Equation générale de degré n

1 Equation de degrée n

Tous les corps considérés dans ce chapitre seront de caractéristique nulle. Soit $b_1,...,b_s$ des éléments d'une extension d'un corps K.

Définition On dira que les éléments $b_1,...,b_s$ sont **algébriquement indépendants** sur K si, et seulement si, ces éléments ne satisfont aucune relation de la forme

$$\sum \alpha_{i_1 i_2 ... i_s} b_1^{i_1} ... b_s^{i_s} = 0$$

à coefficients non nuls.

Autrement dit, $b_1,...,b_s$ sont algébriquement indépendants si, et seulement si, ils n'annulent aucun polynôme non nul $P(X_1,...,X_s) \in K[X_1,...,X_s]$ à n indéterminées.

Exemple Si a est transcendant sur K et b est transcendant sur $K(a)$, alors a,b sont algébriquement indépendants sur K, car si nous avons

$$\sum_{i,j} \alpha_{i,j} a^i b^j = 0$$

alors

$$\sum_j \left(\sum_i \alpha_{ij} a^i \right) b^j = 0$$

Mais b est transcendant sur $K(a)$, d'où

$$\sum_i \alpha_{ij} a^i = 0 \text{ pour tout } j$$

a est aussi transcendant sur K. Les relations précédentes impliquent $\alpha_{ij} = 0$ pour tout i et tout j ce qui prouve l'indépendance algébrique de a et b sur K.

Définition L'**équation générale de degré** n sur un corps K est une équation de la forme

$$x^n + a_{n-1}x^n + \cdots + a_1 x + a_0 = 0$$

où les coefficients $a_0,a_1,...,a_{n-1}$ sont algébriquement indépendants sur K.

Soit $F = K(a_0,a_1,...,a_{n-1})$ et $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$. Nous avons $f(X) \in F[X]$ et $F \simeq K(Y_1,...,Y_n)$ corps des fractions rationnelles en n idéterminées $Y_1,...,Y_n$ et à coefficients dans K. Soit $u_1,u_2,...,u_n$ les racines de f dans un corps des racines $F(u_0,u_1,...,u_{n-1})$ pour f sur F.

Théorème $u_1,u_2,...,u_n$ sont algébriquement indépendants sur K.

Démonstration Sinon, soit

$$\sum \alpha_{i_1 i_2 \ldots i_n} u_1^{i_1} \ldots u_n^{i_n} = 0$$

une relation de dépendance algébrique sur K. Posons

$$P(X_1,\ldots,X_n) = \sum \alpha_{i_1 i_2 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$$

Ce polynôme non nul satisfait $P(u_1,u_2,\ldots,u_n) = 0$. Considérons le polynôme

$$H(X_1,\ldots,X_n) = \prod_{\sigma \in S_n} P\left(X_{\sigma(1)},\ldots,X_{\sigma(n)}\right)$$

Le polynôme H est visiblement symétrique. La théorie des polynômes symétriques nous apprend qu'il existe un polynôme unique $Q(X_1,\ldots,X_n)$ dans $K[X_1,\ldots,X_n]$ tel que

$$H(X_1,\ldots,X_n) = Q(\Sigma_1,\ldots,\Sigma_n)$$

où $\Sigma_1,\Sigma_2,\ldots,\Sigma_n$ sont les polynômes symétriques élémentaires

$$\begin{aligned}
\Sigma_1 &= X_1 + X_2 + \cdots + X_n \\
\Sigma_2 &= X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n \\
\Sigma_3 &= X_1X_2X_3 + \cdots + X_{n-2}X_{n-1}X_n \\
&\vdots \\
\Sigma_n &= X_1X_2\cdots X_n
\end{aligned}$$

La relation $P(u_1,u_2,\ldots,u_n) = 0$ implique $H(u_1,u_2,\ldots,u_n) = 0$ et par suite $Q(\Sigma'_1,\ldots,\Sigma'_n) = 0$ où $\Sigma'_i = \Sigma_i(u_1,u_2,\ldots,u_n)$. Or $\Sigma'_i = (-1)^i a_{n-i}$. Il en résulte

$$Q(-a_{n-1},a_{n-2},-a_{n-3},\ldots,(-1)^n a_0) = 0$$

Mais, les éléments $a_0,\ldots,a_{n-1}$ sont algébriquement indépendants sur K. Ceci implique $Q = 0$ et par suite $H = 0$ et $P = 0$.

