Résolubilité par des radicaux

1 Groupe de Galois d'un polynôme

Dans ce chapitre, tous corps considérés sont de caractéristique nulle. Soient K une corps et f un polynôme dans $K[X]$.

Définition On appelle **groupe de Galois** du polynôme f sur le corps K le groupe de Galois $G(E/K)$ où E est un corps des racines pour f sur K. Il sera noté $G_K(f)$.

Lemme Soit $f \in K[X]$ et M une extension de K. Le groupe $G_M(f)$ est isomorphe à un sous-groupe de $G_K(f)$.

Démonstration Soit N un corps des racines pour f sur M. On a $N = M(a_1,...,a_n)$ où $a_1,...,a_n$ sont les racines de f dans N. Le corps $E = K(a_1,...,a_n)$ est un corps de racines pour f sur K. Si $\sigma \in G(N/M)$, alors sa restriction à E est un $K-$automorphisme de E car E est une extension normale de K. Soit $\varphi; G(N/M) \longrightarrow G(E/K)$ l'application qui associe à chaque $\sigma \in G(N/M)$ sa restriction à E. φ est un homomorphisme de groupes. Il est injectif car si $\varphi(\sigma) = id_E$, alors $\sigma(a_i) = a_i$ pour tout i. Il en résulte $\sigma = id_M$. Ainsi $G(N/M)$ est isomorphe à $\mathrm{Im}(\varphi)$ qui est un sous-groupe de $G(E/K)$.

Soit $f \in K[X]$ et $L = K(a_1,...,a_n)$ un corps des racines pour f sur K, où $a_1,...,a_n$ sont les racines de f dans L. Tout $\sigma \in G(L/K)$ permute les racines de f. D'un autre côté, deux $K-$automorphismes σ et τ de L sont égaux si, et seulement si, $\sigma(a_i) = \tau(a_i)$ pour tout i. Ainsi le groupe de Galois de f peut être regardé comme un sous-groupe de du groupe des permutations de ses racines. Nous avons alors

Lemme Soit $f \in K[X]$. Le groupe de Galois de f sur K est isomorphe à un sous-groupe du groupe symétrique S_n où n est le nombre des racines distinctes de f.

2 Polynômes résolubles et leurs groupes de Galois

Définition On dit qu'un polynôme $f \in K[X]$ est **résoluble par des radicaux** si, et seulement si, les racines de f dans un corps des racines peuvent être construites à partir des coefficients de f en un nombre fini d'étapes faisant intervenir les quatre opérations élémentaires $+,-,\times,\div$ et l'extraction de racines $n^{ièmes}$ pour des entiers naturels appropriés n.

Il découle de cette définition, qu'un polynôme $f \in K[X]$ est résoluble par des radicaux si, et seulement si, il existe des corps $K_0,K_1,...,K_m$ tels que $K_0 = K$, le polynôme f est scindé dans $K_m[X]$ et pour tout entier i entre1et m, le corps K_i est obtenu à partir du corps K_{i-1}, par l'adjonction d'un élément $\alpha_i \in K_i$ qui vérifie $\alpha_i^{p_i} \in K_{i-1}$ pour

un certain entiers positif p_i. En plus, nous pouvons supposer les p_i premiers car si $n = p_1 p_2 ... p_{k-1} p_k$, où les p_i sont premiers, et si α est une racine $n^{ième}$ de a, on adjoint α en adjoignant successivement $\alpha^{p_1}, (\alpha^{p_1})^{p_2}, ..., (((\alpha^{p_1}))...)^{p_k} = \alpha$.

