TD5 : Théorie de Galois

23/10/2023

Exercice 1 : Exemples de groupes de Galois

1. Déterminer $\mathrm{Gal}(\mathbb{C},\mathbb{R})$ et $\mathrm{Gal}(\mathbb{R},\mathbb{Q})$.

2. Déterminer $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q})$.

3. Préciser les corps intermédiaires de L/K lorsque $K=\mathbb{Q}$ et $L=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

4. Préciser les corps intermédiaires de L/K lorsque $K=\mathbb{Q}$ et L est un corps de décomposition de X^3-2. Quels sont ceux qui sont normaux sur K ?

5. Soit α une racine dans $\mathbb{C}$ de $P(X)=X^3+X^2-2X-1$. Montrer que $\alpha'=\alpha^2-2$ est aussi racine de P. Calculer $\mathrm{Gal}(\mathbb{Q}(\alpha):\mathbb{Q})$ et montrer que l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est normale.

Correction :

1. L'extension $\mathbb{C}/\mathbb{R}$ est de degré 2, son groupe de Galois est C_2. Tout morphisme de corps $\mathbb{R}\to\mathbb{R}$ est continu et c'est un exercice classique de montrer qu'une telle application est linéaire, comme elle doit envoyer 1 sur 1, il n'y a que l'identité.

2. Un morphisme de corps $\mathbb{Q}(\sqrt[3]{2})\to\mathbb{Q}(\sqrt[3]{2})$ est déterminé par l'image de $\sqrt[3]{2}$ qui ne peut être que $\sqrt[3]{2}$ et donc il n'y a que l'identité.

3. On a une inclusion $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subset\mathbb{Q}(\sqrt{2},\sqrt{3})$. Cette dernière extension est Galoisienne et cette inclusion est une égalité en vertu de $(\sqrt{2}+\sqrt{3})^3-9(\sqrt{2}+\sqrt{3})=2\sqrt{2}$. Les sous corps possibles sont $\mathbb{Q},\mathbb{Q}(\sqrt{2}),\mathbb{Q}(\sqrt{3}),\mathbb{Q}(\sqrt{6}),L$.

4. Le groupe de Galois du (corps de décomposition du) polynôme est S_3. Ce groupe a 6 sous groupes et il y a donc 6 sous corps qui sont $\mathbb{Q},L,\mathbb{Q}(j),\mathbb{Q}(\sqrt{2}3),\mathbb{Q}(j\sqrt{2}3)$ et $\mathbb{Q}(j^2\sqrt{2}3)$.

5. On vérifie (c'est un calcul) que si $P(X)=X^3+X^2-2X-1$ alors $P(X^2-2)=(X^3-X^2-2X+1)(X^3+X^2-2X-1)$. Ce qui montre que α' est aussi racine de P. Le morphisme $x\mapsto x^2-2$ définit action sur l'ensemble des racines. S'il y a un point fixe alors il y a trois points fixes, en effet un point fixe est une racine de x^2-x-2, ces racines sont $\frac{1\pm i\sqrt{7}}{2}$ et comme P est à coefficients entiers (en particulier réel) les racines de P sont complexes conjuguées, ainsi s'il y a un point fixe, il y en a deux et donc trois car on agit sur un ensemble à trois éléments. Mais si les trois éléments sont fixes alors x^2-x-2 à trois racines ce qui est impossible. Donc il n'y a pas de point fixe. Ainsi $\mathbb{Q}(\alpha)$ est un corps de décomposition de P et en particulier l'extension est normale et même Galoisienne de groupe de Galois C_3.

Exercice 2 : Corps cyclotomiques

1. Quel est le groupe de Galois de $\mathbb{Q}(exp(\frac{2i\pi}{35}))/\mathbb{Q}$? Est-il cyclique ?

2. Combien $\mathbb{Q}(exp(\frac{2i\pi}{35}))$ a-t-il de sous-corps de degré 12 ? De degré 6 ?

Correction :

1. Le groupe de Galois de $\mathbb{Q}(exp(\frac{2i\pi}{35}))/\mathbb{Q}$ est isomorphe à $(\mathbb{Z}/35\mathbb{Z})^\times=C_4\times C_6$, il n'est donc pas cyclique.

