Université de Tours
Master de Mathématiques

Solutions Td 6 : Correspondance de Galois (1)

M1, Algèbre — Semestre 2

Exercice 1 Soit $\mathbb{E} = \mathbb{Q}(\sqrt{2}, i)$ et $G = \mathsf{Gal}(\mathbb{E} : \mathbb{Q})$.

1) Montrer que $\mathbb{E} : \mathbb{Q}$ est un extension de Galois et déterminer G.
2) Pour tout sous groupe $H \leq G$ calculer $\mathrm{Fix}(H)$ et écrire la correspondance de Galois.

Solution:
The field $\mathbb{E}$ is the splitting field of the polynomial $f(x) = (x^2 - 2)(x^2 + 1)$, and thus $\mathbb{E} : \mathbb{Q}$ is a Galois.

Since $\mathbb{E} : \mathbb{Q}$ is a Galois extension we have $|G| = [\mathbb{E} : \mathbb{Q}]$. Thus

$$|G| = [\mathbb{E} : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4.$$

If $\theta \in G$ then θ permutes the roots of $x^2 - 2$ and $x^2 + 1$, and thus $\theta(\sqrt{2}) = \pm\sqrt{2}$ and $\theta(i) = \pm i$. Thus $G = \{\theta_1, \theta_2, \theta_3, \theta_4\}$ where the 4 elements of the Galois group are given by

$$\theta_1 : \begin{matrix} \sqrt{2} \mapsto \sqrt{2} \\ i \mapsto i \end{matrix} \qquad \theta_2 : \begin{matrix} \sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto i \end{matrix}$$
$$\theta_3 : \begin{matrix} \sqrt{2} \mapsto \sqrt{2} \\ i \mapsto -i \end{matrix} \qquad \theta_4 : \begin{matrix} \sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto -i \end{matrix}$$

The only groups of order 4 are C_4 or $C_2 \times C_2$, and since every element of $\mathrm{Gal}(E : \mathbb{Q})$ has order 2 (by direct calculation) we conclude that $\mathrm{Gal}(E : \mathbb{Q}) \cong C_2 \times C_2$ (this is called the *Klein four group* for historical reasons).
Recall that $C_2 \times C_2$ has presentation

$$C_2 \times C_2 = \langle s, t \mid s^2 = t^2 = 1,\ st = ts \rangle.$$

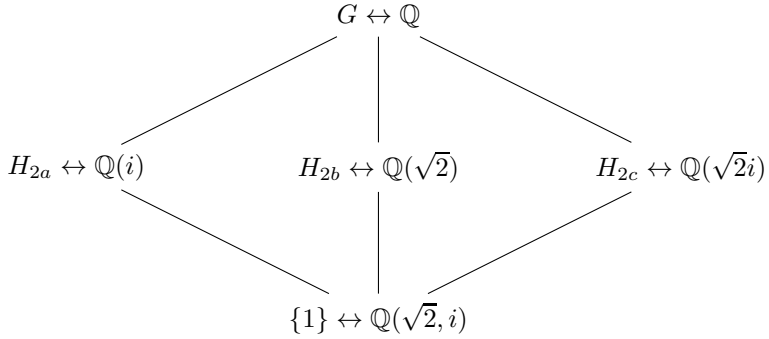
Thus the map $\varphi : C_2 \times C_2 \to \mathrm{Gal}(E : F)$ with $\varphi(s) = \theta_2$ and $\varphi(t) = \theta_3$ is an isomorphism.
The subgroups of $G = C_2 \times C_2$ (or $\mathrm{Gal}(E : \mathbb{Q})$) are $\{1\}$, G, and

$$H_{2a} = \langle s \rangle = \{1, s\}$$
$$H_{2b} = \langle t \rangle = \{1, t\}$$
$$H_{2c} = \langle st \rangle = \{1, st\}.$$

