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 ?

> **Indications :** Soit H un sous-groupe d'ordre 12 de S_4. D'après le lemme d'Ore, H est un sous-groupe distingué de S_4. Par conséquent, s'il contient une transposition, il contient toutes les transpositions, et comme les transpositions engendrent S_4, on obtient $H = S_4$: absurde ! Donc H ne contient aucune transposition. Comme toute permutation impaire est produit d'un nombre impair de transpositions, cela entraîne que H est contenu dans A_4. Comme H est d'ordre 12, on en déduit que $H = A_4$. C'est le seul sous-groupe (transitif) d'ordre 12 de S_4.

2. Exhiber un 2-Sylow H de S_4 et montrer que $H \cong D_8$.

> **Indications :** Le groupe S_4 est d'ordre 24. Il suffit donc d'exhiber un sous-groupe de S_4 isomorphe à D_8. Pour ce faire, on remarque que le groupe D_8 agit sur l'ensemble des sommets d'un carré. Cette action étant fidèle, elle induit un morphisme de groupes injectif $D_8 \hookrightarrow S_4$. L'image de ce morphisme est donc un sous-groupe de S_4 isomorphe à D_8. Plus explicitement, il s'agit du sous-groupe de S_4 engendré par $s = (1\ \ 3)$ et $r = (1\ \ 2\ \ 3\ \ 4)$.

3. Déterminer tous les sous-groupes transitifs de H.

> **Indications :**
> - Commençons par faire la liste des sous-groupes de D_8. Soit r la rotation d'angle $\pi/2$ et s la symétrie par rapport à l'une des diagonales du carré. Alors $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$, et on a les relations $r^4 = 1$, $s^2 = 1$, $srs = r^{-1}$.
>   - Sous-groupes d'ordre 1 : $\{1\}$.
>   - Sous-groupes d'ordre 2 : $\{1, r^2\}$, $\{1, s\}$, $\{1, sr\}$, $\{1, sr^2\}$, $\{1, sr^3\}$.
>   - Sous-groupes d'ordre 4 : le seul sous-groupe cyclique d'ordre 4 de D_8 est $\{1, r, r^2, r^3\}$. Pour trouver les sous-groupes isomorphes à $(\mathbb{Z}/2\mathbb{Z})^2$, on remarque qu'ils sont tous des réunions de trois sous-groupes parmi $\{1, r^2\}$, $\{1, s\}$, $\{1, sr\}$, $\{1, sr^2\}$, $\{1, sr^3\}$. On vérifie alors aisément que ce sont les sous-groupes $\{1, r^2, s, sr^2\}$ et $\{1, r^2, sr, sr^3\}$.
>   - Sous-groupes d'ordre 8 : D_8.
> - Soit maintenant K un sous-groupe transitif contenu dans H. D'après la formule des classes, son ordre est multiple de 4. En utilisant la liste des sous-groupes de D_8, on voit que les sous-groupes transitifs de H sont H, $\{1, r^2, sr, sr^3\}$ et $\{1, r, r^2, r^3\}$.

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 $\langle (1\ \ 2\ \ 3\ \ 4)\rangle \cong \mathbb{Z}/4\mathbb{Z}$.

Indications : Soit K un sous-groupe transitif de S_4. D'après la formule des classes, l'ordre de K est multiple de 4. Si K est d'ordre au moins 12, alors K est A_4 ou S_4 d'après 1. Reste donc à étudier les cas où K est d'ordre 4 ou 8. Mais dans ce cas, d'après les théorèmes de Sylow, K est conjugué à un sous-groupe de H. En utilisant la question précédente, on déduit que les sous-groupes transitifs de S_4 sont S_4, A_4, et tous ceux qui sont conjugués à $H = \langle (1\ 3), (1\ 2\ 3\ 4)\rangle$, à $\langle (1\ 3)(2\ 4), (1\ 2)(3\ 4)\rangle$ ou à $\langle (1\ 2\ 3\ 4)\rangle$.

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 ?

Indications : Voir le corrigé du partiel 2012.

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 $\mathbb{Q}(\sqrt{10}, \sqrt{42})$?

Indications : Voir le corrigé du partiel 2011.

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 $[L : K] = 8$.
2. Montrer que le groupe de Galois $G = \mathrm{Gal}(L/K)$ 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.

> **Indications :** Soit $n = |G|$. Le groupe G s'identifie à un sous-groupe de S_n. On peut donc faire agir G par permutation des variables sur $\mathbb{C}(X_1, ..., X_n)$. D'après le théorème d'Artin, l'extension $\mathbb{C}(X_1, ..., X_n)/\mathbb{C}(X_1, ..., X_n)^G$ est 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.

> **Indications :** C'est un exercice d'analyse ! L'existence de $p-2$ racines réelles simples est assurée par le théorème des valeurs intermédiaires. L'existence d'une racine non réelle découle par exemple du théorème de l'argument en analyse complexe.

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 ?

> **Indications :** Pour tout ℓ, le polynôme ℓ est irréductible d'après le critère d'Eisenstein. De plus, d'après la question 2., pour ℓ assez grand, le polynôme $f(X) + \frac{1}{\ell^{p-1}} = \frac{P_\ell(\ell X)}{\ell^p}$ a deux $p-2$ racines réelles simples et deux racines complexes conjuguées. Il en est donc de même pour P_ℓ. Le groupe de Galois de P_ℓ est alors isomorphe à S_p d'après l'exercice 4.

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 $\mathbb{Q}$.

> **Indications :** Soit $n = |G|$. Le groupe G s'identifie à un sous-groupe de S_n. Il s'identifie donc aussi à un sous-groupe de S_ℓ pour $\ell \geq n$ premier. Pour ℓ assez grand, la question 3. permet de construire une extension finie galoisienne L_ℓ de $\mathbb{Q}$ de groupe de Galois S_ℓ. Il suffit alors d'invoquer la correspondance de Galois pour obtenir l'existence d'un sous corps K de L_ℓ tel que $\mathrm{Gal}(L_\ell/K) \cong G$.

