euclidienne de UV par P.
  Alors $UV(\alpha) = QP(\alpha) + R(\alpha) = R(\alpha)$ car $P(\alpha) = 0$. Or $R \in \mathbf{K}_{n-1}[X]$ donc $R(\alpha) \in \mathbf{K}_{n-1}(\alpha)$. On a donc prouvé que $\mathbf{K}_{n-1}(\alpha)$ est stable par multiplication.

- Soit un polynôme U non-nul de $\mathbf{K}_{n-1}[X]$. Comme P est irréductible dans $\mathbf{K}[X]$, U et P sont premiers entre eux, donc il existe deux polynômes A et B de $\mathbf{K}[X]$ tels que $UA + BP = 1$. Alors $(UA + BP)(\alpha) = UA(\alpha)$ car $P(\alpha) = 0$, donc $U(\alpha)A(\alpha) = 1$. En prenant, comme précédemment, le reste R de la division euclidienne de A par P, on trouve $A(\alpha) = R(\alpha)$ et, comme $R \in \mathbf{K}_{n-1}[X]$, on peut conclure à la stabilité de $\mathbf{K}_{n-1}(\alpha)$ par inversion.

Donc $\mathbf{K}_{n-1}(\alpha)$ est bien un sous-corps de $\mathbf{C}$ qui contient α. Donc $\mathbf{K}(\alpha) \subset \mathbf{K}_{n-1}(\alpha)$. Or, comme $\mathbf{K}(\alpha)$ est stable par addition et multiplication, il contient $\mathbf{K}_{n-1}(\alpha)$, donc finalement $\mathbf{K}(\alpha) = \mathbf{K}_{n-1}(\alpha)$.
Prouvons à présent l'unicité : soient A et B deux polynômes de $\mathbf{K}_{n-1}[X]$ tels que $A(\alpha) = B(\alpha)$. Alors $(A-B)(\alpha) = 0$. Or P est un polynôme irréductible de $\mathbf{K}[X]$ tel que $P(\alpha) = 0$, donc $A - B$ est multiple de P. Comme $A - B$ est au plus de degré $n-1$ alors que P est de degré n, la seule possibilité est $A - B = 0$, c'est-à-dire $A = B$. CQFD. ∎

Lemme 3.6 (Condition nécessaire pour qu'un polynôme devienne réductible) *Soit* $\mathbf{K}$ *un sous-corps de* $\mathbf{C}$*, et soit un polynôme* P*, irréductible dans* $\mathbf{K}[X]$ *et de degré* p *premier.*
Soit un polynôme Q *de* $\mathbf{K}[X]$*, irréductible, de degré* q*, possédant dans* $\mathbf{C}$ *une racine* α *telle que* P *soit réductible dans* $\mathbf{K}(\alpha)[X]$*.*
Alors q *est multiple de* p*.*

Preuve : D'après les hypothèses du lemme, il existe deux polynômes de $\mathbf{K}(\alpha)[X]$ et de degré au moins 1 dont le produit est P. Chaque élément de $\mathbf{K}(\alpha)$ pouvant s'exprimer à l'aide d'un polynôme de $\mathbf{K}[X]$ pris en α, il existe donc deux polynômes $\psi(X, Y)$ et $\phi(X, Y)$, à deux indéterminées et à coefficients dans $\mathbf{K}$, tels que :

$$P(X) = \psi(X, \alpha)\phi(X, \alpha)$$

et dont les degrés respectifs par rapport à X sont des entiers m et n au moins égaux à 1, avec bien sûr $m+n=p$.

Pour tout nombre complexe r, définissons le polynôme U_r par :

$$U_r(Y) = P(r) - \psi(r,Y)\phi(r,Y)$$

Prenons à présent r dans l'ensemble $\mathbf{Q}$ des rationnels.
Comme $P(X) = \psi(X,\alpha)\phi(X,\alpha)$, on a donc $U_r(\alpha) = 0$. De plus r est rationnel et $\mathbf{K}$ contient l'ensemble des rationnels $\mathbf{Q}$ (comme tout sous-corps de $\mathbf{C}$), donc $U_r \in \mathbf{K}[X]$. Enfin α est racine du polynôme Q irréductible dans $\mathbf{K}[X]$. Le théorème d'irréductibilité d'Abel conclut alors que U_r est multiple de Q.
En particulier, si l'on note $(\alpha_i)_{i=1\ldots q}$ les racines de Q (dans $\mathbf{C}$), alors $U_r(\alpha_i) = 0$ pour $i = 1 \ldots q$.

Posons alors, pour tout $i = 1 \ldots q$, $V_i(X) = P(X) - \psi(X,\alpha_i)\phi(X,\alpha_i)$. Pour tout rationnel r, $V_i(r) = U_r(\alpha_i) = 0$ d'après ce que l'on vient de montrer. En particulier, $V_i(X)$ admet un nombre infini de racines et est donc nul. Donc pour tout i de $1 \ldots q$:

$$P(X) = \psi(X,\alpha_i)\phi(X,\alpha_i)$$

Multiplions membre à membre cette égalité pour $i = 1 \ldots q$:

$$P^q(X) = \Psi(X)\Phi(X) \text{ où l'on pose } \left\{ \begin{array}{lcl} \Psi(X) & = & \prod_{i=1}^{q} \phi(X,\alpha_i) \\ \Phi(X) & = & \prod_{i=1}^{q} \psi(X,\alpha_i) \end{array} \right.$$

Soit alors c un coefficient quelconque de Ψ ou de Φ. c s'exprime comme la valeur prise par un certain polyôme symétrique C à q variables et à coefficients dans $\mathbf{K}$, en $(\alpha_1, \ldots, \alpha_q)$ [1]
Or $\alpha_1, \ldots, \alpha_q$ sont les racines de Q, donc il existe, d'après le thèorème de Waring 6.8, un polynôme à $q+1$ variables et à coefficients dans $\mathbf{K}$, dont la valeur prise en $(Q_0, \ldots, Q_q)$ est c (on note Q_k le coefficient de degré k de Q). Comme les coefficients de Q appartiennent tous à $\mathbf{K}$, on en conclut $c \in \mathbf{K}$.
C'est valable pour tout coefficient c de Ψ ou Φ, donc $\Psi \in \mathbf{K}[X]$ et $\Phi \in \mathbf{K}[X]$.

