FICHE DE TD n°6

correction des exos 1 et 3

Exercice 1.

1) Le polynôme X^5-2 est-il résoluble par radicaux sur $\mathbb{Q}$?

$\Leftrightarrow \mathrm{Gal}_{\mathbb{Q}}(X^5-2)$ est résoluble.

1ère méthode (par le groupe de Galois)

Rappel un groupe fini G est résoluble si :

$\exists G=G_0 \geqslant G_1 \geqslant \cdots \geqslant G_N=1, \forall i, G_{i+1} \lhd G_i$ et G_i/G_{i+1} est cyclique.

Exemple.

$\underset{S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}}{S_4 \trianglerighteq A_4} \underset{A_4/K \cong \mathbb{Z}/3\mathbb{Z}}{\trianglerighteq} K=\{1,(12)(34),(13)(24),(14)(23)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \trianglerighteq \{1, (12)(34)\} \cong \mathbb{Z}/2\mathbb{Z} > 1.$

Donc S_4 résoluble $\Rightarrow$donc tous les polynômes de degrés $\leqslant 4$ sont résolubles par radicaux sur $\mathbb{Q}$.

Corps de décomposition de X^5-2 sur $\mathbb{Q}$ $=K=\mathbb{Q}(\sqrt[5]{2}, \sqrt[5]{2}z, \sqrt[5]{2}z^2, \sqrt[5]{2}z^3, \sqrt[5]{2}z^4)=\mathbb{Q}(\sqrt[5]{2}, z)$ où $z=e^{2i\pi/5}$.

$G=\mathrm{Gal}(K/\mathbb{Q})$ est résoluble en effet :

$K>\mathbb{Q}(z)>\mathbb{Q}$ et $\mathrm{Gal}(K/\mathbb{Q}(z)) \cong \mathbb{Z}/5\mathbb{Z}$ et $\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$.

$\Rightarrow G \underset{G/H \cong \mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q})}{\trianglerighteq} H=\mathrm{Gal}(K/\mathbb{Q}(z))>1.$ (car $\mathbb{Q}(z)/\mathbb{Q}$ galoisienne)

Si z est une racine primitive $n-i$ème de l'unité (exemple : $e^{\frac{2i\pi}{n}}$) alors son polynôme minimal sur $\mathbb{Q}$ est le polynôme $\Phi_n(X)=\prod_{k\epsilon(\mathbb{Z}/n\mathbb{Z})^\times}(X-z^k)\epsilon\mathbb{Q}[X]$:

$\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q}) \underset{(z\mapsto z^k)\leftarrow k}{\cong} (\mathbb{Z}/n\mathbb{Z})^\times$cyclique si n premier (par exemple si $n=5$, $\Phi_5(X)=1+X+X^2+X^3+X^4$).

Donc X^5-2 est résoluble par radicaux.

2ème méthode : directement

Posons :

$$z = \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right) \text{avec : } \cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{2},\ \sin\left(\frac{2\pi}{5}\right) = \sqrt{\frac{\sqrt{5}-1}{2}}, i = \sqrt{-1}.$$

Le polynôme $X^5 - 2$ est résoluble par radicaux car ses racines s'expriment avec des radicaux (de nombres rationnels) : $z^k\sqrt[5]{2}\,, 0 \leqslant k \leqslant 4$ $\square$

2) $P(X) = X^5 + 2X^3 - 8X + 2$.

Justifer que P est irréductible sur $\mathbb{Q}$: par Eisenstein ! (avec $p = 2$).

Donc $G = \mathrm{Gal}_{\mathbb{Q}}(P) \leqslant S_5$ est d'ordre un multiple de 5 ($P(X)$ irréductible $\Rightarrow G$ agit transitivement sur les racines : en effet, si $P(X) = (X - x_1)\ldots(X - x_5)$, alors $\forall i, \exists \sigma \epsilon \mathrm{Gal}_{\mathbb{Q}}(P), \sigma(x_1) = x_i$).