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.

> **Indications :** Soit G un tel sous-groupe. On peut supposer que G contient $\sigma = (2\ 3\ ...\ n)$. Soit $t = (a\ b)$ une transposition dans G. Comme G est transitif, il existe $u \in G$ tel que $u(a) = 1$. On remarque alors que $utu^{-1} = (1\ u(b))$ est dans G. Comme $\sigma^k utu^{-1}\sigma^{-k} = (1\ \sigma^k(u(b)))$ est dans G pour tout k, on déduit que G contient $(1\ 2)$, $(1\ 3)$, ..., $(1\ n)$. Mais pour $1 < c < d \leq n$, on a $(1\ c)(1\ d)(1\ c) = (c\ d)$, et donc G contient toutes les transpositions de S_n. On en déduit que $G = S_n$.

2. Quel est le groupe de Galois de :

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

sur $\mathbb{Q}$?

Indications : On remarque d'abord que f est irréductible d'après le critère d'Eisenstein. Donc $Gal(f)$ est un sous-groupe transitif de S_6. On a :

$$f \equiv X(X^5 + X^4 + 2X + 1 \mod 3$$
$$f \equiv X(X+1)(X+2)(X+4)(X^2+2) \mod 5$$

Comme $X^5+X^4+2X+1 \in \mathbb{F}_3[X]$ et $X^2+2 \in \mathbb{F}_5[X]$ sont irréductibles, $Gal(f)$ contient un 5-cycle et une transposition. Donc $Gal(f) = S_6$.

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 $\mathbb{Q}$;

Indications : $\mathbb{Z}/2\mathbb{Z}$ (le corps de décomposition est $\mathbb{Q}(i)$).

(iii) $f_3 = X^8 + 1$ sur $\mathbb{Q}$;

(iv) $f_4 = X^3 - 3TX - T - T^2$ sur $\mathbb{C}(T)$;

Indications : A_3 (polynôme irréductible et le discriminant est un carré).

(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 $\mathbb{Q}$;

Indications : S_4 (Dedekind modulo 2 donne un 4-cycle, Dedekind modulo 3 donne un 3-cycle, Dedekind modulo 4 donne une transposition, une transposition, un 3-cycle et un 4-cycle engendrent S_4).

(viii) $f_8 = X^3 + 2X^2 + 3X + 2$ sur $\mathbb{Q}$, $\mathbb{Q}(i\sqrt{7})$ et $\mathbb{Q}(\sqrt{7})$;

Indications : $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{Q}$ et sur $\mathbb{Q}(\sqrt{7})$, 1 sur $\mathbb{Q}(i\sqrt{7})$ ($f_8 = (X+1)(X - \frac{-1+i\sqrt{7}}{2})(X - \frac{-1-i\sqrt{7}}{2})$).

(ix) $f_9 = X^6 - 3X^2 + 1$ sur $\mathbb{Q}$;

Indications : Soient α, β, γ les racines de $g = X^3 - 3X + 1$. Le polynôme g est irréductible et son discriminant est un carré. Donc $\mathrm{Gal}(g) \cong \mathbb{Z}/3\mathbb{Z}$ et le corps de décomposition de g est $M = \mathbb{Q}(\alpha)$. Le corps de décomposition de f_9 est $L = \mathbb{Q}(\sqrt{\alpha}, \sqrt{\beta}, \sqrt{\gamma})$.
On vérifie aisément que α, β, γ sont réelles et, quitte à supposer $\alpha \leq \beta \leq \gamma$, que $\alpha < 0$ et que $\beta, \gamma > 0$. Il est alors immédiat de voir que $[L : \mathbb{Q}(\sqrt{\beta}, \sqrt{\gamma})] = 2$.
Supposons que $\sqrt{\gamma} \in \mathbb{Q}(\sqrt{\beta})$. Soit $P \in \mathbb{Q}[X]$ tel que $\sqrt{\gamma} = P(\sqrt{\beta})$. Soit $s \in \mathrm{Gal}(g)$ l'élément tel que $s(\beta) = \gamma$. Il existe $\tilde{s} \in \mathrm{Gal}(f)$ qui étend s. On a alors $\tilde{s}(\sqrt{\beta}) = \pm\sqrt{\gamma}$, $\tilde{s}(\sqrt{\gamma}) = \pm\sqrt{\alpha}$ et $\tilde{s}(\sqrt{\alpha}) = \pm\sqrt{\beta}$. Par conséquent $P(\pm\sqrt{\gamma}) = \pm\sqrt{\alpha}$: absurde car $[L : \mathbb{Q}(\sqrt{\beta}, \sqrt{\gamma})] = 2$. Donc $[\mathbb{Q}(\sqrt{\beta}, \sqrt{\gamma}) : \mathbb{Q}(\sqrt{\beta})] = 2$. De même on montre que $[\mathbb{Q}(\sqrt{\beta}) : \mathbb{Q}] = 2$.
On en déduit que $[L : \mathbb{Q}] = 24$ et on a une suite exacte :

$$1 \to (\mathbb{Z}/2\mathbb{Z})^3 \to \mathrm{Gal}(f_9) \to \mathbb{Z}/3\mathbb{Z} \to 1.$$

Les éléments de $\mathrm{Gal}(f)$ sont les :

$$s_{\epsilon_1;\epsilon_2;\epsilon_3} : \alpha \mapsto \epsilon_1\alpha, \beta \mapsto \epsilon_2\beta, \gamma \mapsto \epsilon_3\gamma$$
$$t_{\epsilon_1;\epsilon_2;\epsilon_3} : \alpha \mapsto \epsilon_1\beta, \beta \mapsto \epsilon_2\gamma, \gamma \mapsto \epsilon_3\alpha$$
$$u_{\epsilon_1;\epsilon_2;\epsilon_3} : \alpha \mapsto \epsilon_1\gamma, \beta \mapsto \epsilon_2\alpha, \gamma \mapsto \epsilon_3\beta,$$

avec $(\epsilon_1, \epsilon_2, \epsilon_3) \in \{\pm 1\}^3$. On vérifie immédiatement que $\mathrm{Gal}(f) \cong A_4$.