Or P est irréductible dans $\mathbf{K}[X]$ et $P^q = \Psi\Phi$, donc il existe deux entiers positifs u et v tels que $\Psi = P^u$ et $\Phi = P^v$, avec $u+v=q$. [2]
Les degrés respectifs de $\psi(X,Y)$ et de $\phi(X,Y)$ par rapport à X étant m et n, on conclut donc :

$$\left\{ \begin{array}{lcll} qm & = & up & \text{car } \Psi = P^u \\ qn & = & vp & \text{car } \Phi = P^q \end{array} \right.$$

En particulier p divise qm. Or, comme $m+n=p$, avec $m>0$, $n>0$, on a $0<m<p$, et comme p est premier, il est premier avec m. Donc p divise q. CQFD. ∎

4 Démonstration du théorème de Kronecker

4.1 Modélisation d'une résolution par radicaux

Soit un polynôme P à coefficients rationnels, de degré n premier. Pour exprimer par radicaux une racine ω de l'équation $P(x) = 0$, on s'autorise les opérations qui suivent : addition, soustraction, multiplication, division, conjugaison et extraction d'une racine k-ième (comme tout entier est décomposable en produit de facteurs premiers, on peut se limiter à k premier). Si n est premier, on peut en particulier utiliser les racines n-ièmes de l'unité.

[1] C'est facile à voir en remplaçant $\alpha_1 \ldots \alpha_q$ par des indéterminées $Y_1 \ldots Y_q$ et en constatant que $C(Y_1, \ldots, Y_q)$ est invariant par une permutation quelconque des indéterminées.

[2] Prenons en effet u et v les plus grands tels que P^u divise Ψ et P^v divise Φ. Les conditions de degré imposent $u+v \leq q$. D'autre part il existe deux polynômes U et V de $\mathbf{K}[X]$ tels que $\Psi = P^u U$ et $\Phi = P^v V$, donc par intégrité de $\mathbf{K}[X]$:

$$P^{q-u-v} = UV$$

Si l'on avait $u+v<q$, alors P diviserait UV. Or P étant irréductible dans $\mathbf{K}[X]$, il diviserait U ou V, ce qui entraînerait que P^{u+1} divise Ψ ou que P^{v+1} divise Φ. Ceci contredirait alors le fait que u et v sont les plus grands possibles.

Mathématiquement, on peut traduire tout ça par la construction d'une suite $(\mathbf{K}_i)_{i=0,\dots,M}$ de sous-corps de $\mathbf{C}$, telle que :

$$\begin{array}{l}\mathbf{K}_0 = \mathbf{Q}\\ \mathbf{K}_1 = \mathbf{Q}(\eta) \text{ où } \eta = e^{i\frac{2\pi}{n}}\\ \forall i \geq 1, \mathbf{K}_{i+1} = \mathbf{K}_i(\lambda)\end{array}$$

où λ est une racine k-ième d'un élément de $\mathbf{K}_i$, telle que k soit premier et que K ne soit puissance k-ième d'aucun élément de $\mathbf{K}_i$. [3]
La construction de la suite se poursuit jusqu'à l'étape M, où $\omega \in \mathbf{K}_M$.

P est réductible dans $\mathbf{K}_M$, donc il existe un plus petit indice $N \leq M$ tel que P soit réductible dans $\mathbf{K}_N$.
Remarquons que $N > 1$. En effet, P n'est pas réductible dans $\mathbf{K}_0$ par hypothèse. D'autre part, si P était réductible dans $\mathbf{K}_1 = \mathbf{K}_0(\eta)$, le lemme 3.6 imposerait que tout polynôme irréductible $Q \in \mathbf{K}_0[X]$ dont η est racine ait un degré multiple de n. Or η est racine du polynôme $1 + X + \ldots + X^{n-1}$ [4] , donc le degré de Q serait inférieur ou égal à $n-1$, ce qui serait une contradiction flagrante.

4.2 Expression des racines de P

On va maintenant supposer que $P(X)$ est irréductible dans $\mathbf{Q}[X]$, qu'il est unitaire et que son degré n est premier et impair.

Soit $\mathbf{L}$ un sous-corps de $\mathbf{C}$ contenant η. Soient $K \in \mathbf{L}$, k premier et $\lambda \notin \mathbf{L}$ tels que $\lambda^k = K$ et que $\mathbf{L}$ ne contienne aucune racine k-ième de K.
Supposons P réductible dans $\mathbf{L}(\lambda)$ mais pas dans $\mathbf{L}$. Le lemme 3.6 impose alors que k soit multiple de n. Or k est premier, donc $k = n$.

P se décompose, dans $\mathbf{L}(\lambda)$, en un produit de facteurs irréductibles de degré m strictement inférieur à n et supérieur ou égal à 1. Soit Φ l'un de ces facteurs. D'après le lemme 3.5, il existe des polynômes $\Phi_0, \ldots, \Phi_m$ de $\mathbf{L}[X]$ et de degré au plus $n-1$, tels que :

$$\Phi(X) = \Phi_0(\lambda) + \Phi_1(\lambda)X + \ldots + \Phi_m(\lambda)X^m$$

On peut supposer Φ unitaire, donc $\Phi_m = 1$.

$$\text{Posons : } \left\{\begin{array}{l}\Psi(X,Y) = \Phi_0(Y) + \Phi_1(Y)X + \ldots + \Phi_m(Y)X^m\\ \forall i \in \{0\ldots n-1\}, \psi_i(X) = \Psi(X, \lambda_i) \text{ où } \lambda_i = \lambda\eta^i\end{array}\right.$$