Corollaire Les racines $u_1,u_2,\ldots,u_n$ sont distinctes.

Démonstration Car si $u_i = u_j$, alors $u_i - u_j = 0$ est une relation de dépendence algébrique sur K satisfaites par les éléments $u_1,u_2,\ldots,u_n$.

Théorème $K(u_1,u_2,\ldots,u_n) = F(u_1,u_2,\ldots,u_n)$

Démonstration Nous avons

$$\begin{aligned}
F(u_1,u_2,\ldots,u_n) &= K(a_0,\ldots,a_{n-1})(u_1,u_2,\ldots,u_n) \\
&= K(a_0,\ldots,a_{n-1},u_1,u_2,\ldots,u_n) \\
&= K(u_1,u_2,\ldots,u_n)
\end{aligned}$$

car les coefficients a_i peuvent s'exprimer en fonction des racines $u_1,...,u_n$ par l'intermédiaire des polynômes symétriques élémentaires.

Théorème Le groupe de Galois G du polynôme f est isomorphe au groupe symétrique S_n.

Démonstration Il suffit de prouver que G est le groupe $S(A)$ de toute les permutations de l'ensemble $A = \{u_1,u_2,...,u_n\}$ des racines de f car ce groupe de permutations est isomorphe au groupe S_n. Soit $\sigma \in G$. $\sigma \in S(A)$ car elle permute les racines $u_1,u_2,...,u_n$ de f. Réciproquement, soit t une permutation de $A = \{u_1,u_2,...,u_n\}$ et soit

$$\sigma; K[u_1,u_2,...,u_n] \longrightarrow K[u_1,u_2,...,u_n]$$

l'application définie par

$$\sigma(g(u_1,u_2,...,u_n)) = g(t(u_1),...,t(u_n))$$

σ est bien définie car tout élément de $K[u_1,u_2,...,u_n]$ s'écrit d'une manière unique sous la forme $g(u_1,u_2,...,u_n)$. Il est aisé de prouver que σ est un K-automorphisme de l'anneau $K[u_1,u_2,...,u_n]$. Il peut être prolongé en un K-automorphisme τ du corps $K(u_1,u_2,...,u_n)$, corps des fractions de l'anneau $K[u_1,u_2,...,u_n]$. Il nous reste à prouver que τ est un F-automorphisme de $K(u_1,u_2,...,u_n)$. Mais τ laisse fixe tout élément a_i car a_i est une fonction symétrique des racines $u_1,u_2,...,u_n$. Ainsi, τ appartient au groupe de Galois G de f sur F.

Corollaire L'équation générale de degré n n'est pas résoluble par des radicaux pour $n \geq 5$.

Démonstration Pour $n \geq 5$, le groupe de Galois de l'équation générale de degré n est isomorphie à S_n qui est non résoluble.

2 Discriminant

Soit

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$$

l'équation générale de degré n sur un corps K.

Définition Soit $P = K(a_0,a_1,...,a_{n-1})$ et R un corps des racines sur P pour le polynôme

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

Le groupe de Galois de f est isomorphe à S_n. Soit $u_1,u_2,...,u_n$ les racines de f dans R. On appelle **discriminant** de f l'élément $D = \Delta^2$ où Δ est l'élément $\prod_{i<j}(u_i - u_j) \in R$.

Exemple Le discriminant de l'équation générale de degré 2 sur K est

$$D = \Delta^2 = (u_0 - u_1)^2 = a_1^2 - 4a_0$$

Théorème $\sigma(\Delta) = \pm\Delta$ pour tout $\sigma \in G(R/P)$.

Démonstration Nous avons

$$\sigma(\Delta) = \sigma\left(\prod_{i<j}(u_i - u_j)\right) = \prod_{i<j}(\sigma(u_i) - \sigma(u_j)) = \varepsilon(\sigma)\Delta = \pm\Delta$$

où $\varepsilon(\sigma)$ est la signature de la permutation σ.

Corollaire $\Delta^2 \in P$.

Démonstration Car $\sigma\left(\Delta^2\right) = \sigma(\Delta)^2 = \Delta^2$ pour tout $\sigma \in G(R/P)$.

Théorème Le corps des éléments laissés fixe par le groupe alterné A_n est $P(\Delta)$.

