expo beamer

Algèbre M1-S1

groupe

22 novembre 2019

PLAN

INTRODUCTION

En mathématiques et plus particulièrement en Algèbre,on appelle un corps,un ensemble ayant une structure d'anneau dans lequel tout élément non nul admet un symétrique pour la seconde loi de composition.Il existe plusieurs corps :le corps des nombres rationnels $\mathbb{Q}$,le corps des nombres réels $\mathbb{R}$,le corps des nombres complexes $\mathbb{C}$,le corps $\mathbb{F}_p$ des congruences modulo p où p est un nombre premiers etc.Dans la première partie de notre travail nous nous intéresserons particulièrement aux corps cyclotomiques. Concernant la deuxième partie,on peut retenir que jusqu'au XIX-ième siècle, la résolution des équations algébriques, c'est-à-dire des équations polynomiales est pratiquement synonyme d'algèbre

Le plus important progrès a lieu au début du XVI-ième siècle avec la résolution, par les algébristes italiens (Scipion del Ferro, Tartaglia, Cardan) de l'équation du troisième degré par les formules dites maintenant de Cardan, par exemple pour l'équation $x^3 + ax = b$:

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{(\frac{b}{2})^2 + (\frac{a}{3})^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{(\frac{b}{2})^2 + (\frac{a}{3})^3}}$$

Cette expression, qui fait intervenir des racines carrées et cubiques est l'objectif de ce qu'on appelle une résolution par radicaux de l'équation proposée.

PREMIÈRE PARTIE : CORPS CYCLOTOMIQUES

1. Racine n'ième de l'unité

Définition

Soit $P \in K[X], K$ un corps commutatif,un polynôme s'écrivant sous la forme $P(X) = X^n - 1$ avec $n \in \mathbb{N}^*$.Les racines de P sont appelées racines nîème de l'unité.
L'ensemble de ces racines noté $G_n = \{X \in K / X^n = 1\}$ est un sous groupe cyclique de K pour la loi multiplicative et de cardinal n.

2. Racine primitive de l'unité

Définition

Une racine n-ième de l'unité est dite primitive quand elle est d'ordre exactement n , c'est-à-dire quand c'est un générateur de G_n.On note $P_n(K)$ l'ensemble des racines primitives nième de l'unité.
Pour $\mathbb{K} = \mathbb{C}$ *on a* $G_n = \{e^{(\frac{2ik\pi}{n})} \quad avec \quad k \in \{0, ..., n-1\}\}$

Racine primitive de l'unité

Proposition

L'ensemble des racines n-ièmes de l'unité
$G_n = \{e^{(\frac{2ik\pi}{n})} \quad avec \quad k \in \{0, ..., n-1\}\}$ *est un sous-groupe cyclique de* $\mathbb{C}^*$ *isomorphe à* $\mathbb{Z}/n\mathbb{Z}$

3.polynôme cyclotomique

Définition

Soit K un corps et n un entier qui n'est pas divisible par $car(K)$.On appelle n-ième polynôme cyclotomique de K le polynôme

$$\Phi_{n,K}(x) = \prod_{\alpha \in P_n(x)} (X - \alpha)$$

Quand $K = \mathbb{Q}$,on note plus simplement $\Phi_{n,K} = \Phi_n$.

Propriétés des polynômes cyclotomiques en caractéristique 0

Propriété

1. $\Phi_n(x) \in \mathbb{Z}[x]$
2. $\Phi_n(x)$ *est irréductible dans* $\mathbb{Q}[X]$*(donc dans* $\mathbb{Z}[X]$*)*
3. $deg(\Phi_n(x)) = \varphi(n)(= |\mathbb{Z}/n\mathbb{Z}^*|$ *par définition) avec* φ *l'indicateur d'Euler*
4. *Dans* $\mathbb{C}[x]$*,on a*

$$\Phi_n(x) = \prod_{k \in (Z/n\mathbb{Z})^*} (x - \alpha_n^k)$$

où $\alpha_n = e^{2\Pi i/n}$

Propriétés des polynômes cyclotomiques en caractéristique p

Propriété

1. *Si* $n = p^r - 1$, *alors* $\Phi_n(x)$ *est un produit de polynômes irréductibles de degré* r
2. *Si* n *et* p *sont premiers entre eux et* r *est l'ordre de* p *dans* $(\mathbb{Z}/n\mathbb{Z})^*$ *alors* $\Phi_n(x)$ *est un produit de polynômes irréductibles de degré* r
3. *Si* n *et* p *sont premiers entre eux, alors* $\Phi_{p^i n}(X) = \Phi_n(X)^{\varphi(p^i)}$