(x) $f_{10} = X^6 - 4X^2 - 1$ sur $\mathbb{Q}$;

Indications :

(xi) $f_{11} = X^6 + 3$ sur $\mathbb{Q}$;

Indications : S_3 (le corps de décomposition est $\mathbb{Q}(i\sqrt[6]{3})$; il suffit d'étudier l'action de $\mathrm{Gal}(f)$ sur $\{\zeta_6, i\sqrt[6]{3}\}$).

(xii) $f_{12} = X^4 - 5$ sur $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(i\sqrt{5})$ et $\mathbb{Q}(i)$;

Indications : $GA_1(\mathbb{Z}/4\mathbb{Z}) \cong D_8$ sur $\mathbb{Q}$ ($\mathrm{Gal}(f)$ est un sous-groupe d'ordre 8 du groupe $GA_1(\mathbb{Z}/4\mathbb{Z})$ qui est d'ordre 8). Avec la correspondance de Galois, on obtient $(\mathbb{Z}/2\mathbb{Z})^2$ pour $\mathbb{Q}(\sqrt{5})$ et $\mathbb{Q}(i\sqrt{5})$, et $\mathbb{Z}/4\mathbb{Z}$ pour $\mathbb{Q}(i)$.
Remarque : Pour comprendre le lien entre les extensions de Kummer et le groupe affine GA_1, voir l'exercice 10 du TD15.

(xiii) $f_{13} = X^n - T$ sur $\mathbb{R}(T)$ et $\mathbb{C}(T)$;

Indications : Par le critère d'Eisenstein, le polynôme $f_{13} \in \mathbb{C}(T)[X]$ est irréductible. Donc son groupe de Galois sur $\mathbb{C}(T)$ est cyclique d'ordre n.
L'extension $\mathbb{C}(\sqrt[n]{T})/\mathbb{R}(T)$ étant de degré $2n$, son groupe de Galois est d'ordre $2n$. Ainsi, son groupe de Galois est constitué des automorphismes $\sigma_{k,\epsilon}$ de $\mathbb{C}(\sqrt[n]{T})$ définis par $\sigma_{k,\epsilon}(\sqrt[n]{T}) = \zeta_n^k \sqrt[n]{T}$ $(0 \leq k \leq n-1)$ et $\sigma_{k,\epsilon}(i) = \epsilon i$ $(\epsilon \in \{\pm 1\})$. Il est donc engendré par $\sigma_{1,1}$ et $\sigma_{0,-1}$. En plaçant $\sqrt[n]{T}, \zeta_n \sqrt[n]{T}, \zeta_n^2 \sqrt[n]{T}, ..., \zeta_n^{n-1} \sqrt[n]{T}$ sur les sommets d'un polygone régulier à n-côtés (dans cet ordre), on remarque que $\sigma_{1,1}$ et $\sigma_{0,-1}$ s'identifient respectivement à la rotation d'angle $\frac{2\pi}{n}$ et à une symétrie du polygone. Cela permet d'identifier $\mathrm{Gal}(\mathbb{C}(\sqrt[n]{T})/\mathbb{R}(T))$ au groupe diédral D_{2n}.

(xiv) $f_{14} = (X^5 - 2)(X^5 - 3)$ sur $\mathbb{Q}$;

Indications : Il faut d'abord montrer que $[\mathbb{Q}(\sqrt[5]{2}, \sqrt[5]{3}, \zeta_5) : \mathbb{Q}] = 100$. Supposons que $X^5 - 3$ ne soit pas irréductible sur $\mathbb{Q}(\sqrt[5]{2}, \zeta_5)$. On écrit $X^5 - 3 = PQ$ avec $P, Q \in \mathbb{Q}(\sqrt[5]{2}, \zeta_5)[X]$. Supposons que P et Q soient irréductibles de degrés respectifs 2 et 3. Alors pour chaque $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[5]{2}, \zeta_5)/\mathbb{Q})$, on a $\sigma(P) = P$ et $\sigma(Q) = Q$. Donc P et Q sont à coefficients dans $\mathbb{Q}$: absurde car $X^5 - 3$ est irréductible sur $\mathbb{Q}$. Donc $X^5 - 3$ possède une racine dans $\mathbb{Q}(\sqrt[5]{2}, \zeta_5)$. On en déduit que $\sqrt[5]{3} \in \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$. Mais la seule extension intermédiaire de $\mathbb{Q}(\sqrt[5]{2}, \zeta_5)/\mathbb{Q}$ de degré 5 est $\mathbb{Q}(\sqrt[5]{2})$, ce qui montre que $\sqrt[5]{3} \in \mathbb{Q}(\sqrt[5]{2})$. En procédant comme dans l'exercice 16 du TD6, on prouve que cela est faux, ce qui nous permet de conclure que $X^5 - 3$ est irréductible sur $\mathbb{Q}(\sqrt[5]{2}, \zeta_5)$. Nous avons donc établi que $[\mathbb{Q}(\sqrt[5]{2}, \sqrt[5]{3}, \zeta_5) : \mathbb{Q}] = 100$.
Notons $p : GA_1(\mathbb{Z}/5\mathbb{Z}) \to \mathbb{Z}/4\mathbb{Z}$ la projection canonique. Le groupe de Galois de f_{14} est alors le noyau de :

$$GA_1(\mathbb{Z}/5\mathbb{Z}) \times GA_1(\mathbb{Z}/5\mathbb{Z}) \to \mathbb{Z}/4\mathbb{Z}, (x, y) \mapsto p(x) - p(y).$$

En effet, cela signifie simplement que se donner un élément de $\mathrm{Gal}(f_{14})$, c'est se donner des éléments de $\mathrm{Gal}(\mathbb{Q}(\sqrt[5]{2}, \zeta_5)/\mathbb{Q})$ et $\mathrm{Gal}(\mathbb{Q}(\sqrt[5]{3}, \zeta_5)/\mathbb{Q})$ qui coïncident sur $\mathbb{Q}(\zeta_5)$.