Démonstration Soit L le corps des éléments laissés fixes par A_n. Nous avons $A_n = G(R/L)$. L'extension L de P est normale, car $A_n = G(R/L)$ est un sous-groupe distingué de $S_n = G(R/P)$. En plus, le groupe de Galois $G(L/P)$ est isomorphe au groupe quotient S_n/A_n qui est un groupe d'ordre 2. Ainsi $[L:P] = 2$. L'élément Δ est invariant par chaque élément de A_n car $\sigma(\Delta) = \pm\Delta$. Il en résulte $\Delta \in L$ et $[P(\Delta):P] = 2$. D'où $L = P(\Delta)$.

3 Equation de degré 2

Cette équation est de la forme

$$x^2 + bx + c = 0$$

Nous avons $u_0 - u_1 = \Delta$ et $u_0 + u_1 = b$. En résolvant le système linéaire

$$\begin{cases} u_0 - u_1 = \Delta \\ u_0 + u_1 = b \end{cases}$$

nous obtenons

$$u_0 = \frac{-b + \Delta}{2} \text{ et } u_1 = \frac{-b - \Delta}{2}$$

4 Equation de degré 3

Cette équation es de la forme

$$x^3 + a_2x^2 + a_1x + a_0 = 0$$

En posant $y = x - \dfrac{a_2}{3}$, nous obtenons

$$x^3 + px + q = 0$$

Le discriminant de cette équation est

$$\Delta = -4p^3 - 27q^2$$

Son groupe de Galois, identifié à S_3, est résoluble et

$$S_3 \supseteq A_3 \supseteq \{e\}$$

est une chaîne normale à facteurs abéliens de S_3. Il correspond à cette chaîne par la correspondance de Galois, la chaîne suivante de corps intermédiaires

$$P \subseteq P(\Delta) \subseteq R$$

Le groupe de Galois de l'extension R de $P(\Delta)$ est A_3. Mais A_3 est un groupe cyclique d'ordre 3. Il est engendré par le cycle (123). Il en résulte que le groupe de Galois $G(R/P(\Delta))$ est engendré par le $P(\Delta)$-automorphisme σ de R qui vérifie

$$\sigma(u_1) = u_2,\ \sigma(u_2) = u_3 \text{ et } \sigma(u_3) = u_1$$

Ainsi, $[P(\Delta)(u_1) : P(\Delta)] = 3$ et $R = P(\Delta)(u_1) = P(\Delta,u_1)$.

On applique la méthode de la résolvante de Lagrange. Nous avons

$$\begin{aligned}
\beta_1 &= u_1 + z\sigma(u_1) + z^2\sigma^2(u_1) = u_1 + zu_2 + z^2u_3\\
\beta_2 &= u_1 + z^2u_2 + zu_3\\
\beta_3 &= u_1 + u_2 + u_3
\end{aligned}$$

Un calcul assez complexe nous donne

$$\begin{aligned}
\beta_1^3 &= \left(u_1 + zu_2 + z^2u_3\right)^3 = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\Delta\\
\beta_2^3 &= -\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\Delta\\
\beta_1\beta_2 &= -3p
\end{aligned}$$

Donc, u_1,u_2,u_3 forment une solution du système linéaire suivant

$$\begin{cases}
u_1 + u_2 + u_3 = 0\\
u_1 + zu_2 + z^2u_3 = \beta_1\\
u_1 + z^2u_2 + zu_3 = \beta_2
\end{cases}$$

Pour résoudre ce système, nous devons calculer β_1 et β_2. Parmi les solutions possibles, on choisit celle qui vérifie $\beta_1\beta_2 = -3p$. La résolution du système linéaire nous donne alors

$$u_0 = \frac{\beta_1+\beta_2}{3},\ u_1 = \frac{z^2\beta_1+z\beta_2}{3} \text{ et } u_2 = \frac{z\beta_1+z^2\beta_2}{3}$$

Exemple Pour résoudre l'équation de degré 3 suivante

$$x^3 - 5x^2 + 19x + 25 = 0$$

on pose $y = x - \frac{5}{3}$. Nous obtenons l'équation suivante

$$x^3 + \frac{32}{3}x + \frac{1280}{27} = 0$$

Le discriminant de cette équation est

$$\Delta^2 = -4p^3 - 27q^2 = -4\left(\frac{32}{3}\right)^3 - 27\left(\frac{1280}{27}\right)^2 = -65536$$