Montrons que les $(\psi_i)_{i=0\ldots n-1}$ sont deux à deux distincts.
Supposons en effet qu'il existe $\nu \in \{0\ldots n-1\}$ et $\mu \in \{0\ldots n-1\}$ tels que $\nu \neq \mu$ et $\psi_n u = \psi_m u$.
Alors $\Psi(X, \eta^\nu\lambda) = \Psi(X, \eta^\mu\lambda)$. De l'égalité de ces polynômes découlerait celle de leurs coefficients :

$$\forall j \in \{0\ldots n-1\}, \quad \Phi_j(\eta^\nu\lambda) = \Phi_j(\eta^\mu\lambda)$$

Alors, en posant $A_j(X) = \Phi_j(\eta^\nu X)$ et $B_j(X) = \Phi_j(\eta^\mu X)$, on aurait $A_j(\lambda) = B_j(\lambda)$.
Or, comme $\mathbf{L}$ contient η, A_j et B_j sont à coefficients dans $\mathbf{L}$; en outre, ils sont de degré au plus $n-1$ car Φ_j l'est. Il découlerait donc du lemme 3.5 que $A_j(X) = B_j(X)$. C'est vrai pour tout $j \in \{0\ldots m\}$ donc $\Psi(X, \eta^\nu Y) = \Psi(X, \eta^\mu Y)$, ou encore :

$$\Psi(X,Y) = \Psi(X, hY) \text{ où } h = \eta^{\mu-\nu}$$

[3] Ce n'est pas une restriction gênante : si l'on veut que $\mathbf{K}_{i+1}$ contienne α tel que $\alpha^k = K_0$ et $\alpha \notin \mathbf{K}_i$, on peut procéder comme suit :

- ou bien il n'existe aucun $\lambda_0 \in \mathbf{K}_i$ tel que $\lambda_0^k = K_0$: on peut alors prendre $\lambda = \alpha$ et $K = K_0$.
- ou bien il existe $\lambda_0 \in \mathbf{K}_i$ tel que $\lambda_0^k = K_0$. S'il existait $\rho \in \mathbf{K}_i$ tel que $\rho^k = \eta$, alors $r = \rho^n$ serait une racine k-ième de 1. Comme $r \neq 1$ et k est premier, r serait une racine k-ième primitive de 1, et K_i contiendrait donc toutes les racines k-ièmes de 1. Or $\lambda_0 \in \mathbf{K}_i$, donc $\mathbf{K}_i$ contiendrait aussi toutes les racines k-ièmes de K_0, dont en particulier α. Ceci contredirait $\alpha \notin \mathbf{K}_i$.

Donc η n'est puissance k-ième d'aucun élément de $\mathbf{K}_i$. On peut donc prendre $K = \eta$ et $\lambda = e^{\mathbf{i}\frac{2\pi}{kn}}$. Le raisonnement ci-dessus montre alors que $\alpha \in \mathbf{K}_{i+1}$.

[4] En effet, η est dirrérent de 1, et racine du polynôme $X^n - 1$ qui se factorise en $(X-1)(1 + X + \ldots + X^{n-1})$

Par récurrence sur $i = 0 \dots n-2$: $\Psi(X, h^i Y) = \Psi(X^{i+1} Y) = \Psi(X, Y)$
En particulier, $\Psi(X, Y) = \frac{1}{n}\left[\Psi(X, h^0 Y) + \dots + \Psi(X, h^{n-1} Y)\right]$
Comme $h = \eta^{\nu-\mu}$ est racine n-ième de 1 (car $|\nu - \mu| \leq n-1$ et $\nu \neq \mu$), elle est primitive (puisque n est premier). Donc $h^i \lambda$ décrit $\{\lambda_0, \dots, \lambda_{n-1}\}$ quand i décrit $\{0 \dots n-1\}$. On pourrait alors conclure :

$$\Phi(X) = \frac{1}{n}\left[\Psi(X, \lambda_0) + \dots + \Psi(X, \lambda_{n-1})\right]$$

Chaque coefficient de Φ s'exprimerait donc comme la valeur prise en $(\lambda_0, \dots, \lambda_{n-1})$ par un certain polynôme symétrique à coefficients dans $\mathbf{L}$. Comme $(\lambda_0, \dots, \lambda_{n-1})$ sont les racines de $X^n - K$ dont les coefficients sont aussi dans $\mathbf{L}$, le théorème de Waring permettrait de conclure que chaque coefficient de Φ est dans $\mathbf{L}$. C'est absurde puisque P est irréductible dans $\mathbf{L}$.

Montrons qu'aucun des $(\psi_i)_{i=0\dots n-1}$ n'est réductible dans $\mathbf{L}(\lambda)$. Supposons en effet que pour un certain indice i_0, ϕ_{i_0} soit réductible dans $\mathbf{L}(\lambda)$. Comme λ_0 et λ sont tous deux racines n-ièmes de $K \in \mathbf{L}$, et comme $\mathbf{L}$ contient η, il existe deux polynômes u et v, à coefficients dans $\mathbf{L}$, tels que $\Psi(X, \lambda_0) = u(X, \lambda_{i_0}) v(X, \lambda_{i_0})$. En raisonnant comme dans la preuve du lemme 3.6, on montre que pour tout $i \in \{0 \dots n-1\}$, $\Psi(X, \lambda_i) = u(X, \lambda_i) v(X, \lambda_i)$. En particulier $\Psi(X, \lambda) = u(X, \lambda) v(X, \lambda)$. Alors $\Psi(X) = \Psi(X, \lambda)$ serait réductible dans $\mathbf{L}(\lambda)$, alors qu'il était justement censé y être irréductible : absurde.

Montrons que les $(\psi_i)_{i=0\dots n-1}$ sont tous des diviseurs de P.
Il existe un polynôme $U \in \mathbf{L}(\lambda)[X]$ tel que $P(X) = \Phi(X) U(X)$. Il existe donc un polynôme $V \in \mathbf{L}[X, Y]$ tel que $U(X) = V(X, \lambda)$, i.e. tel que $P(X) = \Psi(X, \lambda) V(X, \lambda)$.
En utilisant (encore !) la technique de la preuve du lemme 3.6, on montre alors que $\forall i \in \{0 \dots n-1\}, P(X) = \Psi(X, \lambda) V(\lambda_i)$. Or $\psi_i(X) = \Psi(X, \lambda_i)$ donc c'est bien un diviseur de P.