2. L'extension $\mathbb{Q}(exp(\frac{2i\pi}{35}))/\mathbb{Q}$ est de degré 24, les sous extensions de degré 12 sont en bijection avec les sous groupes de $Gal(\mathbb{Q}(exp(\frac{2i\pi}{35}))/\mathbb{Q})$ de cardinal 2. Un tel sous groupe est un sous groupe de cardinal 2 de $C_4\times C_2$, il en a 3 (ceux générés par $(2,0),(2,1),(0,1)$ respectivement.

Les sous extensions de degré 6 sont en bijection avec les sous groupes de cardinal 4, il y en en a 2, donné par $C_2\times C_2$ et C_4.

Exercice 3 : Le groupe de Galois comme groupe de permutations des racines d'un polynôme.

Soient K un corps de caractéristique $\neq 2$ et $P\in K[X]$. On note L un corps de décomposition de P sur K. On note $a_1,\dots,a_n$ les racines distinctes de P dans L. On note $G:=\mathrm{Gal}(L/K)$.

✉clement.chivet@ens.fr

1. Montrer que G s'identifie naturellement à un sous-groupe de $\mathcal{S}_n$.

2. On suppose que G agit transitivement sur $\{a_1, \dots, a_n\}$. Montrer qu'alors il existe $Q \in K[X]$ irréductible tel que L est le corps de décomposition de Q sur K.

On rappelle que le discriminant de P est défini par

$$D = \Delta^2 \quad \text{avec} \quad \Delta := (-1)^{\frac{n(n-1)}{2}} \prod_{i<j} (a_i - a_j). \tag{1}$$

On suppose que les racines de P dans L sont simples (on a alors $\deg P = n$).

3. Montrer que $D \in K$.

4. Montrer que $G \subset \mathcal{A}_n$ si et seulement si $\Delta \in K$.

5. On note $H := G \cap \mathcal{A}_n$. Montrer que $L^H = K(\Delta)$.

Correction :

1. Le groupe G agit fidèlement sur les racines de P, il se plonge alors dans S_n.

2. Le polynôme $Q = \prod_n (X - a_n)$ est invariant par G et donc $Q \in K[X]$, ses facteurs premiers dans $K[X]$ sont en bijections avec les G-orbites de $\{a_1, \dots, a_n\}$ et comme l'action est transitive il est irréductible.

3. Pour $\sigma \in G$ on a $\sigma(\Delta) = \varepsilon(\sigma)\Delta$ et donc $\sigma(D) = D$.

4. On a $\Delta \in K$ ssi pour tout $\sigma, \varepsilon(\sigma) = 1$ ssi $G \subset A_n$

5. Si $\Delta \in K$ alors $G \subset A_n$ et $L^H = L^G = K$. Sinon H est d'indice 2 dans G et donc L^H est une extension de degré 2 de K, elle contient Δ qui par hypothèse n'est pas dans K, on a alors des inclusions $K \subset K(\Delta) \subset L^H$ et les degrés impliquent que $L^H = K(\Delta)$.

Exercice 4 : Groupes de Galois et groupes symétriques

Soit p un nombre premier, P un polynôme irréductible sur $\mathbb{Q}$ de degré p. On suppose que P admet exactement deux zéros non réels.

1. Montrer que $\mathrm{Gal}_{\mathbb{Q}}(P)$ s'identifie à un sous-groupe de $\mathcal{S}_p$. Montrer qu'il contient un p-cycle et une transposition.

2. En déduire que $\mathrm{Gal}_{\mathbb{Q}}(P) \simeq \mathcal{S}_p$.

Correction :

1. Soit K le corps de décomposition de P, on fait le choix d'un plongement de $K \hookrightarrow \mathbb{C}$, on note $K_0 = K \cap \mathbb{R}$. L'hypothèse que P a exactement deux zéros non réels implique que $[K : K_0] = 2$.

Comme P est irréductible et de degré p, le groupe $\mathrm{Gal}(P)$ agit sur les racines de P qui est un ensemble à p éléments ce qui plonge $\mathrm{Gal}(P)$ dans $\mathcal{S}_p$.

Comme l'extension K/K_0 est de degré 2 elle est Galoisienne et le groupe de Galois est engendré par la conjugaison complexe qui permute les deux racines. Ce qui défini une transposition dans $\mathrm{Gal}(P)$.