4.Extension cyclotomique

Définition

Une extension cyclotomique est une extension de la forme $K(\alpha_n)/K$ où K est un corps de caractéristique première à n et α_n une racine primitive n-ième de l'unité(dans un corps de décomposition de $X^n - 1$) sur K. Si $K = \mathbb{Q}$ alors $K(\alpha_n) = \mathbb{Q}(\alpha_n)$. Elle sera noté $\mathbb{Q}^{(n)}$ et s'appelle n-ième corps cyclotomique.
Autrement on appelle corps cyclotomique C_n, le corps de décomposition du polynôme cyclotomique Φ_n.

Propriété

Notons n l'ordre de α, c'est-à-dire que α est une racine primitive n-ième de l'unité, ou encore une racine du polynôme cyclotomique Φ_n.

1. *L'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est de degré $\varphi(n)$, où φ désigne la fonction indicatrice d'Euler.*
2. *L'extension cyclotomique est aussi le corps de décomposition du polynôme Φ_n. Elle est donc galoisienne.*

Démonstration.

2. L'extension contient α et donc toutes ses puissances, or les puissances de α forment l'ensemble des racines n-ièmes de l'unité et donc en particulier les racines primitives qui sont les racines du polynôme cyclotomique. Ceci démontre que $\mathbb{Q}(\alpha)$ est le corps de décomposition. Dans un corps parfait comme celui des rationnels (un corps parfait est un corps où tous les polynômes irréductibles sont séparables c'est-à-dire n'ont pas de racines multiples dans la clôture algébrique) un corps de décomposition est toujours une extension de Galois.

Proposition

Soient m et n deux entiers naturels non nuls. Si m et n sont premiers entre eux alors $\mathbb{Q}(\alpha_n\alpha_m) = \mathbb{Q}(\alpha_n, \alpha_m)$.

Démonstration.

En effet il est facile de voir que $\mathbb{Q}(\alpha_n\alpha_m) \subset \mathbb{Q}(\alpha_n, \alpha_m)$. D'autre part si m et n sont premiers entre eux alors il existe u et v deux entiers tels que $un + vm = 1$. Donc $\alpha_m = (\alpha_m\alpha_n)^{nu}$. De même $\alpha_n = (\alpha_n\alpha_m)^{vm}$.Et par suite $\mathbb{Q}(\alpha_n\alpha_m) = \mathbb{Q}(\alpha_n, \alpha_m)$. □

Corollaire

Soient m et n deux entiers naturels non nuls. Si m et n sont premiers entre eux alors $\mathbb{Q}(\alpha_n) \cap \mathbb{Q}(\alpha_m) = \mathbb{Q}$

Démonstration.

En effet on sait que si m et n sont premiers entre eux alors $U_{mn} \simeq U_m x U_n$ avec et par suite
$Gal(\mathbb{Q}(\alpha_{nm})/\mathbb{Q}) \simeq U_{mn} \simeq U_m x U_n \simeq Gal(\mathbb{Q}(\alpha_m)/\mathbb{Q}) x Gal(\mathbb{Q}(\alpha_n)/\mathbb{Q})$ qui permet de conclure que $\mathbb{Q}(\alpha_n) \cap \mathbb{Q}(\alpha_m) = \mathbb{Q}$ □

Groupe de Galois d'une extension cyclotomique

Théorème

1. *Soit une extension cyclotomique $K(\alpha_n)/K$ où K est un corps de caractéristique première à n et α_n une racine primitive n'ième de 1. Alors $K(\alpha_n)/K$ est galoisienne de groupe de galois isomorphe à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$*
2. *Soit $\alpha_n \in \mathbb{C}(x)$,$n$ éléments d'ordre n. L'extension $\mathbb{Q}^{(n)}/\mathbb{Q}$ est galoisienne de groupe de Galois $\simeq (\mathbb{Z}/n\mathbb{Z})^*$.*

Corollaire

Une extension cyclotomique est toujours abélienne

Démonstration.