(xv) $f_{15} = (X^3 - 2)(X^3 - 3)(X^2 - 2)$ sur $\mathbb{Q}(i\sqrt{3})$;

Indications :

(xvi) $f_{16} = X^6 - 2$ sur $\mathbb{Q}$.

Indications : $GA_1(\mathbb{Z}/6\mathbb{Z}) \cong D_{12}$ (c'est un sous-groupe d'ordre 12 de $GA_1(\mathbb{Z}/6\mathbb{Z})$).

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 :

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

Indications : Comme P est irréductible, $\mathrm{Gal}(K/\mathbb{Q})$ s'identifie à un sous-groupe transitif de S_4. Comme $[K:\mathbb{Q}]\leq 8$ (car $(\alpha\beta)^2\in\mathbb{Q}$), l'exercice 1 montre que $\mathrm{Gal}(K/\mathbb{Q})$ est isomorphe à un sous-groupe de D_8. Plus précisément, 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 $\alpha^2-\beta^2\notin\mathbb{Q}$.

Indications : On a $\alpha^2+\beta^2=-a\in\mathbb{Q}$. Si $\alpha^2-\beta^2$ était rationnel, on aurait $\alpha^2,\beta^2\in\mathbb{Q}$ et $P=(X^2-\alpha^2)(X^2-\beta^2)$ contredirait l'irréductibilité de P.

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 $\alpha\beta\in\mathbb{Q}$.

Indications : On note $G=Gal(K/\mathbb{Q})$. Avec 1, G est un sous-groupe de D_8, où ce dernier agit sur $\{\alpha,\beta\}$ par :

$$Id:\begin{array}{ccc}\alpha&\mapsto&\alpha\\ \beta&\mapsto&\beta\end{array},\quad \sigma:\begin{array}{ccc}\alpha&\mapsto&\beta\\ \beta&\mapsto&-\alpha\end{array},\quad \sigma^2:\begin{array}{ccc}\alpha&\mapsto&-\alpha\\ \beta&\mapsto&-\beta\end{array},\quad \sigma^3:\begin{array}{ccc}\alpha&\mapsto&-\beta\\ \beta&\mapsto&\alpha\end{array},$$

$$\tau:\begin{array}{ccc}\alpha&\mapsto&-\alpha\\ \beta&\mapsto&\beta\end{array},\quad \tau\sigma:\begin{array}{ccc}\alpha&\mapsto&\beta\\ \beta&\mapsto&\alpha\end{array},\quad \tau\sigma^2:\begin{array}{ccc}\alpha&\mapsto&\alpha\\ \beta&\mapsto&-\beta\end{array},\quad \tau\sigma^3:\begin{array}{ccc}\alpha&\mapsto&-\beta\\ \beta&\mapsto&-\alpha\end{array}.$$

Si G est isomorphe à $\mathbb{Z}/4\mathbb{Z}$, c'est le groupe engendré par σ. Comme $K/\mathbb{Q}$ est galoisienne, on a $K^G=\mathbb{Q}$; et comme $\dfrac{\alpha}{\beta}-\dfrac{\beta}{\alpha}$ est fixe par σ, cette quantité est rationnelle.

Si G est isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, alors G est $\{Id,\tau,\sigma^2,\tau\sigma^2\}$ ou bien $\{Id,\tau\sigma,\sigma^2,\tau\sigma^3\}$. Dans le premier cas, $\alpha^2-\beta^2$ est fixe par G et est donc dans $\mathbb{Q}$: ce cas n'est en fait pas possible par (b). Dans le second cas, $\alpha\beta$ est fixe par G et est ainsi dans $\mathbb{Q}$.

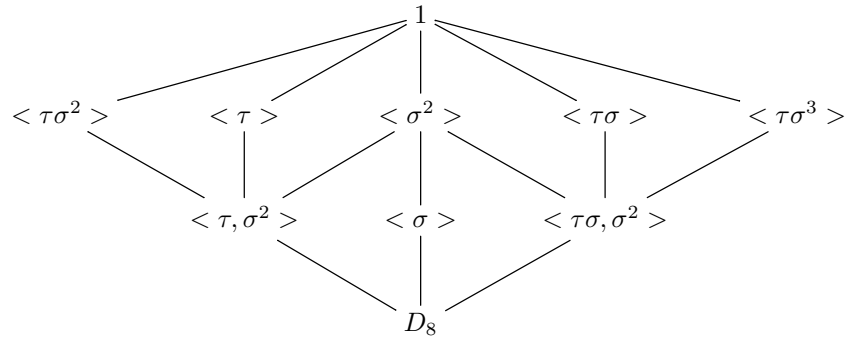
Enfin, si G est isomorphe à D_4, comme τ ne fixe ni $\alpha\beta$ ni $\dfrac{\alpha}{\beta}-\dfrac{\beta}{\alpha}$, ces quantités ne sont pas rationnelles.