On se propose de démontrer le résultat fondamental suivant

Théorème *$f \in K[X]$ est résoluble par radicaux si, et seulement si, son groupe de Galois $G_K(f)$ est résoluble.*

Définition Soit L un corps et p un nombre premier. Supposons le polynôme $X^p - 1$ scindé dans $L[X]$. Ce polynôme ne possède que des racines simples car aucune de ses racines n'est une racine commune avec le polynôme dérivé pX^{p-1}. Un élément $\omega \in L$ est une **racine $p^{ième}$ primitive** de l'unité si, et seulement si, $\omega \neq 1$ et est une racine du polynôme $X^p - 1$. Les racines $p^{ièmes}$ primitives de l'unité sont donc les racines du polynôme

$$X^{p-1} + X^{p-1} + \cdots + X + 1.$$

Théorème L'ensemble des racines $p^{ièmes}$ primitives de l'unité dans L forme un groupe cyclique engendré par n'importe laquelle de ces racines.

Lemme Soit K un corps et p un nombre premier. Si ω est une racine $p^{ième}$ primitive de l'unité dans une extension de K, alors le groupe de Galois de l'extension $K(\omega)$ de K est abélien.

Démonstration Soit $L = K(\omega)$ et soient $\sigma,\tau \in G(L/K)$. $\sigma(\omega)$ et $\tau(\omega)$ sont des racines du polynôme $X^p - 1$. Il existe deux entiers a et b tels que $\sigma(\omega) = \omega^a$ et $\tau(\omega) = \omega^b$. Il en résulte

$$\begin{aligned}(\sigma \circ \tau)(\omega) = \sigma(\tau(\omega)) = \sigma\left(\omega^b\right) = (\sigma(\omega))^b = (\omega^a)^b = \omega^{ab} \\ = \left(\omega^b\right)^a = (\tau(\omega))^a = \tau(\omega^a) = \tau(\sigma(a)) = (\tau \circ \sigma)(a)\end{aligned}$$

ce qui prouve $\sigma \circ \tau = \tau \circ \sigma$ car $L = K(\omega)$.

Lemme Soit K un corps et M un corps des racines sur K pour le polynôme $X^p - c \in K[X]$ où p est un nombre premier. Le groupe de Galois de l'extension M de K est résoluble.

Démonstration Le résultat est trivial si c est nul. Supposons c non nul. Les racines du polynôme $X^p - c$ sont toutes non nulles et distinctes car la seule racine de son polynôme dérivé est nulle. Si α est une racine de ce polynôme et si ω est une racine $p^{ième}$ primitive de l'unité, alors les racines de $X^p - c$ sont $\alpha,\omega\alpha,\omega^2\alpha,...,\omega^{p-1}\alpha$. On

a alors $M = K(\alpha,\omega)$. Le corps $K(\omega)$ est un corps intermédiaire et est une extension normale de K car c'est un corps de racines pour $X^p - 1$ sur K. Il en résulte que le groupe $G(M/K(\omega))$ est un sous-groupe distingué du groupe $G(M/K)$ et que le groupe quotient $G(M/K)/G(M/K(\omega))$ est isomorphe à $G(K(\omega)/K)$. Or ce dernier est un groupe abelien, il suffit alors de prouver que le groupe $G(M/K(\omega))$ est abelien car, dans ce cas, la chaîne

$$\{i\} \subseteq G(M/K(\omega)) \subseteq G(M/K)$$

serait une chaîne normale à facteurs abélien de $G(M/K)$.

M est obtenu à partir de $K(\omega)$ par l'adjonction d'un élément α vérifiant $\alpha^p = c \in K$. Ainsi, tout $\sigma \in G(M/K(\omega))$ est parfaitement déterminé par son action sur α. En plus $\sigma(\alpha)$ est une racine de $X^p - c$. Il en résulte qu'il existe un entier a tel $\sigma(\alpha) = \alpha\omega^a$. De même, si $\tau \in G(M/K(\omega))$, il existe un entier b tel que $\tau(\alpha) = \alpha\omega^b$. On a alors

$$(\sigma \circ \tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma\left(\alpha\omega^b\right)$$
$$= \sigma(\alpha)\sigma\left(\omega^b\right) = \sigma(\alpha)\sigma(\omega)^b = c\omega^a\omega^b = \alpha\omega^{ab}$$
$$(\tau \circ \sigma)(\alpha) = \tau(\sigma(\alpha)) = \tau(\alpha\omega^a)$$
$$= \tau(\alpha)\tau(\omega^a) = \tau(\alpha)\tau(\omega)^a = c\omega^b\omega^a = \alpha\omega^{ab}$$

ce qui prouve $\sigma \circ \tau = \tau \circ \sigma$ et $G(M/K(\omega))$ est abelien.