Pour voir qu'il existe un élément d'ordre p dans $\mathrm{Gal}(P)$ il suffit de voir que $\mathrm{Gal}(P)$ agit transitivement sur les racines de P. Pour cela on décompose $P = \prod_{orbite} \prod_{x \in Orb}(X - x)$ et chaque facteur $\prod_{x \in Orb}(X - x)$ est Galois invariant donc un polynôme à coefficients dans $\mathbb{Q}$, ce qui donne une décomposition de P en produit. Comme P est irréductible, il n'y a qu'un seul facteur et donc une seule orbite ce qui prouve la transitivité de l'action. Alors $p || \mathrm{Gal}(P)|$ et donc $\mathrm{Gal}(P)$ contient un élément d'ordre p, ie un p-cycle car p premier.

2. Le groupe S_p est engendré par toute combinaison d'un p-cycle et d'une transposition.

Exercice 5 : Groupe de Galois d'un polynôme de degré 3.

Soit $P = X^3 + pX + q$ avec $p, q \in \mathbb{Q}$ et $K \subset \mathbb{C}$ l'extension de $\mathbb{Q}$ engendrée par es racines complexes (éventuellement confondues) z_1, z_2, z_3 de P. On note $G = Gal(K/\mathbb{Q})$.

1. Montrer la formule $\mathrm{disc}(P) = -\prod_i P'(z_i)$. En déduire la formule $\mathrm{disc}(P) = -4p^3 - 27q^2$.

2. Si P est réductible dans $\mathbb{Q}$, déterminer G en fonction du nombre de racines de P dans $\mathbb{Q}$.

On suppose désormais P sans racine dans $\mathbb{Q}$.

3. Montrer que les racines de P sont simples.

On plonge G dans S_3 en le faisant agir sur les racines.

4. Déterminer G en fonction des valeurs de $\mathrm{disc}(P)$.

5. Montrer que P est irréductible sur $\mathbb{Q}(\sqrt{\mathrm{disc}(P)})$.

Correction :

1. Le discriminant peut être calculé dans n'importe quelle extension de K, en particulier dans le corps de décomposition de P. La formule $disc(P) = (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(a_i - a_j)$ combinée avec le fait que $P'(z_i) = \prod_{j\neq i}(z_i - z_j)$ donne la première formule. Un calcul évident montre que $\prod_i P'(z_i) = 27(z_1z_2z_3)^2 + 3p^2(z_1^2+z_2^2+z_3^2) + p^3 + 9p((z_1z_2)^2 + (z_2z_3)^2 + (z_1z_3)^2)$ ce qui donne la formule du discriminant en utilisant les relations coefficients-racines.

2. Si P es réductible il a au moins une racine. Si P a deux racines, il est scindé et donc en a trois alors G est trivial. Si P n'a qu'une seule racine alors $K/\mathbb{Q}$ est de degré 2 et donc $G = \mathbb{Z}/2\mathbb{Z}$.

3. Si P n'a qu'une seule racine (de multiplicité 3) dans K alors celle-ci est invariante par G et donc dans $\mathbb{Q}$ ce qui est impossible. Si P a une racine double alors comme l'action de G sur P permute ses racines en préservant les multiplicités cette racine double est invariante par G et donc dans $\mathbb{Q}$.

4. Par les question précédente on sait que P est irréductible sur $\mathbb{Q}$, et donc $G = A_3$ ou $G = S_3$ et par l'exercice 2 $G = A_3$ ssi $disc(P)$ est un carré dans $\mathbb{Q}$.

5. L'extension $K/\mathbb{Q}(\sqrt{disc(P)})$ est de degré 3 et Galoisienne de groupe de Galois C_3 ce groupe agit transitivement sur les racines de P et donc P est irréductible sur $Q(\sqrt{disc(P)})$.

Exercice 6 :

Soit $P = (X^2+3)(X^3-3X+1) \in \mathbb{Q}[X]$. Et G le groupe de Galois de P.

1. Montrer que G se plonge dans $\mathbb{Z}/2\mathbb{Z} \times \mathcal{S}_3$.

2. Déterminer G. Est-il commutatif ? cyclique ?

Correction :

1. En notant $P = P_1P_2$, on voit que $G \hookrightarrow \mathrm{Gal}(P_1) \times \mathrm{Gal}(P_2)$. (et car P_1,P_2 irréductibles). $\mathrm{Gal}(P_1) = \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{Gal}(P_2) = \mathfrak{S}_3$ ou $\mathfrak{A}_3$

2. Comme $\mathrm{disc}(P) = -(4\times(-3)^3 + 27\times 1^2) = 27\times 3 = 9^2$, on vot que $\mathrm{Gal}(P_2) \subset \mathfrak{A}_3$, et $G = \mathbb{Z}/6\mathbb{Z}$.