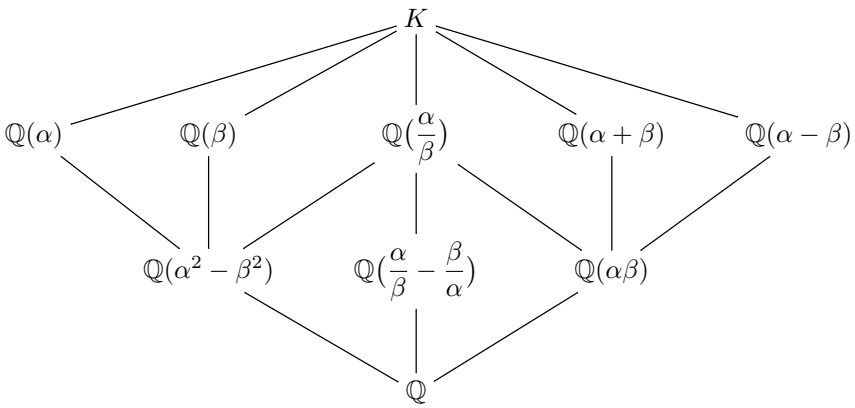
Les cas envisagés étant exclusifs (car si G fixait $\alpha\beta$ et $\dfrac{\alpha}{\beta}-\dfrac{\beta}{\alpha}$, on aurait $\alpha^2-\beta^2\in\mathbb{Q}$, ce qui est exclu), les implications prouvées deviennent des équivalences.

4. Pour chacun des polynômes suivants, déterminer le groupe de Galois et faire la liste des sous-corps d'un corps de décomposition :

(i) $f_1=X^4-4X^2-1$;

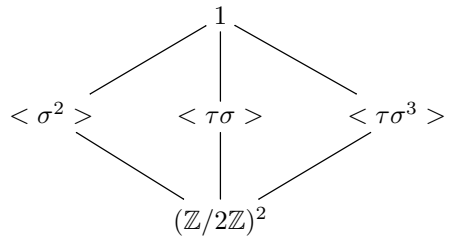
Indications : On a $f_1 = X^4 - 4X^2 - 1 = (X^2-2)^2 - 5 = (X^2 - 2 - \sqrt{5})(X^2 - 2 + \sqrt{5})$. Ses racines sont $\pm\alpha = \pm\sqrt{2+\sqrt{5}}$ et $\pm\beta = \pm i\sqrt{\sqrt{5}-2}$. Il est irréductible puisque α^2, β^2 et $\alpha \pm \beta$ ne sont pas rationnels. On calcule $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} = 2i\sqrt{5} \notin \mathbb{Q}$ et $\alpha\beta = i \notin \mathbb{Q}$: son groupe de Galois est donc isomorphe à D_8 et est constitué de tous les éléments exhibés en 3. On a les treillis de sous-groupes et de sous-corps suivants.

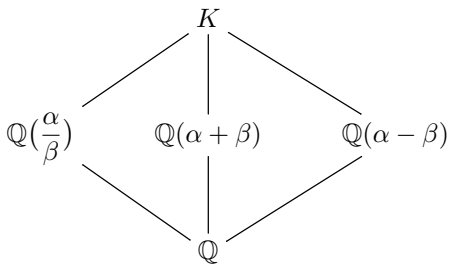




(ii) $f_2 = X^4 - 6X^2 + 4$;

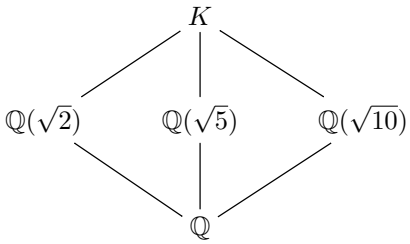
Indications : Les racines de f_2 sont $\pm\alpha = \pm\sqrt{3+\sqrt{5}}$ et $\pm\beta = \pm\sqrt{3-\sqrt{5}}$. Le polynôme f_2 est irréductible puisque α^2, β^2 et $\alpha \pm \beta$ ne sont pas rationnels. On calcule $\alpha\beta = 2 \in \mathbb{Q}$: son groupe de Galois est donc isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ et est constitué des éléments $Id, \sigma^2, \tau\sigma, \tau\sigma^3$ de 3. On a les treillis de sous-groupes et de sous-corps suivants.





(iii) $f_3 = X^4 - 7X^2 + 10$;

Indications : Le polynôme f_3 n'est pas irréductible. On a $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. On a donc $G = (\mathbb{Z}/2\mathbb{Z})^2$ et le treillis de sous-corps est :



(iv) $f_4 = X^4 + 5X^2 + 5$.

Indications : Les racines de f_4 sont $\pm\alpha = \pm i\sqrt{\frac{5+\sqrt{5}}{2}}$ et $\pm\beta = \pm i\sqrt{\frac{5-\sqrt{5}}{2}}$. Le polynôme f_4 est irréductible (Eisenstein). On calcule $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} = 1 \in \mathbb{Q}$: son groupe de Galois est donc isomorphe à $\mathbb{Z}/4\mathbb{Z}$ et est constitué des éléments $Id, \sigma, \sigma^2, \sigma^3$ de 3. Les sous-corps sont donc K, $\mathbb{Q}\left(\frac{\alpha}{\beta}\right)$ et $\mathbb{Q}$.

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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

> **Indications :** Soit $M = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Le corps K est contenu dans M. De plus, le groupe $\mathrm{Gal}(M/\mathbb{Q})$ s'identifie à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et ses éléments sont donnés par :
>
> $$\sigma_i : \begin{array}{ccc} \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & \sqrt{3} \end{array}, \quad \sigma_j : \begin{array}{ccc} \sqrt{2} & \mapsto & \sqrt{2} \\ \sqrt{3} & \mapsto & -\sqrt{3} \end{array}, \quad \sigma_k : \begin{array}{ccc} \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & -\sqrt{3} \end{array}.$$
>
> On vérifie aisément que $\sigma_i(\alpha) \neq \alpha$, $\sigma_j(\alpha) \neq \alpha$ et $\sigma_k(\alpha) \neq \alpha$, ce qui montre que $K = M$. Par conséquent, 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.

