TD14 : Théorie de Galois I

Diego Izquierdo

Les exercices 3, 4 et les questions (i), (iii), (v), (vi) de l'exercice 7 sont à préparer. Nous traiterons les exercices dans l'ordre suivant : 3, 4, 7(i)(iii)(v)(vi), 11. Nous traiterons ensuite l'exercice 8 ou l'exercice 9.

Nous ne ferons pas l'exercice 0, mais je vous conseille de le faire : en tous cas, vous pouvez utiliser sa conclusion dans les autres exercices.

Ce TD (ainsi que le prochain) est particulièrement important : *il faut que vous sachiez calculer des groupes de Galois et expliciter la correspondance de Galois sur des exemples. Je vous conseille donc fortement de faire plus d'exercices de cette feuille que ceux qui seront traités pendant la séance.*

Exercice 0 : Sous-groupes transitifs de S_4

Dans cet exercice, on va déterminer tous les sous-groupes transitifs de S_4.

1. Quels sont les sous-groupes transitifs de S_4 d'ordre 12 ?
2. Exhiber un 2-Sylow H de S_4 et montrer que $H \cong D_8$.
3. Déterminer tous les sous-groupes transitifs de H.
4. Montrer que les sous-groupes transitifs de S_4 sont S_4, A_4, et tous ceux qui sont conjugués à $\langle (1\ 3), (1\ 2\ 3\ 4)\rangle \cong D_8$, à $\langle (1\ 3)(2\ 4), (1\ 2)(3\ 4)\rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$ ou à $\langle (1\ 2\ 3\ 4)\rangle \cong \mathbb{Z}/4\mathbb{Z}$.

Exercice 1 : Partiel 2012

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 tous les sous-corps de K.
5. L'extension $\mathbb{Q}(\sqrt{5+\sqrt{15}})/\mathbb{Q}$ est-elle galoisienne ?

Exercice 2 : Partiel 2011

Soient $p_1, ..., p_n$ des nombres premiers deux à deux distincts.

1. Montrer que l'extension $\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})/\mathbb{Q}$ est galoisienne. On note G son groupe de Galois.
2. Montrer que tout élément de G est d'ordre 2. En déduire que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^r$ pour un certain r.
3. Exprimer en fonction de r le nombre de sous-extensions de $\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$ de degré 2 sur $\mathbb{Q}$.
4. Montrer que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$.
5. Le réel $\sqrt{15}$ est-il dans $\mathbb{Q}(\sqrt{10}, \sqrt{42})$?

Exercice 3 : Rattrapage 2014

Soit L un corps de décomposition sur $\mathbb{Q}$ du polynôme $X^4 - 6 \in \mathbb{Q}[X]$.

1. Montrer que $L = \mathbb{Q}(\sqrt[4]{6}, i)$ et que $[L : \mathbb{Q}] = 8$.
2. Montrer que le groupe de Galois $G = \mathrm{Gal}(L/\mathbb{Q})$ contient des éléments r et s tels que $r(\sqrt[4]{6}) = i\sqrt[4]{6}$, $r(i) = i$, $s(\sqrt[4]{6}) = \sqrt[4]{6}$ et $s(i) = -i$.

3. Montrer que G est isomorphe à D_8.
4. Expliciter les sous-groupes de G.
5. Faire la liste des sous-corps de L. On donnera un élément primitif pour chacun d'entre eux.
6. Parmi eux, lesquels sont des extensions galoisiennes de $\mathbb{Q}$?

Exercice 4 : Groupe symétrique comme groupe de Galois 1

1. Soit p un nombre premier. Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible de degré p ayant exactement deux racines non réelles. Montrer que le groupe de Galois de P est isomorphe à S_p.
2. Quel est le groupe de Galois de $X^5 - 6X + 3$?

Exercice 5 : Extensions ayant un groupe de Galois fixé

1. Montrer que, pour tout groupe fini G, il existe une extension finie galoisienne de groupe de Galois G.

Soit p un nombre premier impair. Soit m un entier naturel non nul. Soit $(n_1, ..., n_{p-2})$ un $p-2$-uplet d'entiers relatifs distincts. On pose $f = (X^2 + m)\prod_{i=1}^{p-2}(X - n_i)$.

2. Montrer que pour tout réel ϵ de valeur absolue suffisamment petite, le polynôme $f + \epsilon \in \mathbb{R}[X]$ admet $p-2$ racines réelles simples et deux racines complexes conjuguées.
3. Pour tout nombre premier ℓ, on considère le polynôme $P_\ell = \ell^p f(X/\ell) + \ell$. Montrer que pour ℓ assez grand, le polynôme $P_\ell \in \mathbb{Q}[X]$ est un polynôme irréductible ayant $p-2$ racines réelles simples et deux racines complexes conjuguées. Quel est le groupe de Galois de P_ℓ ?
4. Soit G un groupe fini. Montrer qu'il existe une extension finie galoisienne L/K de groupe de Galois G telle que K est une extension finie de $\mathbb{Q}$.