Soit d un entier plus petit que n et premier à n. Alors α^d est une racine du polynôme cyclotomique donc il existe un $\mathbb{Q}$-automorphisme (évidemment unique) m_d du corps de décomposition ($\mathbb{Q}(\alpha)$) qui envoie α sur α^d. Considérons alors l'application du groupe multiplicatif des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ dans le groupe de Galois qui, à la classe de d associe l'automorphisme m_d. Cette application est clairement un isomorphisme de groupes. Cet isomorphisme montre que le groupe de Galois est abélien, ce qui termine la démonstration. □

DEUXIÈME PARTIE :ÉQUATIONS RÉSOLUBLES PAR RADICAUX

Définition

Une extension $K \subset L$ est dite radicale s'il existe une tour :
$K = K_0 \subset K_1 \subset ... \subset K_n = L$ avec, pour tout $i = 1, ..., n$, $K_i = K_{i-1}(\alpha_i)$
où α_i vérifie $\alpha_i^{n_i} = a_i \in K_{i-1}$, avec $n_i \in \mathbb{N}^*$.

Définition

Une extension $K \subset L$ est dite résoluble (sous-entendu par radicaux), s'il existe une extension M de L telle que $K \subset M$ soit radicale.

Définition

Soit $P \in K[X]$ un polynôme. On dit que l'équation $P(x) = 0$ est résoluble par radicaux si l'extension $K \subset D_K(P)$ est résoluble.

Remarque

Une équation est résoluble par radicaux si toutes ses racines s'écrivent à l'aide de radicaux. On pourrait imaginer une définition plus faible où l'on impose seulement qu'une des racines soit de cette forme.

Proposition

Soient $K \subset L \subset M$ des extensions.
1) Si M/K est radicale, M/L l'est aussi.
2) Si L/K et M/L sont radicales, M/K l'est aussi.

Proposition

Soit L/K une extension radicale et M une clôture normale de L sur K. Alors l'extension M/K est radicale.

Proposition

On considère des extensions $K \subset L \subset M$. Alors M/K est résoluble si et seulement si L/K et M/L sont résolubles.

Théorème

(Galois) Soit $K \subset L$ une extension galoisienne. Alors l'extension est résoluble si et seulement si son groupe de Galois l'est.

Définition

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

Lemme

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

Théorème

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

Théorème

Soit $K \subset L$ une extension galoisienne. On suppose que le groupe $G := Gal(L/K)$ est résoluble et il s'agit de montrer que l'extension est résoluble.

Démonstration.

On raisonne par récurrence sur $|G|$, le cas $|G| = 1$ étant trivial.
Par dévissage on se ramène au cas où G est résoluble et simple, c'est-à-dire cyclique d'ordre p premier . En effet, si G n'est pas simple, il admet un sous-groupe distingué H non trivial qui correspond, par la théorie de Galois à une extension galoisienne intermédiaire non triviale $K \subset M \subset L$ avec $H = Gal(L/M)$ et $G/H = Gal(M/K)$. Comme ces groupes sont résolubles l'hypothèse de récurrence assure que les extensions M/K et L/M le sont et on conclut. □

Lemme

Soit $K \subset L$ une extension galoisienne de groupe de Galois $\mathbb{Z}/p\mathbb{Z}$ avec p premier. Alors L/K est résoluble.