Résumons : les $(\psi_i)_{i=0\dots n-1}$ sont n facteurs irréductibles de P dans $\mathbf{L}(\lambda)$, deux à deux distincts. Comme $\Phi_m = 1$, ils sont en outre tous unitaires et de même degré $m \geq 1$.
Ces polynômes unitaires, irréductibles et distincts sont premiers deux à deux, donc le produit $\psi_0 \dots \psi_{n-1}$ divise P. P est en particulier de degré au moins mn. Or $m \geq 1$ et P est de degré n, donc $m = 1$ et le produit $\psi_0 \dots \psi_{n-1}$ est unitaire et de degré n.
Enfin, P étant unitaire, on conclut $P = \psi_0 \dots \psi_{n-1}$. Alors, par définition des $(\phi_i)_{i=0\dots n-1}$ et de Φ :

$$P(X) = (X + \Phi_0(\lambda_0))(X + \Phi_0(\lambda_1)) \dots (X + \Phi_0(\lambda_{n-1}))$$

donc les $(\omega_i)_{i=0\dots n-1}$, où $\omega_i = -\Phi_0(\lambda_i)$, sont les racines de P.
En particulier, il existe des éléments $\alpha_0, \dots, \alpha_{n-1}$ de $\mathbf{L}(\lambda)$ tels que :

$$\forall i \in \{0 \dots n-1\}, \omega_i = \alpha_0 \lambda_i^0 + \alpha_1 \lambda_i^1 + \dots + \alpha_{n-1} \lambda_i^{n-1}$$

Remarque : Ce résultat montre en particulier que toutes les racines de P appartiennent à $\mathbf{L}(\lambda)$.
Remarque : Etant donnée une racine ω quelconque de P, on peut, quitte à remplacer Φ par l'un des ψ_i, supposer $\omega = \alpha_0 \lambda^0 + \dots + \alpha_{n-1} \lambda^{n-1}$.

4.3 Localisation des racines de P

Le résultat démontré en 4.2 montre qu'à l'étape N on extrait une racine n-ième.

Moyennant quelques contraintes supplémentaires (et nullement pénalisantes) sur le choix des racines k-ièmes ajoutées à chaque étape [5] , de la construction de $(\mathbf{K}_i)_{i=0\dots M}$, on peut supposer que l'on se trouve dans l'un des deux cas suivants : • (a) : $N \geq 3$, $\mathbf{K}_N = \mathbf{K}_{N-1}(\lambda)$ et $\mathbf{K}_{N-1} = \mathbf{K}_{N-2}(\overline{\lambda})$ avec

[5] On peut par exemple imposer, pour tout $i \geq 1$:
(1) Si $\mathbf{K}_{i+1} = \mathbf{K}_i(\lambda)$ avec $\lambda^k = K$ et $K \neq \eta$, alors $\mathbf{K}_i$ contient les racines k-ièmes de 1.
(2) Si $\mathbf{K}_{i+1} = \mathbf{K}_i(\lambda)$ et $(\lambda) \notin \mathbf{K}_{i+1}$, alors $\mathbf{K}_{i+2} = \mathbf{K}_{i+1}(\overline{\lambda})$.
On montre alors par récurrence sur $i \geq 2$ que $\mathbf{K}_i$ ou $\mathbf{K}_{i-1}$ est stable par conjugaison (H_i).
• (H_1) est vraie, car $\mathbf{K}_1 = \mathbf{Q}(\eta)$ et $\eta^{n-1} = \overline{\eta}$ donc $\mathbf{K}_1$ est stable par conjugaison.
• Supposons (H_i) vraie pour i fixé. Alors :
1) ou bien $\mathbf{K}_i$ est stable par conjugaison, donc (H_{i+1}) est vraie.
2) ou bien $\mathbf{K}_{i-1}$ est stable par conjugaison, et $\mathbf{K}_i$ ne l'est pas.
Remarquons $\overline{\lambda} \notin \mathbf{K}_i$, sinon $\mathbf{K}_i = \mathbf{K}_{i-1}(\lambda, \overline{\lambda})$ serait stable par conjugaison. En particulier, $K \neq \eta$, sinon on aurait $\overline{\lambda} = \lambda^{nk-1} \in \mathbf{K}_i$.

$\lambda^n = K \in \mathbf{K}_{N-2}$ et $\forall x \in \mathbf{K}_{N-2}, \overline{x} \in \mathbf{K}_{N-2}$.

- $(b) : N \geq 2$, $\mathbf{K}_N = \mathbf{K}_{N-1}(\lambda)$ avec $\lambda^n = K \in \mathbf{K}_{N-1}$ et $\forall x \in \mathbf{K}_{N-1}, \overline{x} \in \mathbf{K}_{N-2}$.

Posons $\mathbf{L} = \mathbf{K}_{N-2}$ dans le cas (a), $\mathbf{L} = \mathbf{K}_{N-1}$ dans le cas (b).
Alors P est irréductible dans $\mathbf{L}$, qui est un sous-corps de $\mathbf{C}$, stable par conjugaison et contenant les racines n-ièmes de 1 (puisque $\mathbf{K}_1$ les contient).

P est à coefficients rationnels (en particulier réels) et de degré impair, donc il admet au moins une racine réelle ω. Appelons $\omega_0, \dots \omega_{n-1}$ les racines de P, avec $\omega_0 = \omega$.

- Si $K \in \mathbf{R}$: comme n est impair et comme les racines n-ièmes de 1 ont dans $\mathbf{K}_N$, on peut supposer $\lambda \in \mathbf{R}$.

Alors $\overline{\lambda} = \lambda$, donc c'est le cas (b) qui s'applique.