Exercice 6 : Groupe symétrique comme groupe de Galois 2

1. Montrer qu'un sous-groupe transitif de S_n contenant une transposition et un $n-1$-cycle est égal à S_n.
2. Quel est le groupe de Galois de :

$$f = X^6 + 22X^5 + 6X^4 + 12X^3 - 52X^2 - 14X - 30$$

sur $\mathbb{Q}$?

Exercice 7 : Groupes de Galois divers et variés

Calculer les groupes de Galois des polynômes suivants :

(i) $f_1 = X^3 - 3X + 1$ sur $\mathbb{Q}$;
(ii) $f_2 = X^4 + 4$ sur $\mathbb{Q}$;
(iii) $f_3 = X^8 + 1$ sur $\mathbb{Q}$;
(iv) $f_4 = X^3 - 3TX - T - T^2$ sur $\mathbb{C}(T)$;
(v) $f_5 = X^5 - 70X^4 - 49X^3 - 70X^2 + 98X + 105$ sur $\mathbb{Q}$;
(vi) $f_6 = 32X^5 + 16X^4 - 32X^3 - 12X^2 + 6X + 1 = 32\prod_{i=1}^{5}\left(X - \cos\left(\frac{2i\pi}{11}\right)\right)$ sur $\mathbb{Q}$;

(vii) $f_7 = X^4 + 4X^3 + 2X^2 + 3X - 5$ sur $\mathbb{Q}$;
(vii) $f_8 = X^3 + 2X^2 + 3X + 2$ sur $\mathbb{Q}$, $\mathbb{Q}(i\sqrt{7})$ et $\mathbb{Q}(\sqrt{7})$;
(ix) $f_9 = X^6 - 3X^2 + 1$ sur $\mathbb{Q}$;
(x) $f_{10} = X^6 - 4X^2 - 1$ sur $\mathbb{Q}$;
(xi) $f_{11} = X^6 + 3$ sur $\mathbb{Q}$;
(xii) $f_{12} = X^4 - 5$ sur $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(i\sqrt{5})$ et $\mathbb{Q}(i)$;
(xiii) $f_{13} = X^n - T$ sur $\mathbb{R}(T)$ et $\mathbb{C}(T)$;
(xiv) $f_{14} = (X^5 - 2)(X^5 - 3)$ sur $\mathbb{Q}$;
(xv) $f_{15} = (X^3 - 2)(X^3 - 3)(X^2 - 2)$ sur $\mathbb{Q}(i\sqrt{3})$;
(xvi) $f_{16} = X^6 - 2$ sur $\mathbb{Q}$.

Exercice 8 : Extensions biquadratiques

Soit $P = X^4 + aX^2 + b$ un polynôme irréductible sur $\mathbb{Q}$. On note $\pm\alpha$ et $\pm\beta$ ses racines dans un corps de décomposition K.

1. Montrer que $\mathrm{Gal}(K/\mathbb{Q})$ est isomorphe à un sous-groupe de D_8. En déduire qu'il est isomorphe à l'un des trois groupes suivants :

$$\mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ D_8.$$

2. Montrer que l'on a $\alpha^2 - \beta^2 \notin \mathbb{Q}$.

3. Montrer que l'on est dans le premier cas de la question 1. si et seulement si on a $\dfrac{\alpha}{\beta} - \dfrac{\beta}{\alpha} \in \mathbb{Q}$, et que l'on est dans le deuxième si et seulement si on a $\alpha\beta \in \mathbb{Q}$.

4. Pour chacun des polynômes suivants, déterminer le groupe de Galois et faire la liste des sous-corps d'un corps de décomposition :
(i) $f_1 = X^4 - 4X^2 - 1$;
(ii) $f_2 = X^4 - 6X^2 + 4$;
(iii) $f_3 = X^4 - 7X^2 + 10$;
(iv) $f_4 = X^4 + 5X^2 + 5$.

Remarque. On pourra faire le lien entre cet exercice et l'exercice 15 du TD6.

Exercice 9 : Quaternions

On rappelle que le groupe des quaternions $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ est défini par les relations suivantes :

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j.$$

Soient $\alpha = (2 + \sqrt{2})(3 + \sqrt{6})$ et $K = \mathbb{Q}(\alpha)$.

1. Montrer que l'extension $K/\mathbb{Q}$ est galoisienne, de groupe de Galois isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On notera $\sigma_i, \sigma_j, \sigma_k$ les éléments de $\mathrm{Gal}(K/\mathbb{Q})$ distincts de l'identité.

2. Montrer que pour tout $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, le quotient $\sigma(\alpha)\alpha^{-1}$ est le carré d'un élément de K que l'on précisera.

Soient $\delta = \sqrt{\alpha}$ et $L = \mathbb{Q}(\delta)$.

3. Montrer $\delta \notin K$ et en déduire le groupe de Galois de L/K.

On note τ le générateur de $\mathrm{Gal}(L/K)$, que l'on considérera par la suite également comme un élément de $\mathrm{Gal}(L/\mathbb{Q})$.