Calcul du discriminant

Proposition-Définition

Soit P un polynôme de degré n avec $x_1, x_2, ..., x_n$; $n \in \mathbb{N}$. On pose $\delta = \prod_{1 \leq i < j \leq n}(x_i - x_j)$ et $\Delta = \delta^2 = \prod_{1 \leq i < j \leq n}(x_i - x_j)^2$. Le nombre Δ est appelé discriminant du polynôme P. Et $\Delta = (-1)^{n(n-1)/2} \prod_{i \neq j}(x_i - x_j)$

Le signe $(-1)^{n(n-1)/2}$ est égal à 1 si $n \equiv 0$, 1 (mod 4) et à -1 sinon.

Règles de calculs

Soit P un polynôme. $P(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$. On suppose que la caractéristique du corps ne divise pas n. On considère le polynôme dérivé $P'(x)$ et on note $y_1, ..., y_{n-1}$ ses racines. On a donc :
$P'(X) = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + ... + a_1 = n\prod_{j=1}^{n-1}(X - y_j)$

Théorème

Soit Δ le discriminant de P . On a les formules :
$\Delta = (-1)^{n(n-1)/2}\prod_{i,j}(x_i - x_j) = (-1)^{n(n-1)/2}n^n\prod_{j=1}^{n-1}P(y_j)$

3.Exemple de l'équation de degré 3

Le Cadre
Soit K un corps et $P(X) = X^3 + aX^2 + bX + c$ un polynôme unitaire de degré 3 à coefficients dans K. On se propose d'étudier, voire de calculer, l'extension $L = D_K(P)$

Proposition

On suppose que K n'est pas de caractéristique 3. Il existe $p, q \in K$ tels que L soit le corps de décomposition du polynôme $P(Y) = Y^3 + pY + q$.

Démonstration.

Pour avoir P(Y) on effectue le changement de variable suivant $Y = X + \frac{a}{3}$ et on a $P(X) = P(Y - \frac{a}{3}) = Y^3 + pY + q$ avec $p = b - \frac{a^3}{3}$ et $q = \frac{2a^3}{27} - \frac{ab}{3} + c$. □

Dans ce qui suit on suppose K de caractéristique différente de 2 et 3.

On peut alors supposer P(Y) de la forme $Y^3 + pY + q$ et on le suppose irréductible. L'extension L/K est galoisienne et on note G son groupe de Galois. Si les racines de P dans L sont notées x_1, x_2, x_3, on a $L = K(x_1, x_2, x_3)$ et G s'identifie à un sous-groupe du groupe S_3 des permutations des x_i.

Les coefficients du polynôme se calculent à partir des racines : $0 = x_1 + x_2 + x_3$, $p = x_2x_3 + x_3x_1 + x_1x_2$ et $q = -x_1x_2x_3$. On sait, que le discriminant de P est alors $\Delta = -4p^3 - 27q^2$ et on a la proposition suivante :

Proposition

1)Si Δ n'est pas un carré de K, on a $[L : K] = 6$ et $G \simeq S_3$.
2) Si Δ est un carré de K, on a $[L : K] = 3$ et $G \simeq A_3$.

Les coefficients du polynôme se calculent à partir des racines :
$0 = x_1 + x_2 + x_3$, $p = x_2x_3 + x_3x_1 + x_1x_2$ et $q = -x_1x_2x_3$. On sait, que le discriminant de P est alors $\Delta = -4p^3 - 27q^2$ et on a la proposition suivante :

Proposition

1)Si Δ n'est pas un carré de K, on a $[L : K] = 6$ et $G \simeq S_3$.
2) Si Δ est un carré de K, on a $[L : K] = 3$ et $G \simeq A_3$.

i :La méthode par résolvante de Lagrange

On cherche à résoudre une équation de degré 3 dont les racines sont x_1, x_2, x_3. En vue de résoudre l'équation, la quantité intermédiaire que l'on veut considérer est $u = x_1 + jx_2 + j^2x_3$ où j est un nombre complexe vérifiant $j^3 = 1$.
A partir du sous-groupe A_3 de S_3 engendré par la permutation circulaire des racines du polynôme P. Ce qui donne :

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix}$$

Les valeurs respectives que prend u sont alors

$$\begin{cases} u = x_1 + jx_2 + j^2x_3 \\ u' = x_2 + jx_3 + j^2x_2 \\ u'' = x_3 + jx_1 + j^2x_2 \end{cases}$$

On remarque alors que $u' = j^2u$ et $u'' = ju$.