D'après 4.2, il existe alors des éléments $\alpha_0, \dots, \alpha_{n-1}$ de $\mathbf{L}$ tels que pour tout $i \in \{0 \dots n-1\}$:

$$\omega_i = \alpha_0 \lambda_i^0 + \alpha_1 \lambda_i^1 + \dots + \alpha_{n-1} \lambda_i^{n-1} \text{ où } \lambda_i = \lambda \eta^i$$

Comme ω est réel, $\overline{\omega} = \omega$, donc $(\alpha_0 - \overline{\alpha_0}) + (\alpha_1 - \overline{\alpha_1})\lambda + \dots + (\alpha_{n-1} - \overline{\alpha_{n-1}})\lambda^{n-1} = 0$.
Or λ est racine de $X^n - K$, qui est irréductible dans $\mathbf{L}$, donc le polynôme ci-dessus à coefficients dans $\mathbf{L}$, est multiple de $X^n - K$, d'après le théorème d'Abel 3.4.
Comme il est au plus de degré $n-1$, il est donc nul, d'où : $\forall j \in \{0 \dots n-1\}, \alpha_j = \overline{\alpha_j}$, i.e. $\alpha_j \in \mathbf{R}$.
Or pour tout $i = 1 \dots n-1$, $\left\{ \begin{array}{lcl} \omega_i & = & \alpha_0 + \alpha_1 \lambda \eta^i + \alpha_2 (\lambda \eta^i)^2 + \dots + \alpha_{n-1} (\lambda \eta^i)^{n-1} \\ \omega_{n-i} & = & \alpha_0 + \alpha_1 \lambda \eta^{n-i} + \alpha_2 (\lambda \eta^{n-i})^2 + \dots + \alpha_{n-1} (\lambda \eta^{n-i})^{n-1} \end{array} \right.$ En remarquant que $\eta^{n-i} = \overline{\eta}$, et comme on vient de montrer $\alpha_j \in \mathbf{R}$ pour tout $j \in \{0 \dots n-1\}$, on conclut $\omega_i = \overline{\omega_{n-i}}$.
Si, pour $i \in \{1 \dots n-1\}$, ω_i était réel, on aurait alors $\omega_i = \overline{\omega_i} = \omega_{n-i}$, ce qui conduirait à l'existence d'une racine double de P.
Mais P est irréductible dans $\mathbf{L}$, donc toutes ses racines sont simples [6] donc c'est impossible.
On conclut donc que toutes les racines de P sont réelles.

- Si $K \notin \mathbf{R}$, alors P est réductible dans $\mathbf{L}(\lambda, \overline{\lambda})$ et pas dans $\mathbf{L}$.

En posant $a = \lambda\overline{\lambda}$, on remarque que $\mathbf{L}(\lambda, \overline{\lambda}) = \mathbf{L}(a, \lambda)$.

Si P est réductible dans $\mathbf{L}(a)$, on est ramené au cas $K \in \mathbf{R}$ [7].

Sinon, P est réductible dans $\mathbf{L}(a)(\lambda)$ et pas dans $\mathbf{L}(a)$. Comme au paragraphe ci-dessus, on montre que K n'est puissance n-ième d'aucun élément de $\mathbf{L}(a)$.

D'après 4.2, il existe n éléments $\alpha_0, \dots, \alpha_{n-1}$ de $\mathbf{L}(a)$ tels que :

$$\omega = \alpha_0 + \alpha_1 \lambda + \dots + \alpha_{n-1} \lambda^{n-1}$$

Comme $\omega = \overline{\omega}$ et $\overline{\lambda} = \frac{a}{\lambda}$, on en tire : $\alpha_0 + \alpha_1 \lambda + \dots + \alpha_{n-1} \lambda^{n-1} = \overline{\alpha_0} + \overline{\alpha_1} \frac{a}{\lambda} + \dots + \overline{\alpha_{n-1}} \left(\frac{a}{\lambda}\right)^{n-1}$.
En multipliant par λ^{n-1}, on constate que λ est racine du polynôme :

$$\begin{array}{rcl} Q(X) & = & \alpha_{n-1} X^{2n-2} + \alpha_{n-2} X^{2n-3} + \alpha_1 X^n + (\alpha_0 - \overline{\alpha_0}) X^{n-1} \\ & & -\overline{\alpha_1} a X^{n-2} - \overline{\alpha_2} a^2 X^{n-3} - \dots - \overline{\alpha_{n-1}} a^{n-1} X^0 \end{array}$$

Ce polynôme est à coefficients dans $\mathbf{L}(a)$ [8]. Or les $(\lambda_i)_{i=0 \dots n-1}$ sont les racines de $X^n - K$, qui est

Alors la règle (1) impose que $\mathbf{K}_{i-1}$ (et donc $\mathbf{K}_i$) contienne les racines k-ièmes de 1. Si $\overline{K}$ était puissance k-ième d'un élément λ_0 de $\mathbf{K}_i$, $\mathbf{K}_i$ contiendrait alors toutes les racines k-ièmes de $\overline{K}$, dont $\overline{\lambda}$: absurde.
D'autre part, $\mathbf{K}_{i-1}$ est stable par conjugaison donc $\overline{K} \in \mathbf{K}_{i-1}$ et par conséquent $K \in \mathbf{K}_i$.
Donc prendre $\mathbf{K}_{i+1} = \mathbf{K}_i(\overline{\lambda})$ respecte la relation de récurrence de la suite. Alors $\mathbf{K}_{i+1} = \mathbf{K}_{i-1}(\lambda, \overline{\lambda})$ est stable par conjugaison, et (H_{i+1}) est donc vraie.

[6] Sinon, le pgcd de P et de sa dérivée P' serait de degré au moins 1, ce qui contredirait l'irréductibilité de P dans $\mathbf{L}$.