> **Indications :** Avec les notations de la question précédente, on calcule :
>
> $$\frac{\sigma_k(\alpha)}{\alpha} = (\sqrt{2}-1)^2, \quad \frac{\sigma_j(\alpha)}{\alpha} = (\sqrt{3}-\sqrt{2})^2, \quad \frac{\sigma_i(\alpha)}{\alpha} = (-2+\sqrt{2}-\sqrt{3}+\sqrt{6})^2.$$

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

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

> **Indications :** Supposons $\delta \in K$. Alors σ_k est bien définie sur $L = K$ et on a $\dfrac{\sigma_k(\delta)}{\delta} = \pm(\sqrt{2}-1)$. On calcule ensuite
>
> $$1 = \frac{\sigma_k^2(\delta)}{\sigma_k(\delta)} \cdot \frac{\sigma_k(\delta)}{\delta} = (-\sqrt{2}-1)(\sqrt{2}-1) = -1,$$
>
> ce qui n'est pas possible. On a donc $\delta \notin K$ et L/K est de degré 2, galoisienne de groupe de Galois isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

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.

> **Indications :** On pose simplement $\widetilde{\sigma}_i(\delta) = (-2+\sqrt{2}-\sqrt{3}+\sqrt{6})\delta$ et $\widetilde{\sigma}_j(\delta) = (\sqrt{3}-\sqrt{2})\delta$. Ces morphismes sont bien définis puisque le polynôme minimal de δ sur K est $X^2 - \alpha$. On a donc besoin (et cela suffit) que $\widetilde{\sigma}_j(\delta)$ soit zéro de $X^2 - \sigma_j(\alpha)$, c'est-à-dire de $X^2 - (\sqrt{3}-\sqrt{2})^2\alpha$.

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 $\mathbb{H}_8$.

> **Indications :** Comme on a $L = \mathbb{Q}(\delta)$, il suffit de vérifier les relations entre $\widetilde{\sigma}_i, \widetilde{\sigma}_j, \widetilde{\sigma}_k$ et τ en δ pour conclure. On a par définition $\widetilde{\sigma}_i\widetilde{\sigma}_j = \widetilde{\sigma}_k$. Aussi, on calcule :
>
> $$\widetilde{\sigma}_i^2(\delta) = (-2-\sqrt{2}-\sqrt{3}-\sqrt{6})(-2+\sqrt{2}-\sqrt{3}+\sqrt{6})\delta = -\delta = \tau(\delta),$$
>
> $$\widetilde{\sigma}_k^2(\delta) = (-\sqrt{2}-1)(\sqrt{2}-1)\delta = -\delta = \tau(\delta),$$
>
> $$\widetilde{\sigma}_j^2(\delta) = (-\sqrt{3}-\sqrt{2})(\sqrt{3}-\sqrt{2})\delta = -\delta = \tau(\delta).$$
>
> Ces quatre relations suffisent à établir le groupe engendré G : il est d'ordre 8, isomorphe à $\mathbb{H}_8$. En particulier, l'extension $\mathbb{Q} \subseteq L$, qui est de degré 8, est galoisienne et on a $G = \mathrm{Gal}(L/\mathbb{Q})$.

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

> **Indications :** Il y en a autant que de sous-groupes de $\mathbb{H}_8$ d'ordre 4 : autrement dit, il y en a 3. Ce sont $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ et $\mathbb{Q}(\sqrt{6})$.

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 $n = 4$?

> **Indications :** Voir le corrigé de l'examen 2011.

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.

> **Indications :** Comme P est irréductible, le groupe de Galois de L/K est un sous-groupe de S_3 d'ordre un multiple de 3 : c'est $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ ou bien $S_3 \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

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

> **Indications :** Dans les deux cas, on voit bien que $\mathrm{Gal}(L/K)$ possède un sous-groupe H normal d'ordre 3 : il est engendra par le 3-cycle (vu dans le groupe de permutations des racines) $\alpha \rightsquigarrow \beta \rightsquigarrow \gamma \rightsquigarrow \alpha$, que l'on notera σ.

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

> **Indications :** On calcule
>
> $$\sigma(\alpha + j\beta + j^2\gamma)^3 = (\beta + j\gamma + j^2\alpha)^3 = (j^2)^3(\alpha + j\beta + j^2\gamma)^3 = (\alpha + j\beta + j^2\gamma)^3.$$
>
> De même on a
>
> $$\sigma(\alpha + j^2\beta + j\gamma)^3 = (\beta + j^2\gamma + j\alpha)^3 = j^3(\alpha + j^2\beta + j\gamma)^3 = (\alpha + j^2\beta + j\gamma)^3.$$
>
> On en déduit $(\alpha + j\beta + j^2\gamma)^3, (\alpha + j^2\beta + j\gamma)^3 \in L^H$.

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

Indications : On note $\delta = (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)$; on remarque qu'il est fixé par σ mais pas par un éventuel (s'il existe) élément d'ordre 2 de $\mathrm{Gal}(L/K)$. On a alors $L^H = K(\delta)$, et on a besoin d'évaluer $(\alpha+j\beta+j^2\gamma)^3, (\alpha+j^2\beta+j\gamma)^3 \in K(\delta)$. On écrit

$$\begin{aligned}(\alpha+j\beta+j^2\gamma)^3 &= (\alpha^3+\beta^3+\gamma^3) + 3j(\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha) + 3j^2(\alpha^2\gamma+\beta^2\alpha+\gamma^2\beta) + 6\alpha\beta\gamma \\ &= (\alpha+\beta+\gamma)^3 + (3j-3)(\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha) + (3j^2-3)(\alpha^2\gamma+\beta^2\alpha+\gamma^2\beta).\end{aligned}$$