Maintenant, regardons les transpositions (32) , (13) et (12) suivants :

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix}$$

Par ces transformations,u prend trois valeurs qui sont :

$$\begin{cases} v = x_1 + jx_3 + j^2x_2 \\ v' = x_3 + jx_2 + j^2x_1 \\ v'' = x_2 + jx_1 + j^2x_3 \end{cases}$$

Pour cela utilisons l'identité $1 + j + j^2 = 0$

On a le système suivant :

$$\begin{cases} \sigma = x_1 + x_2 + x_3 \\ u = x_1 + jx_2 + j^2x_3 \\ v = x_1 + jx_3 + j^2x_2 \end{cases}$$

En sommant membre à membre ,on obtient
$\sigma + u + v = 3x_1 + (1 + j + j^2)x_2 + (1 + j + j^2)x_3 = 3x_1$
d'où $x_1 = \frac{\sigma+u+v}{3}$, $x_2 = \frac{\sigma+u'+v''}{3} = \frac{\sigma+j^2u+jv}{3}$, $x_3 = \frac{\sigma+u''+v'}{3} = \frac{\sigma+ju+j^2v}{3}$
Pour la détermination de u et v nous proposons ceci :
On calcule d'abord uv ce qui va donné $uv = -3p \Rightarrow u^3v^3 = -27p^3$
Comme $\sigma = 0$ en calculant $u + v$ on aura $u + v = 3x_1 \Rightarrow (u + v)^3 = 27x_1^3$.
Par identification après développement on aura
$u^3 + v^3 = 27x_1^3 + 27px_1 = -27q$ et on peut calculer u^3 et v^3 comme racines de $X^2 + 27X - 27p^3 = 0$.
Le discriminant de cette équation est égal à -27Δ. On obtient alors
$u^3 = \frac{-27+3\sqrt{-3\Delta}}{2}$ $v^3 = \frac{-27-3\sqrt{-3\Delta}}{2}$
Donc $3x_1 = u + v$ et $x_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$
En combinant les autres valeurs de u et v en système on a également les résultats suivants : $x_2 = j^2u + jv$ et $x_3 = ju + j^2v$.
Ce qui achève la méthode de résolution par la résolvante de Lagrange.

Après le changement de variable de l'équation initiale qui donne $P(Y) = Y^3 + pY + q = 0$, on a :
Posons $y = u + v$ ce qui donne $u^3 + v^3 + q + (3uv + p)(u + v) = 0$
Nous fixons maintenant : $u^3 + v^3 + q = 0$ et $3uv + p = 0$
$v = -p/(3u) \Rightarrow u^3 + v^3 + q = 0$ devient $u^3 + (-p/(3u))^3 + q = 0$ et
$v = -p/(3u) \Rightarrow u^3 v^3 = -\frac{p^3}{27}$
On a : $u^3 + v^3 = -q$ et $u^3 v^3 = -27p^3$
donc $(u^3)^2 + (v^3)^2 + 2v^3u^3 - 4v^3u^3 = (-q)^2 + \frac{4p^3}{27} \Rightarrow$
$(u^3)^2 + (v^3)^2 - 2v^3u^3 = (-q)^2 + \frac{4p^3}{27} \Rightarrow (u^3 - v^3) = \pm\sqrt{(-q)^2 + \frac{4p^3}{27}}$
donc on a le système suivant :

$$\begin{cases} u^3 + v^3 = -q \\ (u^3 - v^3) = \pm\sqrt{(-q)^2 + \frac{4p^3}{27}} \end{cases}$$

Après résolution de ce système on aura $u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$ et $v = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$ donc

$x_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$ et $x_2 = j^2u + jv$,
$x_3 = ju + j^2v$

Pour chaque méthode les racines trouvées sont pour l'équation $Y^3 + pY + q = 0$ donc pour avoir les racines du polynôme P initial il faudra revenir au premier cas par le biais de la relation, en prenant r_1 comme la première racine on a $r_1 = x_1 - \frac{a}{3}$

4.Cas des équations de degré ≥ 5

Tous les corps considérés seront de caractéristique nulle.