[7] a est en effet racine n-ième de $K\overline{K}$, qui ne peut être puissance n-ième d'aucun élément de $\mathbf{L}$ (sinon, comme $\eta \in \mathbf{L}$, $a \in \mathbf{L}$ donc $\mathbf{L} = \mathbf{L}(a)$; absurde car P est irré ductible dans $\mathbf{L}$) ; on est alors ramené au cas $K \in \mathbf{R}$ traité ci-dessus (remplacer K par $K\overline{K}$)

[8] en effet, a et $\alpha_0, \dots, \alpha_{n-1}$ appartiennent à $\mathbf{L}(a)$; de plus, $\mathbf{L}$ est stable par conjugaison et $a \in \mathbf{R}$, donc $\mathbf{L}(a)$ aussi est stable par conjugaison

irréductible dans $\mathbf{L}(a)$, donc Q est multiple de $X^n - K$. En particulier, pour tout $i \in \{0 \dots n-1\}$:

$$Q(\lambda_i) = 0$$

On divise par $(\lambda_i)^{n-1}$, et on remarque que $\frac{a}{\lambda_i} = \frac{\lambda\overline{\lambda}}{\lambda\eta^i} = \overline{\lambda}\overline{\eta}^i = \overline{\lambda_i}$, d'où :

$$\alpha_0 + \alpha_1\lambda_i^1 + \ldots + \alpha_{n-1}\lambda_i^{n-1} = \overline{\alpha_0} + \overline{\alpha_1}\overline{\lambda_i}^1 + \ldots + \overline{\alpha_{n-1}}\overline{\lambda_i}^{n-1}$$

On reconnaît à gauche l'expression de ω_i, à droite celle de $\overline{\omega_i}$. Donc $\omega_i = \overline{\omega_i}$, c'est-à-dire $\omega_i \in \mathbf{R}$.
C'est vrai pour tout $i \in \{0 \dots n-1\}$, donc toutes les racines de P sont réelles.

4.4 Enoncé du théorème de Kronecker

En regroupant les résultats de la section précédente, on arrive au théorème de Kronecker :

Théorème 4.1 (Théorème de Kronecker) *Soit P un polynôme à coefficients dans $\mathbf{Q}$, irréductible dans $\mathbf{Q}$, de degré n premier et impair. Si l'une des racine de P est exprimable par radicaux, alors le nombre des racines réelles distinctes de P est 1 ou n.*

Remarque : Le fait que les racines soient distinctes vient directement du fait que P est irréductible dans $\mathbf{Q}$.
D'autre part, d'aucuns se demanderont où est passée l'hypothèse "P unitaire" : on peut s'en passer, car si on divise P par son coefficient dominant, on obtient un polynôme à coefficients dans $\mathbf{Q}$, unitaire et qui a les mêmes racines que l'original.

5 Déduction du théorème d'Abel

5.1 Le théorème d'Abel

Théorème 5.1 (Théorème d'impossibilité d'Abel) *Il existe des polynômes à coefficients rationnels, de degré $n \geq 5$, dont on ne peut exprimer aucune racine par radicaux.*

Preuve : Il suffit d'exhiber un tel polynôme. Prenons par exemple $P(X) = x^5 - 6x - 2$.
C'est un polynôme unitaire à coefficients entiers. A part le coefficient dominant, tous ses coefficients sont multiples du nombre premier 2, et 2^2 n'est pas diviseur du coefficient constant 2.
Le théorème d'irréductibilité de Schœnemann nous assure alors que P est irréductible dans $\mathbf{Q}$.
D'autre part, P est de degré 5, qui est premier et impair.
Supposons que P possède une racine exprimable par radicaux. Le théorème de Kronecker nous dit qu'il possède 1 ou 5 racines réelles distinctes.
Or, une étude de fonction montre immédiatement que P possède exactement 3 racines réelles.
C'est une belle contradiction, qui démontre du même coup le théorème. CQFD. ∎

5.2 Commentaires

Le théorème d'Abel implique en particulier qu'il n'existe pas de formule générale (du moins par radicaux) donnant, en fonction de ses coefficients, les racines d'un polynôme de degré supérieur ou égal à 5.

Malheureusement, il ne dit pas quand une équation polynomiale est soluble par radicaux.
Le théorème de Kronecker, que l'on a utilisé au cours de la démonstration, ne donne en effet qu'une condition nécessaire pour cela.
Les travaux de Galois ont permis de trouver des critères de résolubilité par radicaux, mais c'est hors de portée de cet article.

6 L'essentiel des polynômes symétriques

Définition 6.1 (Degré, degré partiel, poids d'un monôme) *Soit un monôme* $M = \beta X_1^{\alpha_1} \dots X_n^{\alpha_n}$, *avec* $\beta \neq 0$

- *Pour tout* $k \in \{1 \dots n\}$, α_k *est appelé degré partiel du monôme par rapport à l'indéterminée* X_k. *On le note* $\mathrm{dp}_{X_k}(M)$.
- *La somme* $\alpha_1 + \dots + \alpha_n$ *est le degré du monôme.*
- *La somme* $\alpha_1 + 2\alpha_2 + \dots + n\alpha_n$ *est le poids du monôme.*
- *Par convention (commode), si* $\beta = 0$, *alors degré et degré partiel valent* $-\infty$, *avec : pour tout entier* α, $\alpha > -\infty$ *et* $-\infty + \alpha = -\infty$.

Soit un polynôme P *à* n *indéterminées.*

- *Pour tout* $k \in \{1 \dots n\}$, *on appelle degré partiel de* P *par rapport à* X_k *le plus grand des degrés partiels, par rapport à* X_k, *de ses monômes. On le note* $\mathrm{dp}_{X_k}(P)$
- *On appelle degré de* P *le plus grand des degrés de ses monômes.*
- *On appelle poids de* P *le plus grand des poids de ses monômes.*

Définition 6.2 (Polynôme symétrique) *Soit un polynôme* P *à* n *indéterminées* $X_1, \dots, X_n$. *Ce polynôme est dit symétrique si et seulement si, pour toute permutation* φ *des entiers* $1, \dots, n$, $P(X_1, \dots, X_n) = P(X_{\varphi(1)}, \dots, X_{\varphi(n)})$.