Lemme Soit $f \in K[X]$ et soit $K' = K(\alpha)$ où $\alpha^p \in K$ pour un nombre premier p. Le groupe $G_K(f)$ est résoluble si, et seulement si, le groupe $G_{K'}(f)$ est résoluble.

Démonstration Soit N un corps des racines pour le polynôme $f(X)(X^p - c)$ sur K, où $c = \alpha^p \in K$. N contient un corps des racines L pour f sur K et un corps des racines M pour $X^p - c$ sur K. Les extensions N de K, L de K et M de K sont toutes galoisiennes. Les groupes $G(N/M)$ et $G(N/L)$ sont des sous-groupes distingués de $G(N/K)$. En plus le groupe $G(L/K)$ est isomorphe au groupe quotient $G(N/K)/G(N/L)$ et le groupe $G(M/K)$ est isomorphe au groupe quotient $G(N/K)/G(N/M)$. M et N sont des corps des racines pour le polynôme $X^p - c$ sur K et L respectivement. Il résulte du lemme précédent que $G(M/K)$ et $G(N/L)$ sont résolubles. Or nous savons que si H est un sous-groupe distingué d'un groupe G, alors G est résoluble si, et seulement si H et G/H le sont. Ainsi $G(N/K)$ est résoluble si, et seulement si, $G(N/M)$ est résoluble. De même, $G(N/K)$ est résoluble si, et seulement si, $G(L/K)$ est résoluble. Mais $G(N/M) \approx G_M(f)$ et $G(L/K) \approx G_K(f)$.Il en résulte que $G_M(f)$ est résoluble si, et seulement si, $G_K(f)$ est résoluble.

Maintenant M est aussi un corps des racines pour le polynôme $X^p - c$ sur K', car $K' = K(\alpha)$ où α est une racine de ce polynôme. Ainsi, le groupe $G_M(f)$ est résoluble si, et seulement si, le groupe $G_{K'}(f)$ est résoluble. Il en résulte que le groupe $G_K(f)$ est résoluble si, et seulement si, le groupe $G_{K'}(f)$ est résoluble.

Théorème Soit $f \in K[X]$. Si f est résoluble par des radicaux, alors son groupe de Galois $G_K(f)$ est résoluble.

Démonstration Si f est résoluble par des radicaux, alors il existe une suite K_0,K_1,...,K_m de corps tel que $K_0 = K$, f est scindé dans $K_m[X]$ et, pour i entre 1 et m, $K_i = K_{i-1}(\alpha_i)$ avec $\alpha_i^{p_i} \in K_{i-1}$ pour un nombre premier p_i. Le groupe $G_{K_m}(f)$ est résoluble car c'est le groupe réduit à l'identité de K_m. D'un autre côté, le lemme précédent montre que le groupe $G_{K_i}(f)$ est résoluble si, et seulement si, le groupe $G_{K_{i-1}}(f)$ est résoluble, et ce pour tout $i > 0$. Il en résulte que $G_K(f) = G_{K_0}(f)$ est résoluble.

Lemme Soit p un nombre premier, K un corps et L une extension galoisienne de degré p de K. On suppose que K contient une racine $p^{ième}$ primitive de l'unité. Alors il existe $\alpha \in L$ tel que $L = K(\alpha)$ et $\alpha^p \in K$.