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 $\sum(\alpha_{i_1 i_2 ... i_s} b_1^{i_1} ... b_s^{i_s})$ 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 .

Définition

L'équation générale de degré n sur un corps K est une équation de la forme $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$ *où les coefficients* $a_0, a_1...a_{n-1}$ *sont algébriquement indépendants sur K.*

Théorème

Les racines $u_1, ..., u_n$ *sont algébriquement indépendants et distinctes deux à deux.*

Corollaire

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

Démonstration.

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

Théorème

(Abel) L'expression la plus proche de celle d'Abel est la suivante :
Il n'existe pas de formule générale exprimant les solutions de l'équation du cinquième degré sous forme de radicaux.

5.Exemple d'équation non résoluble par radicaux

Montrons que l'équation suivante n'est pas résoluble par radicaux
$P(X) = X^5 - 3X - 1 = 0$
La méthode la plus manuelle consiste à rechercher les diviseurs possibles de P(X) dans $\mathbb{Q}$[X]. Le caractère factoriel de l'anneau $\mathbb{Z}$[X] montre que si le polynôme est réductible dans $\mathbb{Q}$[X], il l'est aussi dans $\mathbb{Z}$[X] . Le polynôme n'admet pas de racine entière, on en déduit qu'il n'existe pas de diviseur de degré 1 ou 4 dans $\mathbb{Z}$[X]. Recherchons un diviseur de degré 2 ou 3. S'il en existe un, alors il existe deux entiers a et b, avec $b = 1$ ou $b = -1$, tels que $X^5 - 3X - 1 = (X^3 + aX^2 + (a^2 + b)X + b)(X^2 - aX - b)$.

Le calcul du terme d'ordre 1 montre que $a(a+1) = 2b$, c'est-à-dire b=1 et a=1 ou -2, ce qui est incompatible avec le calcul du terme d'ordre 2, $a^3 + 2ab - b = 0$.
On en déduit qu'il n'existe aucun diviseur de degré 2 ou 3 de P(X) dans $\mathbb{Z}$[X], ce qui montre son irréductibilité dans $\mathbb{Z}$[X].
L'équation $P(X) = 0$ n'est pas résoluble par radicaux dans $\mathbb{Q}$, l'ensemble des nombres rationnels : Soit G le groupe de Galois du corps de décomposition K du polynôme. G opère sur les racines du polynôme, on en déduit que G s'identifie à un sous-groupe de S_5 car les racines du polynôme engendre K, considéré comme une extension de $\mathbb{Q}$.

La conjugaison complexe est un automorphisme de K laissant invariant Q et permutant les deux racines complexes, on en déduit que G contient une transposition.
Montrons que G contient un élément d'ordre 5. Soit α une racine de P, le rapport entre l'ordre du groupe G et le cardinal du stabilisateur de α est égal au cardinal de l'orbite de α . Comme le polynôme P est irréductible, l'orbite de α est l'ensemble des 5 racines . Ceci montre que l'ordre de G est un multiple de 5. Le théorème de Cauchy montre que G contient un élément d'ordre 5.
Montrons que G est isomorphe à S_5. Les seuls éléments d'ordre 5 étant des cycles d'ordre 5, G en contient un. Or le groupe symétrique d'ordre 5 est engendré par tout couple composé d'une transposition et d'un élément d'ordre 5. Le groupe de Galois est en conséquence isomorphe à S_5.
Le groupe de Galois contient un unique sous-groupe distingué propre A_5. Ce sous-groupe est simple et non abélien, en conséquence, le groupe de Galois n'est pas résoluble. Le théorème d'Abel montre que l'équation polynomiale n'est pas résoluble par radicaux.

Merci pour votre aimable attention