Exercice 7 :

On pose $a = \sqrt{5+\sqrt{21}}$ et on note $K = \mathbb{Q}(a)$.

1. Calculer $[K : \mathbb{Q}]$.

2. Montrer que $K/\mathbb{Q}$ est galoisienne.

3. Déterminer le groupe de Galois de l'extension $K/\mathbb{Q}$.

4. Déterminer les sous-corps de K.

5. L'extension $\mathbb{Q}(\sqrt{5+\sqrt{15}})/\mathbb{Q}$ est-elle galoisienne ?

Correction :

1. On a la tour d'extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{21}) \subset K$, il suffit alors de montrer que $\sqrt{5+\sqrt{21}} \notin \mathbb{Q}(\sqrt{21})$ pour conclure que $[K : \mathbb{Q}] = 4$. Or si $5+\sqrt{21} = (u+v\sqrt{21})^2$, cela conduit au système

$$\begin{cases} 2uv = 1 \\ 5 = u^2 + 21v^2 \end{cases}$$

et donc u vérifie $u^2 + \frac{21}{4u^2} = 5$, soit u racine de $X^4 - 5X^2 + \frac{21}{4}$ qui n'a pas de racine rationnelle, ses racines étant $\pm\sqrt{\frac{5\pm 2}{2}}$, absurde. D'où le degré de l'extension.

2. Le polynôme $P(X) = (X^2-5)^2 - 21$ annule a et est de degré 4, c'est donc le polynôme minimal de a sur $\mathbb{Q}$. Ses racines sont $\pm a$ et $\pm \underbrace{\sqrt{5-\sqrt{21}}}_{=:b}$. Or a^2 et b^2 racines de $(X-5)^2 - 21$ donc leur produit vaut 4, et par positivité $ab = 2$ (on peut aussi juste faire le calcul). Alors $b \in K$, donc K est le corps de décomposition de P sur $\mathbb{Q}$, et $\mathbb{Q}$ étant parfait l'extension $K/\mathbb{Q}$ est galoisienne.

3. Le groupe de galois G est d'ordre 4, ne contient que des éléments d'ordres au plus 2 (un morphisme revient à choisir l'image de a, car b est lié à a par la relation $ab = 2$. Finalement, $G = (\mathbb{Z}/2\mathbb{Z})^2$.

4. A part K et $\mathbb{Q}$, les sous-extensions correspondent par la correspondance de Galois aux sous-groupes do'rdre 2 de G, c'est à dire au choix d'un morphisme qui n'est pas l'identité. Par exemple prenons $a \to -a$. Le corps stable contient $\mathbb{Q}(a^2) = \mathbb{Q}(\sqrt{21})$ car a^2 est stable par ce morphisme, or cette extension est de degré 2 donc c'est exactement le corps stable.

Prenons maintenant $a \mapsto -b$. Alors b est envoyé sur $\frac{2}{-b} = -a$, et la quantité $a - b$ est dans le corps stable. On a donc l'extension $\mathbb{Q}(a-b) = \mathbb{Q}(\sqrt{6})$ correspondant à ce sous-groupe. Finalement avec $a \to b$ on trouve $\mathbb{Q}(a+b) = \mathbb{Q}(\sqrt{14})$.

5. Non, on peut vérifier qu'elle est aussi de degré 4, on note de même $a = \sqrt{5+\sqrt{15}}$ et $b = \sqrt{5-\sqrt{15}}$. On remarque que $ab = \sqrt{10}$ cette fois (car $P(X) = (X^2-5)^2 - 15$), donc il n'y a pas de raison que $\mathbb{Q}(a)$ contienne b. Prouvons le vraiment, supposons par l'absurde que cette extension soit galoisienne, soit G son groupe de Galois (d'ordre 4). Alors la sous extension $\mathbb{Q}(\sqrt{15})$ correspond au corps stable par un morphisme $g \in G$ d'ordre 2 qui fixe $\sqrt{15}$, donc a^2, mais pas a. On a donc forcément $g(a) = -a$, et $g(b) = \pm b$. Si $g(b) = b$, alors $b \in \mathbb{Q}(\sqrt{15})$ ce qui est absrude par un même calcul qu'en question 1. Alors $g(b) = -b$, mais dans ce cas $g(ab) = ab$ et $ab \in \mathbb{Q}(\sqrt{15}$. Or $ab = \sqrt{10}$, ce qui est absurde. D'où l'extension $\mathbb{Q}(\sqrt{5+\sqrt{15}})/\mathbb{Q}$ n'est pas galoisienne.