D'où

$$\beta_1^3 = \left(4\left(\sqrt{3}+1\right)\right)^3 \text{ et } \beta_2^3 = \left(-4\left(\sqrt{3}-1\right)\right)^3$$

et $\beta_1\beta_2 = -3p = -32$. On en déduit

$$\beta_1 = 4\left(\sqrt{3}-1\right) \text{ et } \beta_2 = -4\left(\sqrt{3}+1\right)$$

ce qui donne

$$\begin{aligned} u_0 &= \frac{\beta_1+\beta_2}{3} = -\frac{8}{3} \\ u_1 &= \frac{z^2\beta_1+z\beta_2}{3} = \frac{4}{3} - i \\ u_2 &= \frac{z\beta_1+z^2\beta_2}{3} = \frac{4}{3} + i \end{aligned}$$

et

$$\begin{aligned} x_0 &= u_0 + \frac{5}{3} = -1 \\ x_1 &= u_1 + \frac{5}{3} = 3 - 4i \\ x_2 &= u_2 + \frac{5}{3} = 3 + 4i \end{aligned}$$

5 Equation de degré 4

Cette équation est de la forme suivante

$$x^4+a_3x^3+a_2x^2+a_1x+a_0=0$$

En posant $y=x-\dfrac{a_3}{4}$, nous obtenons

$$x^4+px^2+qx+r=0$$

Le discriminant de cette équation est

$$\Delta=16p^4r-4p^3q^3-128p^2r^2+144pq^2r-27q^4+256r^3$$

Le groupe de Galois de cette équation, identifié à S_4, est résoluble et

$$S_4\supseteq A_4\supseteq V\supseteq W\supseteq\{e\}$$

Où

$$V=\{e,u=(12)(34),v=(13)(24),t=(14)(23)\},W=\{e,u\}$$

est une chaîne normale à facteurs abéliens de S_4. Il lui correspond, par la correspondance de Galois, la chaîne suivante de corps intermédiaires

$$P\subseteq P(\Delta)\subseteq L_1\subseteq L_2\subseteq R$$

Nous avons

$$G(R/P(\Delta))\simeq A_4,\ G(R/L_1)\simeq V,\ G(R/L_2)\simeq W$$

et

$$[R:P]=24,\ [R:P(\Delta)]=12,\ [R:L_1]=4,\ [R:L_2]=2$$
$$[L_2:L_1]=2,[L_2:P(\Delta)]=6,[L_1:P(\Delta)]=3 \text{ et } [P(\Delta):P]=2$$

L_1 est engendré sur $P(\Delta)$ par un élément invariant par tous les $\sigma\in V$. Mais cet élément est modifié par au moins un élément de A_4. Considérons l'élément $\theta=(u_0+u_1)(u_2+u_3)$. Cet élément vérifie

$$u(\theta)=(u_1+u_0)(u_3+u_2)=\theta$$
$$v(\theta)=(u_2+u_3)(u_0+u_1)=\theta$$
$$t(\theta)=(u_3+u_2)(u_1+u_0)=\theta$$

Donc $\theta\in L_1$. d'un autre côté, $\sigma=(123)\in A_4$ et $\sigma(\theta)\neq\theta$ ce qui prouve $\theta\notin P(\Delta)$. D'où $L_1=P(\Delta)(\theta)=P(\Delta,\theta)$. Le polynôme minimal de θ sur $P(\Delta)$ est le polynôme ayant comme racines les $\sigma(\theta)$ pour tout élément σ de $A_4=G(R/P(\Delta))$. Mais

$$A_4=\left\{\begin{array}{c}e,(123),(124),(134),(234),(132),(142),(143),\\(243),(13)(24),(14)(23),(12)(34)\end{array}\right\}$$

Calculant ces image de θ, nous obtenons

$$\begin{aligned}\theta_1 &= \theta\\ \theta_2 &= (u_0+u_2)(u_1+u_3)\\ \theta_3 &= (u_0+u_3)(u_1+u_2)\end{aligned}$$

Or ces images sont les racines de l'équation

$$(x-\theta_1)(x-\theta_2)(x-\theta_3) = x^3 - b_1x^2 + b_2x - b_3 = 0$$

avec

$$\begin{aligned}b_1 &= \theta_1+\theta_2+\theta_3 = 2p\\ b_2 &= \theta_1\theta_2+\theta_1\theta_3+\theta_2\theta_3 = p^2-4r\\ b_3 &= \theta_1\theta_2\theta_3 = -q^2\end{aligned}$$

Cette équation de degré 3 est appelée **la résolvante cubique** de l'équation de degré 4. Le polynôme minimal de θ sur $P(\Delta)$ est donc le polynôme $X^3-b_1X^2+b_2X-b_3$. θ_1 et θ_2 appartiennent à L_1 car ils sont invariants par tous les éléments de $V = G(R/L_1)$.