Remarque : Pour les polynômes symétriques, le degré partiel par rapport à chacune des indéterminées est identique, donc on parle du degré partiel, tout court, et on se contente de le noter $\mathrm{dp}(P)$.

Définition 6.3 (Polynômes symétriques élémentaires) *Soit un entier* $n \geq 1$. *Pour tout entier* $i \in \{1 \dots n\}$, *on appelle* i*-ème fonction symétrique élémentaire à* n *indéterminées et on note* Σ_i^n *le polynôme formé par la somme de tous les produits possibles de* i *indéterminées sur* n *:* $\Sigma_i^n = \sum_{1 \leq k_1 < k_2 < \dots < k_i \leq n} X_{k_1} X_{k_2} \dots X_{k_i}$

Exemple : Pour $n = 3$: $\Sigma_1^3 = X_1 + X_2 + X_3$, $\Sigma_2^3 = X_1X_2 + X_1X_3 + X_2X_3$, $\Sigma_3^3 = X_1X_2X_3$

Lemme 6.4 (Degré d'une somme ou d'un produit de polynômes) *Soient deux polynômes* P *et* Q, *à* n *indéterminées, et à coefficients dans un anneau* $\mathbf{A}$ *commutatif intègre. Alors :* $\begin{cases} \mathrm{degre}(P+Q) & \leq & \max\{\mathrm{degre}(P \\ \mathrm{degre}(PQ) & = & \mathrm{degre}(P) + \end{cases}$

Preuve : Si un coefficient de $P + Q$ est non-nul, alors l'un au moins des coefficients correspondants de P ou de Q est non-nul, ce qui démontre le lemme pour la somme.
Si P ou Q est nul, alors $PQ = 0$ donc $\mathrm{degre}(PQ) = -\infty$ donc le lemme est vrai.
Pour le produit c'est moins évident : soient P et Q sont non-nuls et de degrés respectifs p et q. Prenons, parmi les coefficients non-nuls de degré p de P, celui qui a le plus grand indice $\alpha = (\alpha_1, \dots, \alpha_n)$ pour l'ordre lexicographique [9] . On procède de même pour extraire de Q le coefficient d'indice $\beta = (\beta_1, \dots, \beta_n)$ et de degré q.
L'ordre lexicographique est compatible avec l'addition, donc le coefficient d'indice $\gamma = \alpha + \beta$ du produit $R = PQ$ est le produit de P_α et Q_β [10] . Or $\mathbf{A}$ est intègre, donc ce produit est non-nul. Or il est de degré $p + q$, donc $R = PQ$ est au moins de degré $p + q$. Enfin, il est clair que PQ est de degré inférieur ou égal à $p + q$, donc le lemme est démontré.CQFD. ∎

Lemme 6.5 *Soit un polynôme* P *à* n *indéterminées, et soient* n *polynômes* $Q_1, \dots, Q_n$, *tels que pour* $k = 1, \dots, n$, $\mathrm{degre}(Q_k) = k$. *Alors le degré de* $P(Q_1, Q_2, \dots, Q_n)$ *est inférieur ou égal au poids de* P.

Preuve : Le degré d'un produit $Q_1^{\alpha_1} \dots Q_n^{\alpha_n}$ est inférieur ou égal au poids du monôme $X_1^{\alpha_1} \dots X_n^{\alpha_n}$. On applique ça à chaque monôme de P et c'est gagné. ∎

[9] Pour deux n-uplets d'entiers $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$, on dit que $x \leq y$ pour l'ordre lexicographique si et seulement si $x = y$ ou si, pour le plus petit indice i tel que $x_i \neq y_i$, on a $x_i < y_i$. On vérifie alors facilement qu'il s'agit d'une relation d'ordre (Pour tout x, $x \leq x$; Si $x \leq y$ et $y \leq x$ alors $x = y$; Si $x \leq y$ et $y \leq z$ alors $x \leq z$), qu'elle est totale (on a toujours $x \leq y$ ou $y \leq x$) et qu'elle est compatible avec l'addition (Si $x \leq y$ et $x' \leq y'$ alors $x + x' \leq y + y'$).

[10] On peut expliciter ce "donc" : Soient deux indices ρ et φ tels que $P_\rho Q_\varphi$ apparaisse dans l'expression de R_γ. Ces indices correspondent obligatoirement à des termes de degrés p et q. Par définition de α et β, on a alors $\rho \leq \alpha$ et $\varphi \leq \beta$. Donc, si $\rho < \alpha$ ou $\varphi < \beta$, alors $\rho + \varphi < \alpha + \beta$, ce qui serait absurde puisque l'on doit avoir $\rho + \varphi = \gamma = \alpha + \beta$. Donc $\rho \geq \alpha$ et $\varphi \geq \beta$, et comme on a déjà les inégalités $\rho \leq \alpha$ et $\varphi \leq \beta$, on conclut $\rho = \alpha$ et $\varphi = \beta$.

Théorème 6.6 (Polynôme symétrique et symétriques élémentaires) *Soit un anneau commutatif* $\mathbf{A}$*, et soit un polynôme symétrique à n indéterminées* $P \in \mathbf{A}[X_1, \ldots, X_n]$*. Alors il existe un polynôme* $Q \in \mathbf{A}[X_1, \ldots, X_n]$*, de poids inférieur ou égal au degré de* P*, tel que* $P = Q(\Sigma_1^n, \ldots, \Sigma_n^n)$*.*

Remarque : On peut de plus montrer que Q est unique, et que $\text{degre}(Q) \leq \text{dp}(P)$, mais on n'en a pas besoin ici.

Preuve : On peut procéder par récurrence sur le nombre d'indéterminées n.
Soit $H(n)$ la proposition : "Le théorème est vrai pour tous les polynômes à n indéterminées ou moins".

- $H(1)$ est vraie : il suffit de prendre $Q = P$.
- Soit $n \geq 1$ et supposons $H(n)$ vraie. Soit P un polynôme symétrique à $n+1$ indéterminées. On va montrer par récurrence sur le degré de P que $H(n+1)$ est vraie.