En utilisant $\alpha+\beta+\gamma = 0$ et $(\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\gamma\alpha) = 0$, on a :

$$(\alpha+j\beta+j^2\gamma)^3 = (3j-3)\big(-\frac{1}{2}\delta+\frac{3}{2}b\big) + (3j^2-3)\big(\frac{1}{2}\delta+\frac{3}{2}b\big) = \frac{3}{2}(j^2-j)\delta - \frac{27}{2}b.$$

De même, on calcule :

$$\begin{aligned}(\alpha+j^2\beta+j\gamma)^3 &= (\alpha^3+\beta^3+\gamma^3) + 3j(\gamma\alpha^2+\alpha\beta^2+\beta\gamma^2) + 3j^2(\alpha\gamma^2+\beta\alpha^2+\gamma\beta^2) + 6\alpha\beta\gamma \\ &= (3j^2-3)\big(-\frac{1}{2}\delta+\frac{3}{2}b\big) + (3j-3)\big(\frac{1}{2}\delta+\frac{3}{2}b\big) \\ &= \frac{3}{2}(j-j^2)\delta - \frac{27}{2}b.\end{aligned}$$

On se rappelle ensuite $\delta^2 = -4a^3 - 27b^2$ que l'on remplace dans

$$3\alpha = (\alpha+\beta+\gamma) + (\alpha+j\beta+j^2\gamma) + (\alpha+j^2\beta+j\gamma) = (\alpha+j\beta+j^2\gamma) + (\alpha+j^2\beta+j\gamma),$$

$$3\beta = j^2(\alpha+j\beta+j^2\gamma) + j(\alpha+j^2\beta+j\gamma),$$

$$3\gamma = j(\alpha+j\beta+j^2\gamma) + j^2(\alpha+j^2\beta+j\gamma),$$

pour retrouver les formules de Cardan.

Polynômes de degré 4 : Prenons $P = X^4 + aX^2 + bX + c$ irréductible sur K et notons x, y, z, t ses racines dans un corps de décomposition M. On suppose encore que K contient j, une racine primitive 3-ème de l'unité. Le groupe de Galois G de M/K est un sous-groupe de S_4 et on va exploiter la tour (non complète) de sous-groupes normaux, et donc d'extensions galoisiennes, suivants

$$\begin{array}{ccc} 1 & & M \\ | & & | \\ G \cap V_4 & & L \\ | & & | \\ G & & K \end{array}$$

où V_4 désigne le groupe de Klein, isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et engendré par les doubles transpositions. On note ensuite

$$u = (x+y)(z+t), \quad v = (x+z)(y+t), \quad w = (x+t)(y+z),$$

qui sont dans $L = M^{G \cap V_4}$ et sont les racines du polynôme de degré 3 suivant :

$$X^3 - 2aX^2 + (a^2 - 4c)X + b^2 \in \mathbb{Q}[X].$$

Par 4., on dispose donc d'expressions explicites pour u, v, w et il s'agit d'en déduire pour x, y, z, t à partir de ces dernières.
Comme on a $x + y + z + t = 0$ et $(x + y)(z + t) = u$, on choisit une racine $\sqrt{-u}$ de $-u$ pour écrire $x + y = \sqrt{-u}$ et $z + t = -\sqrt{-u}$. De même on choisit $x + z = \sqrt{-v}$ et $y+t = -\sqrt{-v}$; cela fixe le choix de $x+t = \sqrt{-w}$ puisque l'on a $(x+y)(x+z)(x+t) = -b$.
On exploite enfin

$$2x = (x+y) + (x+z) + (x+t) = \sqrt{-u} + \sqrt{-v} + \sqrt{-w},$$

$$2y = \sqrt{-u} - \sqrt{-v} - \sqrt{-w}, \quad 2z = -\sqrt{-u} + \sqrt{-v} - \sqrt{-w}, \quad 2t = -\sqrt{-u} - \sqrt{-v} + \sqrt{-w},$$

pour conclure.

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.

Indications : Comme L/K est galoisienne, son groupe de Galois est d'ordre $[L : K] = 3$ et est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

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.

Indications : Soit $x \in L \setminus K$. Cet élément x est de degré 3 et est donc zéro d'un polynôme $P \in K[X]$ irréductible de degré 3. Parce que L/K est galoisienne, L contient les autres racines de P et L est donc 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.

Indications : Prendre $K = \mathbb{Q}$ et $P = X^3 - 2$. Son corps de décomposition est de degré 6 sur $\mathbb{Q}$ et son groupe de Galois est ainsi isomorphe à S_3.

Soient σ l'automorphisme de corps qui fixe les éléments de K et qui envoie X sur

$\frac{1}{1-X}$ et G le sous-groupe de $\mathrm{Gal}(K(X)/K)$ engendré par σ.

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

> **Indications :** On a $\left(\frac{1}{1-X}\right)^{\circ 2} = \frac{X-1}{X}$ et $\left(\frac{1}{1-X}\right)^{\circ 3} = X$. En particulier, cela implique que σ est un automorphisme de $K(X)$.

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.

> **Indications :** Soit $T = X + \sigma(X) + \sigma^2(X) = \frac{X^3 - 3X + 1}{X^2 - X}$. Le corps fixe $K(X)^G$ contient $K(T)$ et l'extension $K(T) \subseteq K(X)$ est de degré majoré par 3 puisque l'on a $X^3 - TX^2 + (T-3)X + 1 = 0$. Enfin $K(X)^G \subseteq K(X)$ est non triviale puisque X n'est pas fixe par G. De ce fait, on a $K(X)^G = K(T)$; en particulier, X étant de degré 3 sur $K(X)^G$ par lemme d'Artin, $U^3 - TU^2 + (T-3)U + 1 \in K(T)[U]$ est irréductible (cela pouvait bien sûr aussi se voir directement) et $K(X)$ est son corps de décomposition : l'extension $K(T) \subseteq K(X)$ est galoisienne.