Exercice 8 : Compositum de deux Corps

1. Soient $k \subset E, F \subset K$ des corps. On définit EF comme le plus petit sous-corps de K contenant E et F. On a $EF = E(F) = F(E)$.

a. Supposons que l'extension F/k est galoisienne. Montrer que EF/E et $F/F \cap E$ sont galoisienne et que $\text{res}_{|E} : \text{Gal}(EF/E) \to \text{Gal}(F/F \cap E)$ est un isomorphisme.

b. Dans ce cas, en déduire la relation sur les degrés :

$$[EF : k] = \frac{[F:k][E:k]}{[E \cap F : k]}$$

c. Supposons maintenant que E/k et F/k sont galoisiennes. Montrer que EF/k et $E \cap F/k$ sont galoisiennes et que l'application $\sigma \to (\sigma_{|E}, \sigma_{|F})$ de $\text{Gal}(EF/k) \to \text{Gal}(E/k) \times \text{Gal}(F/k)$ est un morphisme de groupe injectif et déterminer son image.

2. Soient m en n deux entiers naturels non nuls. On pose $N = ppcm(m,n)$ et $d = pgcd(m,n)$. Pour tout entier naturel non nul t, on désigne par ζ_t une racine primitive t-ème de l'unité dans $\mathbb{C}$.

a. Montrer que $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_N)$.

b. Montrer que $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$.

Correction :

1.

a.

b.

c.

2.

a. Clairement on a $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_N)$ et de même pour $\mathbb{Q}(\zeta_n)$ ce qui donne $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_N)$. Dans l'autre sens $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n, \zeta_m) \ni \zeta_N$, en effet si on écrit $n = dn', m = dm'$ alors il existe a, b non tous deux nuls tels que $an' + bm' = 1$ et on a alors $\zeta_m^a \zeta_n^b = \zeta_N$.

3.

a. Le corps $\mathbb{Q}(\zeta_d)$ est contenu dans $\mathbb{Q}(\zeta_n)$ et $\mathbb{Q}(\zeta_m)$ et donc dans leur intersection. Toutes les extensions en vue sont Galoisienne et on a donc la relation suivante sur les degrés

$$[\mathbb{Q}(\zeta_N) : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_n) : \mathbb{Q}][\mathbb{Q}(\zeta_m) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) : \mathbb{Q}]} \tag{2}$$

L'égalité des extensions suivra si on arrive à montrer que $[\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_d) : \mathbb{Q}]$.

Cela revient à montrer la formule suivante :

$$\phi(N) = \frac{\phi(n)\phi(m)}{\phi(d)} \tag{3}$$

où ϕ est l'indicatrice d'Euler, mais cela devient trivial si on écrit que $\phi(n) = \prod_{p|n} p^{v_p(n)}(1 - \frac{1}{p})$ où p parcours l'ensemble des diviseurs premiers de p.

Remarque : La question 2. n'est vraie que pour $\mathbb{Q}$! Elle est fausse en générale, voir par exemple example 3.1 de

https ://kconrad.math.uconn.edu/blurbs/galoistheory/cyclotomic.pdf

Exercice 9 : Méthode de Hilbert et Galois inverse

Soient K un corps de caractéristique nulle et $K \subseteq L$ une extension galoisienne de degré 3.

1. Déterminer le groupe de Galois de L/K.

2. Montrer qu'il existe un polynôme $P \in K[X]$ irréductible de degré 3 tel que L soit le corps de décomposition de P.

3. Donner l'exemple d'un corps K et d'un polynôme $P \in K[X]$ irréductible de degré 3 dont le corps de décomposition est de degré 6 sur K.

Soient σ l'automorphisme de corps qui fixe les éléments de K et qui envoie X sur $\dfrac{1}{1-X}$ et G le sous-groupe de $\mathrm{Gal}(K(X)/K)$ engendré par σ.