Il suffit de montrer que G contient une transposition.

Montrer que P a trois racines réelles et deux complexes non réelles conjuguées.

$P'(x) = 5x^4 + 6x^2 - 8 = 5(x^2 + 2)\left(x^2 - \frac{4}{5}\right)$

Tableau de variations $\Rightarrow$ trois racines réelles (par le théorème des valeurs intermédiaires).

x	$-\infty$		$-\frac{2}{\sqrt{5}}$		$\frac{2}{\sqrt{5}}$		$+\infty$
$P'(x)$		$+$	0	$-$	0	$+$	
$P(x)$	$-\infty$	$\nearrow$	$\frac{388}{25\sqrt{5}}+2>0$	$\searrow$	$-\frac{388}{25\sqrt{5}}+2<0$	$\nearrow$	$+\infty$

$\Rightarrow$ la conjugaison complexe réalise une transposition des racines.

$\Rightarrow G \cong S_5$.

3) $P(X) = X^6 - 6X^3 + 7 = (X^3)^2 - 6X^3 + 7$.

$P(x) = 0 \Leftrightarrow x^3 = 3 \pm \sqrt{2}$.

Corps de décomposition $= \mathbb{Q}\left(\sqrt[3]{3-\sqrt{2}}, \sqrt[3]{3+\sqrt{2}}, j\right)$ résoluble par radicaux …

Exercice 3.

1) $G = \mathrm{Gal}_{\mathbb{Q}}(P)$ agit transitivement sur les racines de P :$x_1,x_2,\ldots,x_p$.

Donc G s'identifie à un sous-groupe transitif de S_p donc d'ordre un multiple de p donc contient un élément d'ordre p.

Or dans S_p un élément d'ordre p est forcément un cycle c de longueur p. (Contre-exemple si $n=6$: $(12)(345)$ est d'ordre 6 mais n'est pas un $6-$cycle !).

Quitte à renuméroter les racines, on peut supposer que $c=(12\ldots p)$.

2) Soient x_i, x_j les deux racines non réelles. Elles sont conjuguées car $P \epsilon \mathbb{R}[X]$. Donc la conjugaison complexe correspond à la transposition $t=(i\,j)$ dans G.

Montrer que $\left\langle \underset{c}{(12\ldots p)}, \underset{t}{(i\,j)} \right\rangle = S_p$.

$c^k t c^{-k} = (c^k(i) c^k(j))$. On peut choisir k tel que $c^k(i) = 1$.

Donc on peut supposer (quitte à remplacer t par $c^k \mathrm{t} \mathrm{c}^{-k}$) que $t=(1j)$avec $2 \leqslant j \leqslant p$.

Quitte à remplacer c par $c^{j-1}=(1j\ldots)$ on peut supposer que $j=2$ c-à-d : $G = <(12\ldots p),(12)> \geqslant <(12),(23),\ldots,(p-1\,p)> = S_p$.

3) Supposer $p = \text{nombre premier impair}$.

Nous allons montrer que le polynôme :

$P(X) = X(X-2)(X-2a)\ldots.(X-2(p-2)a)-(b+2)$

avec $a=2^p(p-2)!$ et $b=2^p a^{p-2}(p-2)!$

est irréductible sur $\mathbb{Q}$ et de groupe de Galois S_p.[1]

Posons $g(X) = X(X-2)(X-2a)\ldots.(X-2(p-2)a)$.

Alors $\deg P = \deg g = 2+p-2 = p$.

1. Désolé, ce n'est pas le polynôme original de la fiche de TD mais au moins pour celui ci au moins je peux justifier que le groupe de Galois est S_p …

De plus, d'après le théorème des accroissements finis, $g' = P'$ s'annule en :

$s_1 < \ldots < s_{p-1}$ où $0 < s_1 < 2 < s_2 < 2a < s_3 < \ldots < s_{p-1} < 2(p-2)a$

Comme P' est de degré $p-1$, on en déduit :

$P'(X) = p(X - s_1)(X - s_2)\ldots(X - s_{p-1})$.