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.

> **Indications :** Soient L le corps de décomposition de P sur K et $\alpha \in L$ une racine de P. Les autres racines de P sont donc $\frac{1}{1-\alpha}$ et $\frac{\alpha - 1}{\alpha}$ (puisque X, $\sigma(X)$ et $\sigma^2(X)$ sont les racines de $U^3 - TU^2 + (T-3)U + 1$) et on a $L = K(\alpha)$. De ce fait, L est galoisienne de degré 3 sur K.
> *Remarque :* Pour $K = \mathbb{Q}$, le théorème d'irréductibilité de Hilbert nous assure l'existence d'une infinité de tels $t \in K$. Il est aussi facile de vérifier quand P a une racine ou non dans $\mathbb{Q}$...

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

> **Indications :** Dans ce cas-là, σ est un automorphisme d'ordre 4, et on prend $T = X + \sigma(X) + \sigma^2(X) + \sigma^3(X) = \frac{X^4 - 6X^2 + 1}{X^3 - X}$. Les $t \in K$ tels que le polynôme $X^4 - tX^3 - 6X^2 + tX + 1 \in K[X]$ soit irréductible fournissent alors une famille d'extensions galoisiennes de K de groupes de Galois $\mathbb{Z}/4\mathbb{Z}$.

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 $L = K(x)$.

> **Indications :** Voir le corrigé du partiel 2011.

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 $L = \mathbb{F}_q(x)$.

> **Indications :** Comme $\mathbb{F}_q$ est parfait, P est séparable. On a sait aussi que $\mathrm{Gal}(L/\mathbb{F}_q)$ est un groupe cyclique. La question 1 permet donc de conclure.

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 $\left(\frac{x}{p}\right) = 1$ si x est un carré dans $\mathbb{F}_p$, $\left(\frac{x}{p}\right) = -1$ sinon. C'est le symbole de Legendre.

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

Indications :

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

Indications : Comme p est impair, le polynôme $X^8 - 1$ est séparable et a 8 racines distinctes dans $\overline{\mathbb{F}_p}$. Comme seules 4 d'entre elles sont racines de $X^4 - 1$, $\overline{\mathbb{F}_p}$ possède une racine primitive 8-ème de l'unité α. De plus, α vérifie alors $\alpha^4 + 1 = 0$ et $\alpha^{\pm 2}$ sont racines de $X^2 + 1$. Ils vérifient donc $\alpha^{\pm 2} + \alpha^{\mp 2} = 0$. Il s'ensuit $\left(\pm(\alpha + \alpha^{-1})\right)^2 = 2$ et ce sont les racines de $X^2 - 2$ dans $\overline{\mathbb{F}_p}$. Il reste à examiner si $\alpha + \alpha^{-1}$ appartient à $\mathbb{F}_p$ ou non.
Si $p = \pm 1$ modulo 8, alors on a $(\alpha + \alpha^{-1})^p = \alpha^p + \alpha^{-p} = \alpha^{\pm 1} + \alpha^{\mp 1}$ et donc $\alpha + \alpha^{-1}$ est dans $\mathbb{F}_p$. Si $p = 3$ modulo 8, alors $\alpha^p + \alpha^{-p} = \alpha^3 + \alpha^{-3}$; et de même pour $p = -3$ modulo 8. Or on sait $0 = (\alpha + \alpha^{-1})(\alpha^2 + \alpha^{-2}) = \alpha^3 + \alpha^{-3} + \alpha + \alpha^{-1}$. Ainsi, si $p = \pm 3$ modulo 8, $\alpha + \alpha^{-1}$ n'appartient pas à $\mathbb{F}_p$.

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 $S = \sum_{x \in \mathbb{F}_\ell^\times} \left(\frac{x}{\ell}\right) \xi^x$ la somme de Gauss correspondante.

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

Indications : On calcule :

$$\begin{aligned} S^2 &= \sum_{x \in \mathbb{F}_\ell^\times} \sum_{y \in \mathbb{F}_\ell^\times} \left(\frac{xy}{\ell}\right) \xi^{x+y} \\ &= \sum_{c \in \mathbb{F}_\ell^\times} \sum_{x \in \mathbb{F}_\ell^\times} \left(\frac{cx^2}{\ell}\right) \xi^{(c+1)x} \\ &= \sum_{c \in \mathbb{F}_\ell^\times} \left(\frac{c}{\ell}\right) \sum_{x \in \mathbb{F}_\ell^\times} \xi^{(c+1)x} \\ &= (\ell - 1)\left(\frac{-1}{\ell}\right) - \sum_{c \in \mathbb{F}_\ell^\times \setminus \{-1\}} \left(\frac{c}{\ell}\right) = \ell (-1)^{\frac{\ell-1}{2}}. \end{aligned}$$

4. En déduire la loi de réciprocité quadratique :

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

Indications : On vérifie si S appartient à $\mathbb{F}_p$: comme p est impair, on a $S^p = \sum_{x \in \mathbb{F}_\ell^\times} \left(\frac{x}{\ell}\right) \xi^{xp}$. D'où $S^p = \sum_{y \in \mathbb{F}_\ell^\times} \left(\frac{p}{\ell}\right)^{-1} \left(\frac{y}{\ell}\right) \xi^y = \left(\frac{p}{\ell}\right) S$. On en déduit $\left(\frac{(-1)^{\frac{\ell-1}{2}} \ell}{p}\right) = \left(\frac{p}{\ell}\right)$, c'est-à-dire $\left(\frac{p}{\ell}\right)\left(\frac{\ell}{p}\right) = \left(\frac{(-1)^{\frac{\ell-1}{2}}}{p}\right) = (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}$. C'est bien la loi de réciprocité quadratique voulue.