L_2 est engendré sur L_1 par un élément de degré 2. Si $\lambda = u_1+u_2$, alors λ est invariant par tous les éléments de W mais transformé par l'élément v de V car nous avons

$$v(\lambda) = u_3+u_4 \neq \lambda \quad (u_1+u_2+u_3+u_4 = 0)$$

Donc $\lambda \in L_1$ et $\lambda \notin L_2$. Il en résulte $L_2 = L_1(\lambda)$ et la chaîne des corps intermédiaires devient

$$P \subseteq P(\Delta) \subseteq P(\Delta,\theta) \subseteq P(\Delta,\theta,\lambda) \subseteq R$$

Pour calculer les racines u_1,u_2,u_3,u_4 en fonction de $\theta_1,\theta_2,\theta_3$, nous avons

$$\begin{cases}(u_1+u_2)(u_3+u_4) = \theta_1\\ u_1+u_2+u_3+u_4 = 0\end{cases}$$

Ces deux équations nous donnent

$$\begin{cases}u_1+u_2 = \sqrt{-\theta_1}\\ u_3+u_4 = -\sqrt{-\theta_1}\end{cases}$$

De même, nous avons

$$\begin{cases}u_1+u_3 = \sqrt{-\theta_2}\\ u_2+u_4 = -\sqrt{-\theta_2}\end{cases}$$

et

$$\begin{cases}u_1+u_4 = \sqrt{-\theta_3}\\ u_2+u_3 = -\sqrt{-\theta_3}\end{cases}$$

Le choix de $\sqrt{-\theta_1},\sqrt{-\theta_2},\sqrt{-\theta_3}$ doit satisfaire

$$\left(\sqrt{-\theta_1}\right)\left(\sqrt{-\theta_2}\right)\left(\sqrt{-\theta_3}\right) = (u_1+u_2)(u_1+u_3)(u_1+u_4) = -q$$

Nous obtenons

$$u_1 = \frac{1}{2}\left(\sqrt{-\theta_1}+\sqrt{-\theta_2}+\sqrt{-\theta_3}\right)$$
$$u_2 = \frac{1}{2}\left(\sqrt{-\theta_1}-\sqrt{-\theta_2}-\sqrt{-\theta_3}\right)$$
$$u_3 = \frac{1}{2}\left(\sqrt{-\theta_1}+\sqrt{-\theta_2}-\sqrt{-\theta_3}\right)$$
$$u_4 = \frac{1}{2}\left(\sqrt{-\theta_1}-\sqrt{-\theta_2}+\sqrt{-\theta_3}\right)$$

Exemple Soit à résoudre l'équation de degré 4 suivante

$$x^4 - 2x^3 + 4x^2 + 2x - 5 = 0$$

En posant $y = x - \frac{1}{2}$, nous obtenons

$$y^4 + \frac{5}{2}y^2 + 5y - \frac{51}{16} = 0$$

La résolvante cubique est

$$x^3 - 5x^2 + 19x + 25 = 0$$

Les racines de cette équation de degré 3 sont

$$\theta_1 = -1, \theta_2 = 3 - 4i \text{ et } \theta_3 = 3 + 4i.$$

Nous avons

$$\sqrt{-\theta_1} = \pm 1$$
$$\sqrt{-\theta_2} = \sqrt{4i-3} = \pm(1+2i)$$
$$\sqrt{-\theta_3} = \sqrt{-3-4i} = \pm(1-2i)$$

La condition

$$\left(\sqrt{-\theta_1}\right)\left(\sqrt{-\theta_2}\right)\left(\sqrt{-\theta_3}\right) = (u_1+u_2)(u_1+u_3)(u_1+u_4) = -q = -5$$

nous donne $\sqrt{-\theta_1} = 1, \sqrt{-\theta_2} = 1+2i$ et $\sqrt{-\theta_3} = 2i-1$. Les racines de l'équation en y sont

$$y_0 = \frac{1}{2} + 2i, y_1 = \frac{1}{2} - 2i, y_2 = \frac{1}{2} \text{ et } y_3 = -\frac{3}{2}$$

On en déduit les racines de l'équation initiale en x. Ces racines sont

$$x_0 = 1 + 2i, x_1 = 1 - 2i, x_2 = 1 \text{ et } x_3 = -1$$