4. Définir des automorphismes $\widetilde{\sigma}_i$ et $\widetilde{\sigma}_j$ de L sur $\mathbb{Q}$ qui prolongent σ_i et σ_j respectivement.

On pose $\widetilde{\sigma}_k = \widetilde{\sigma}_i\widetilde{\sigma}_j$.

5. Montrer que le groupe de Galois de l'extension galoisienne $L/\mathbb{Q}$ est isomorphe à $\mathbb{H}_8$.

6. Combien le corps L possède-t-il de sous-corps quadratiques (ie de degré 2 sur $\mathbb{Q}$) ?

Exercice 10 (difficile) : Un groupe de Galois d'ordre 48

Soit $P = X^6 + (3-2T)X^4 + TX^3 + (3-2T)X^2 + 1 \in \mathbb{Q}(T)[X]$. Montrer que le groupe de Galois G de P sur $\mathbb{Q}(T)$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_3$, où S_3 agit sur $(\mathbb{Z}/2\mathbb{Z})^3$ par permutation des coordonnées. Si vous ne savez pas ce qu'est un produit semi-direct, montrez à la place qu'il existe une suite exacte :

$$1 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^3 \xrightarrow{f} G \xrightarrow{g} S_3 \longrightarrow 1$$

et un morphisme $h : S_3 \to G$ tel que :

- $g \circ h = \mathrm{Id}$;
- pour tout $(a_1, a_2, a_3) \in (\mathbb{Z}/2\mathbb{Z})^3$ et tout $\sigma \in S_3$, on a :

$$h(\sigma)f(a_1, a_2, a_3)h(\sigma)^{-1} = f(a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}).$$

Exercice 11 : Examen 2011

Soit L/K une extension galoisienne finie de groupe de Galois S_n pour un certain $n \geq 5$. Montrer que le degré sur K d'un élément de L est soit 1, soit 2, soit supérieur ou égal à n. Le résultat subsiste-t-il pour $n = 4$?

Exercice 12 : Formules de Cardan

Soit K un corps de caractéristique nulle contenant une racine primitive 3-ème de l'unité que l'on notera j. Soient $P = X^3 + aX + b \in K[X]$ un polynôme irréductible et L son corps de décomposition. On note $\alpha, \beta, \gamma \in L$ les racines de P.

1. Déterminer les groupes de Galois possibles pour l'extension L/K.

2. Montrer que $\mathrm{Gal}(L/K)$ contient un sous-groupe normal H d'ordre 3 que l'on précisera.

3. Montrer que $(\alpha + \rho\beta + \rho^2\gamma)^3$ est un élément de L^H, et qu'il en est de même de $(\alpha + \rho^2\beta + \rho\gamma)^3$.

4. En déduire des expressions explicites de α, β, γ.

Exercice 13 : 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.

7. Que se passe-t-il si on remplace σ par l'élément de $\mathrm{Gal}(K(X)/K)$ qui envoie X sur $\dfrac{X+1}{-X+1}$?

Exercice 14 : Partiel 2011 et rattrapage 2014

1. Soit L un corps de décomposition d'un polynôme $P \in K[X]$ irréductible séparable. L'extension L/K est alors galoisienne ; on suppose que son groupe de Galois est abélien. Soit x une racine de P dans L. Montrer que $L = K(x)$.

2. Soit L un corps de décomposition d'un polynôme $P \in \mathbb{F}_q[X]$ irréductible. Montrer que, pour tout racine x de P dans L, on a $L = \mathbb{F}_q(x)$.

Exercice 15 : Réciprocité quadratique

Soit $p > 2$ un nombre premier et $\overline{\mathbb{F}_p}$ une clôture algébrique fixée de $\mathbb{F}_p$. Pour $x \in \mathbb{F}_p^\times$, on note $\left(\dfrac{x}{p}\right) = 1$ si x est un carré dans $\mathbb{F}_p$, $\left(\dfrac{x}{p}\right) = -1$ sinon. C'est le symbole de Legendre.

1. Montrer que, pour tout $x \in \mathbb{F}_p^\times$, $\left(\dfrac{x}{p}\right) = x^{\frac{p-1}{2}}$ dans $\mathbb{F}_p$.

2. En considérant $\alpha + \alpha^{-1}$ avec $\alpha \in \overline{\mathbb{F}_p}$ une racine primitive 8-ème de l'unité, montrer l'égalité $\left(\dfrac{2}{p}\right) = (-1)^{\frac{(p-1)(p+1)}{8}}$.

Soit $\ell > 2$ un nombre premier distinct de p. Soit $\xi \in \overline{\mathbb{F}_p}$ une racine ℓ-ème primitive de l'unité. On note $S = \sum_{x \in \mathbb{F}_\ell^\times} \left(\dfrac{x}{\ell}\right) \xi^x$ la somme de Gauss correspondante.

3. Montrer l'égalité $S^2 = (-1)^{\frac{\ell-1}{2}} \ell$.

4. En déduire la loi de réciprocité quadratique :

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{(p-1)(\ell-1)}{4}}.$$