Soit $G(d)$ la proposition : "H(n+1) est vraie pour les polynômes de degré inférieur ou égal à d".

- Si $d = 0$, alors P est constant et $Q = P$ suffit.
- Prenons $d \geq 0$ et supposons $G(d)$ vraie.

Supposons P de degré $d+1$. Posons $P_1 = P(X_1, \ldots, X_n, 0)$. C'est un polynôme symétrique à n indéterminées, dont le degré est inférieur ou égal à celui de P. Comme $H(n)$ est vraie, il existe un polynômes Q_1, tel que $P_1 = Q_1(\Sigma_1^n, \ldots, \Sigma_n^n)$, avec $\text{poids}(Q_1) \leq \text{degre}(P_1) \leq \text{degre}(P)$. Posons $P_2 = P_1 - Q_1(\Sigma_1^{n+1}, \ldots, \Sigma_n^{n+1})$. P_2 est symétrique, et $\text{degre}(P_2) \leq \text{Max}\{\text{degre}(P_1), \text{poids}(Q_1)\} \leq \text{degre}(P)$. Par construction, on a $P_2(X_1, \ldots, X_n, 0) = 0$, et comme il est symétrique, on a pour tout entier j tel que $1 \leq j \leq n$,

$$P_2(X_1, \ldots, X_{j-1}, 0, X_{j+1}, \ldots, X_{n+1}) = 0$$

et est donc multiple de X_j. Donc P_2 est multiple de $X_1 \ldots X_{n+1}$, qui n'est autre que Σ_{n+1}^{n+1}. Il existe donc un polynôme P_3 tel que $P_2 = \Sigma_{n+1}^{n+1} P_3$. P_2 est symétrique donc P_3 aussi.
On a alors : $\text{degre}(P_3) = \text{degre}(P_2) - (n+1)$ donc $\text{degre}(P_3) \leq (d+1) - (n+1)$. On peut alors appliquer $G(d)$: il existe un polynôme Q_2 à $n+1$ indéterminées, tel que $\text{poids}(Q_2) \leq \text{degre}(P_3) \leq (d+1) - (n+1)$, avec $P_3(X_1, \ldots, X_{n+1}) = Q_2(\Sigma_1^{n+1}, \ldots, \Sigma_{n+1}^{n+1})$.Alors :

$$P = Q_1(\Sigma_1^n, \ldots, \Sigma_n^n) + \Sigma_{n+1}^{n+1} Q_2(\Sigma_1^{n+1}, \ldots, \Sigma_{n+1}^{n+1})$$

En conclusion, $Q(X_1, \ldots, X_{n+1}) = Q_1(X_1, \ldots, X_n) + X_{n+1} Q_2(X_1, \ldots, X_{n+1})$ convient, et avec les remarques faites sur les poids de Q_1 et Q_2, on conclut que $\text{poids}(Q) \leq \text{degre}(P)$. Donc $G(d+1)$ est vraie.

- Par récurrence sur d, $G(d)$ est donc vraie pour tout entier d. Du coup, on a montré la véracité de $H(n+1)$, ce qui achève la première récurrence. CQFD. ∎

Théorème 6.7 (Relation coefficients-racines d'un polynôme) *Soit un corps commutatif* $\mathbf{K}$ *et soit* P *un polynôme scindé sur* K*, de degré* n*, dont le coefficient de degré* i *est noté* p_i*. Alors, si l'on note* $\omega_1, \ldots, \omega_n$ *les racines de* P *dans* $\mathbf{K}$*, on a la relation :*

$$\forall i \in \{0 \ldots n-1\}, \frac{p_i}{p_n} = (-1)^{n-i} \Sigma_{n-i}^n(\omega_1, \ldots, \omega_n)$$

Preuve : On peut écrire P sous la forme : $P(X) = p_n(X - \omega_1) \ldots (X - \omega_n)$. En développant, on constate que, pour $i = 0 \ldots n-1$, le terme de degré i est la somme de tous les produits possibles de $n - i$ racines, multipliée par $(-1)^i$ et par p_n. On reconnaît la définition de $\Sigma_{n-i}^n(\omega_1, \ldots, \omega_n)$et on en conclut le résultat annoncé. ∎

Théorème 6.8 (Waring) *Soient un corps commutatif* $\mathbf{K}$*,* $\mathbf{A}$ *un sous-anneau de* $\mathbf{K}$*, et* P *un polynôme unitaire de degré* n *à coefficients dans* $\mathbf{A}$*, possédant* n *racines* $\omega_1, \ldots, \omega_n$ *dans* $\mathbf{K}$*.*
Soit Q *un polynôme symétrique à* n *indéterminées et à coefficients dans* $\mathbf{A}$*.*
Alors $Q(\omega_1, \ldots, \omega_n) \in \mathbf{A}$*.*

Preuve : Q est symétrique, donc il existe un polynôme R à coefficients dans $\mathbf{A}$ tel que :

$$Q = R(\Sigma_1^n, \ldots, \Sigma_n^n)$$

Notons $p_0, \ldots, p_n$ les coefficients de P. D'après les relations entre coefficients et racines, on a pour tout $i \in \{1, \ldots, n\}$:

$$\Sigma_i^n(\omega_1, \ldots, \omega_n) = (-1)^i p_{n-i} \text{ car } p_n = 1$$

Donc $Q(\omega_1, \ldots, \omega_n) = R((-1)^1 p_{n-1}, \ldots, (-1)^n p_0)$. Or les coeficients $p_0, \ldots, p_{n-1}$ appartiennent à l'anneau $\mathbf{A}$, et les coefficients de R aussi, donc $Q(\omega_1, \ldots, \omega_n) \in \mathbf{A}$. CQFD. ∎

Remarque : Si $\mathbf{A}$ est un sous-corps de $\mathbf{K}$, il n'est plus nécessaire que P soit unitaire car, en divisant tous ses coefficients par p_n, on obtient un polynôme Q unitaire dont les coefficients sont encore dans $\mathbf{A}$ et qui a les mêmes racines que P. On peut alors appliquer le théorème à Q.