4. Montrer que σ est un automorphisme d'ordre 3.

5. Montrer que le corps fixe $K(X)^G$ est de la forme $K(T)$, où l'extension $K(T) \subseteq K(X)$ est galoisienne de degré 3 et où T est une fraction rationnelle que l'on explicitera.

Supposons l'existence de $t \in K$ tel que le polynôme

$$P = X^3 - tX^2 + (t-3)X + 1 \in K[X]$$

soit irréductible.

6. Montrer que le corps de décomposition de P est une extension galoisienne de degré 3 de K.

Correction :

1. L'extension L/K est le corps de décomposition d'un polynôme de degré 3 (le polynôme minimal d'un élément primitif), et donc le groupe de Galois se plonge dans S_3 mais comme l'extension est de degré 3 on a $\#G = 3$ et donc $G = C_3$.

2. Fait dans 1.

3. On a déjà traité l'exemple de $X^3 - 2$.

4. C'est un calcul trivial.

5. Si on trouve $R \in K(X)^G$ tel que $R = \frac{P}{Q}$ avec P, Q premier entre eux et $\max(deg(P), deg(Q)) = 3$ alors $K(X)^G = K(R)$ pour des questions de degré. Il suffit alors de trouver un tel R, s'il existe le

polynôme minimal de X sur $K(X)$ est $P(T) - Q(T)R$ mais le polynôme minimal de X est aussi $\mu_X = (T-X)(T-\sigma(X))(T-\sigma^2(X))$. On développe et on trouve que $\mu_X = (T^3 - 3T + 1) + (T^2 - T)\frac{X^3-3X+1}{X^2-X}$. On pose alors $R = \frac{X^3-3X+1}{X^2-X}$ et ce R convient.

6. Le même calcul montre que si α est une racine alors $\frac{1}{1-\alpha}$ et $\frac{\alpha-1}{\alpha}$ sont aussi racines de P et donc que le groupe de Galois est C_3 et le corps de décomposition de P est de degré 3 sur K.

Exercice 10 : Encore des exemples

Calculer les groupes de Galois suivants :

(i) $X^3 - 3X + 1$ sur $\mathbb{Q}$,

(ii) $X^3 - 3TX - T - T^2$ sur $\mathbb{C}(T)$,

(iii) $X^6 - 3X^2 - 1$,

(iv) $X^3 + 2X^2 + 3X + 2$ sur $\mathbb{Q}$, $\mathbb{Q}(\sqrt{7})$, et $\mathbb{Q}(i\sqrt{7})$.

Correction :

On décrit la méthode. D'abord on vérifie si le polynôme est irréductible. Ensuite on applique la méthode de l'exercice 9. On calcul le discriminant et on détermine ainsi le groupe de Galois. Pour le point (iv), on commence par faire une translation $X \mapsto X + \alpha$ pour se ramener au cas où le polynôme est de la forme $X^3 + pX + q$. Pour le point (iii), c'est un polynôme de la forme $Q = P(X^2)$ où P est un polynôme de degré 3, un corps de décomposition est obtenu en extrayant des racines carrés des racines de P, on calcule donc d'abord un corps de décompsition de P et on determine si les racines de P sont déjà des carrés.

Exercice 11 : Equation non résoluble par radicaux

On considère le polynôme

$$P(X) = X^5 - 5X^2 + 1 \in \mathbb{Q}[X] \tag{4}$$

et G le groupe de Galois de P sur $\mathbb{Q}$.

1. Montrer que G se plonge dans S_5.

Soit $\bar{P}$ la réduction de P dans $\mathbb{F}_2[X]$.

2. Montrer que $\bar{P}$ est irréductible dans $\mathbb{F}_2[X]$.

3. En déduire que P est irréductible dans $\mathbb{Z}[X]$ puis dans $\mathbb{Q}[X]$.

4. Montrer que G possède un élément d'ordre 5.

On note σ la conjugaison complexe.