Démonstration Le groupe $G(L/K)$ est un groupe cyclique car son ordre est un nombre premier. Soient σ un générateur de ce groupe et ω une racine $p^{ième}$ primitive de l'unité. Soit $b \in L - K$ et soit, pour $i = 0,1,...,p-1$,

$$\alpha_j = b + \omega^j \sigma(b) + \omega^{2j}\sigma^2(b) + \cdots + \omega^{(p-1)j}\sigma^{p-1}(b)$$

Cet élément est parfois appelé la **résolvante de Lagrange**. Nous avons $\sigma(\alpha_j) = \omega^{-j}\alpha_j$ pour $j = 0,1,...,p-1$, car $\sigma(\omega) = \omega$, $\sigma\left(\sigma^{p-1}(b)\right) = b$ et $\omega^p = 1$ Il en résulte $\sigma\left(\alpha_j^p\right) = \alpha_j^p$ et par suite $\alpha_j^p \in K$ pour $j = 0,1,...,p-1$. Mais

$$\alpha_0 + \alpha_1 + \cdots + \alpha_{p-1} = pb$$

car ω^j est une racine du polynôme $X^{p-1} + X^{p-2} + \cdots + X + 1$ pour tous les j non divisibles par p. Or $pb \in L - K$ car $b \in L - K$ et $p \neq 0$ dans K. Il en résulte qu'un des éléments α_0,α_1,...,α_{p-1} appartient à $L - K$. Soit $\alpha = \alpha_i$ un tel élément. $[K(\alpha) : K]$ divise $[L : K] = p$. On en déduite $[K(\alpha) : K] = p$ car p est premier et $\alpha \notin K$. Ainsi $L = K(\alpha)$ avec $\alpha^p \in K$.

Théorème Soit $f \in K[X]$ où K est un corps de caractéristique nulle. Si le groupe $G_K(f)$ est résoluble, alors f est résoluble par des radicaux.

Démonstration Soit ω une racine $p^{ième}$ primitive de l'unité où p est un nombre premier. Le groupe $G_{K(\omega)}(f)$ est isomorphe à un sous-groupe de $G_K(f)$ et est par suite résoluble. D'un autre côté, f est résoluble par des radicaux sur K si, et seulement si, f est résoluble par des radicaux sur $K(\omega)$ car $K(\omega)$ est obtenue à partir de K par adjonction d'un élément ω qui vérifie $\omega^p = 1 \in K$. Dès lors, on peut supposer que le corps K contient une racine $p^{ième}$ primitive de l'unité pour tous les diviseurs premiers de $n = Ord(G_K(f))$.

Le résultat est trivialement vrai pour $n = 1$ car dans ce cas f est scindé dans $K[X]$. Supposons la propriété vraie pour les extensions dont l'ordre du groupe de Galois est inférieur à n. Soit L un corps des racines pour f sur K. L est une extension galoisienne de K et $G(L/K) \approx G_K(f)$. Le groupe résoluble $G(L/K)$ possède un sous-groupe distingué H tel que le groupe quotient $G(L/K)/H$ soit cyclique d'ordre un nombre premier diviseur de $n = Ord(G_K(f))$. Soit M le corps des invariants de H. On a $H = G(L/M)$ et $G(M/K) \approx G(L/K)/H$. D'où $[M : K] = Ord(G(L/K)/H) = p$. Il en résulte que M

est de la forme $M = K(\alpha)$ pour un $\alpha \in M$ qui vérifie $\alpha^p \in K$. Comme $G_M(f) \approx H$ et H est résoluble, alors $G_M(f) = G(L/M)$ est résoluble. L'hypothèse de récurrence montre que f est résoluble par des radicaux sur M. Les racines de f se trouvent donc, dans une extension de M obtenue par adjonction successive de radicaux. Or M est obtenue à partir de K par l'adjonction du radical α, donc les racines de f se trouvent dans une extension de K obtenue par adjonction successive de radicaux. f est alors résoluble par des radicaux.