Comme $p-1$ est impair, on en déduit le signe de P':

$P'(x) > 0$ si $x \epsilon]-\infty, s_1[\cup]s_2, s_3[\cup \ldots \cup]s_{p-3}, s_{p-2}[\cup]s_{p-1}, +\infty[$

et $P'(x) < 0 \,\mathrm{si}\, x \epsilon]s_1, s_2[\cup]s_3, s_4[\cup \ldots \cup]s_{p-2}, s_{p-1}[$

On obtient un tableau de variations de P ressemblant à ceci :

$-\infty$		s_1		s_2					s_{p-2}		s_{p-1}		$+\infty$
P'	$+$	0	$-$	0	$+$				0	$-$	0	$+$	
P	$\nearrow$		$\searrow$		$\nearrow$					$\searrow$		$\nearrow$	

Or si $x < 0$, $g(x) < 0 \Rightarrow P(x) < 0$.

De plus, si $x \epsilon [0, 2]$, $|g(x)| \leqslant 2 \times 2 \times 2a \times \cdots \times 2(p-2)a = 2^p a^{p-2}(p-2)!$

$\Rightarrow P(x) < 0$. donc P n'a pas de racines sur $]-\infty, 2[$

Comme $s_2 < 2a < s_3$, et comme $P(2a) < 0$, et comme P croît sur $[s_2, 2a]$, P n'a pas de racines non plus dans l'intervalle $[2, 2a]$.

Puisque $2a < s_3 < 4a < s_4$, puisque P croît sur $[2a, s_3]$ et décroît sur $[s_3, 4a]$,puisque $P(2a), P(4a) < 0$, puique :

$g(3a) = 3a(3a-2)a(-1)^{p-3}(a)\ldots(2p-5)a \geqslant a^p > b + 2 \Rightarrow P(3a) > 0$

on a forcément : $P(s_3) \geqslant P(3a) > 0$ et donc d'après le théorème des valeurs intermédiaires P s'annule exactement deux fois dans l'intervalle $[2a, 4a]$.

Puisque P décroît sur $[4a, s_4]$, croît sur $[s_4, 6a]$, Puisque $P(4a), P(6a) < 0$, P est <0 sur $[4a, 6a]$ et donc ne s'annule pas.

De même, on voit que P a deux racines exactement sur chaque intervalle :

$[2ka, 2(k+1)a]$ si k est impair et $2 \leqslant 2k < 2(k+1) \leqslant 2(p-2)$

et n'a pas de racines sur $[2ka, 2(k+1)a]$ si k est pair et $2 \leqslant 2k < 2(k+1) \leqslant 2(p-2)$.

On remarque aussi que P s'annule une seule fois sur l'intervalle :

$[2(p-2)a, +\infty[$.

Conclusion : P a exactement : $2 \times \frac{p-3}{2} + 1 = p-2$ racines réelles.

Pour montrer que $\mathrm{Gal}_{\mathbb{Q}}(P) = S_p$ il reste à montrer que P est irréductible sur $\mathbb{Q}$.

Or, $P(X) = X(X-2)(X-2a)\ldots.(X-2(p-2)a) - (b+2)$ vérifie le critère d'Eisenstein pour $p = 2$ $\square$

4) Si G est fini, alors il existe n tel que $G \leqslant S_n$. Il suffit en effet de prendre $n = |G|$. Si p premier $>n$, on peut identifier S_n à un sous-groupe de S_p.

Supposons $G \leqslant S_p$.

$\mathbb{Q} < K < L$ Où $L =$ corps de décomposition d'un polynôme de groupe de Galois S_p.

Prenons $K = L^G$. Alors L/L^Gest galoisienne de groupe de Galois G.