5. Montrer que $\sigma \in G$ et déterminer le type de l'image de σ dans S_5.

6. Déterminer le cardinal de G. L'équation $P(x) = 0$ est-elle résoluble par radicaux ?

Correction :

1. Le polynôme P a cinq racines donc son groupe de Galois agit sur ces cinq racines et se plonge donc dans S_5.

2. On fait le calcul explicite : mod 2 on a $P = X^5 + X^2 + 1$ qui n'a clairement pas de racine dans $\mathbb{F}_2$, s'il est réductible c'est donc un produit d'un polynôme de degré 3 par un polynôme de degré 2, alors $P = (X^3 + aX^2 + bX + 1)(X^2 + cX + 1) = X^5 + (c+a)X^4 + (1 + ac + b)X^3 + (a + bc + 1)X^2 + (b + c)X + 1$, alors $a + c = 0$ et $b + c = 0$ comme on est en caractéristique 2, on a $a = b = c$ et donc $1 + a + a^2 = 0$ ce qui est impossible donc P est bien irréductible mod 2.

3. Si P était réductible dans $\mathbb{Z}[X]$ il le serait dans $\mathbb{F}_2[X]$ donc P est irréductible dans $\mathbb{Z}[X]$, comme son contenu est 1 il est aussi irréductible dans $\mathbb{Q}[X]$ par le lemme de Gauss.

4. Comme P est irréductible toutes ses racines sont simples et conjuguées, comme G agit transitivement sur les racines et que l'ensemble des racines est de cardinal 5, on a $5|\#G$ et donc il existe un élément d'ordre 5 dans G.

5. Une étude de fonction montre que P a exactement 3 racines réelles et donc deux racines complexes qui sont par conséquents conjuguées. La conjugaison complexes échange ces deux racines. Et donc σ est une transposition.

6. Comme S_5 est engendré par un 5 cycle et une transposition on a $G = S_5$ et G est de cardinal 120. Comme G n'est pas résoluble P n'est pas résoluble par radicaux.

Exercice 12 : Groupe de Galois mod p

Soit $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$ un polynôme unitaire à coefficients entiers. Notons $z_1, \ldots, z_n$ ses racines complexes et $K := \mathbb{Q}(z_1, \ldots, z_n) \subset \mathbb{C}$ le corps de décomposition de P, et $G = \mathrm{Gal}(K/\mathbb{Q})$. Soit p un nombre premier, $\overline{P}$ la réduction de P dans $\mathbb{F}_p[X]$ et $\overline{G}$ le groupe de Galois de $\overline{P}$.

On note $A = \mathbb{Z}[z_1, \ldots, z_n]$ sous-anneau de K.

1.

a. Montrer que l'action de G sur K laisse A stable.

b. Pour $a \in A, N(a) := \prod_{g\in G} g(a)$. Montrer que $N(a) \in \mathbb{Z}$.

c. Montrer que l'idéal pA est distinct de A.

d. Soit $\mathfrak{m}$ un idéal maximal de A contenant pA. Montrer que $k := A/\mathfrak{m}$ est un corps de décomposition de $\overline{P}$.

2. On pose $D_\mathfrak{m} := \{g \in G, g(\mathfrak{m}) = \mathfrak{m}\}$, et on note $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_i\} = \{g(\mathfrak{m}), g \in G\backslash D_\mathfrak{m}\}$ l'ensemble des idéeaux distincts conjugués à $\mathfrak{m}$.

a. Montrer que $D_\mathfrak{m}$ est un sous-groupe de G.

b. Montrer que pour tout i, $\mathfrak{m}_i + \mathfrak{m} = A$, puis que $\mathfrak{m} + \mathfrak{m}_1 \ldots \mathfrak{m}_r = A$.

c. Montrer qu'il existe $x \in A$ tel que $\overline{x} \in k$ engendre l'extension $k/\mathbb{F}_p$. Montrer qu'il existe $z \in A$ tel que $\overline{z} = \overline{x}$ et $g(z) \in \mathfrak{m}$ pour tout $g \in G\backslash D_\mathfrak{m}$.

d. Montrer que le polynôme $\mu(X) := \prod_{g\in G}(X - g(z))$ est à coefficients dans $\mathbb{Z}$.

e. Si $g \in D_\mathfrak{m}$, expliquer pourquoi g induit un élément $\overline{g} \in \overline{G}$. Montrer que le morphisme $\psi : g \in D_\mathfrak{m} \to \overline{g} \in \overline{G}$ est un isomorphisme.

f. Si $\overline{P}$ est séparable, montrer que ψ est surjectif.

3. Quelle est la nature de $\overline{G}$?

Correction :

Voir `https://www.math.ens.psl.eu/shared-files/9555/?ExamenA2-2013.pdf`