Every element of $\mathbb{E}$ can be written as $x = a + b\sqrt{2} + ci + d\sqrt{2}i$ with $a, b, d, c \in \mathbb{Q}$ in a unique way. To compute $\mathrm{Fix}(H_{2a})$ we find the elements $x \in E$ with $\theta_2(x) = x$. We have

$$\theta_2(x) = a - b\sqrt{2} + ci - d\sqrt{2}i,$$

and so $\theta_2(x) = x$ if and only if $b = d = 0$. Thus $\mathrm{Fix}(H_{2a}) = \mathbb{Q}(i)$. Similarly, $\mathrm{Fix}(H_{2b}) = \mathbb{Q}(\sqrt{2})$, and $\mathrm{Fix}(H_{2c}) = \mathbb{Q}(\sqrt{2}i)$ (for this calculation, note that $st \leftrightarrow \theta_4$). Finally, $\mathrm{Fix}(\{1\}) = \mathbb{Q}(\sqrt{2}, i)$, and $\mathrm{Fix}(G) = \mathbb{Q}$. We arrange the correspondence in the following diagram. Note that the Galois correspondence is inclusion reversing :



Exercice 2 Soit $t = \sqrt{1+\sqrt{2}}$ et soit E le corps de décomposition du polynôme minimal m de t sur $\mathbb{Q}$.

1) Déterminer $m(x)$ et E.
2) Déterminer l'ordre de $G = \mathrm{Gal}(E : \mathbb{Q})$.
3) Déterminer $G = \mathrm{Gal}(E : \mathbb{Q})$.
4) Déterminer tous les sous-groupes de G. Pour chaque sous-groupe H of G, déterminer le sous-corps de L de E associé par la correspondance de Galois. Présenter vos résultats sous la forme de deux diagrammes : l'un représentant les sous-groupes de G et l'autre les sous-corps de E.

Solution: 1. On a $t^2 - 1 = \sqrt{2}$ et donc $(t^2-1)^2 = 2$. Ainsi t est une racine de $m = X^4 - 2X^2 - 1$. Montrons que ce polynôme est irréductible.

Méthode 1. Les seules racines rationnelles de m possibles sont ± 1 et ni 1, ni -1 n'est racine de m. Ainsi, si m se factorise sur $\mathbb{Q}$, c'est nécessairement comme un produit de deux polynômes irréductibles de degré 2 à coefficients dans $\mathbb{Q}$. Le polynôme m admet deux racines réelles t et $-t$ et deux racines complexes (non-réelles) conjuguées $t' := i\sqrt{\sqrt{2}-1}$ et $-t'$. Ainsi la factorisation de m en irréductibles sur $\mathbb{R}$ est :

$$m = (X-t)(X+t)(X^2 + (\sqrt{2}-1))$$

Le polynôme $X^2 + (\sqrt{2}-1)$ n'étant pas à coefficients dans $\mathbb{Q}$, on voit, par unicité de la décomposition en irréductibles, que m ne peut pas se factoriser comme un produit de deux polynômes irréductibles de degré 2 à coefficients dans $\mathbb{Q}$.

Méthode 2. On a $m(X+1) = X^4 + 4X^3 + 4X^2 - 2$ et le critère d'Eisenstein avec $p = 2$ montre que $m(X+1)$ est irréductible et donc que m est irréductible.

Le corps de décomposition de m est

$$\mathbb{Q}(t, -t, t', -t') = \mathbb{Q}(t, t').$$

On remarque que $t \cdot t' = i$ ainsi, $\mathbb{Q}(t,t') = \mathbb{Q}(t,i)$.

2. Puisque E est le corps de décomposition de m sur $\mathbb{Q}$, on a $|G| = [E : \mathbb{Q}]$. Comme t est réel, on obtient

$$[E : \mathbb{Q}] = [\mathbb{Q}(t,i) : \mathbb{Q}(t)] \cdot [\mathbb{Q}(t); \mathbb{Q}] = 2 \cdot 4 = 8$$

Ainsi G est de cardinal 8.

3. Soit $\theta \in G$. Puisque $E = \mathbb{Q}(t,i)$ pour déterminer θ il suffit de déterminer $\theta(i)$ et $\theta(t)$. De plus

- θ permute les racines de X^2+1 et donc $\theta(i) \in \{i, -i\}$;
- θ permute les racines de m et donc $\theta(t) \in \{t, -t, t', -t'\}$.

On a donc 8 possibilités pour θ et comme $|G| = 8$, chaque choix donne un élément du groupe G. Les élements de G sont donc les $\{\theta_i\}_{1 \le 1 \le 8}$ décrit ci-dessous. Comme cela sera utile dans la suite de l'exercice, on indique également la valeur de $\theta_i(t')$ qui peut-être calculer à partir de $\theta(t)$ et $\theta(i)$ en utilisant $t \cdot t' = i$.

$$\begin{cases} \theta_1(t) = t \\ \theta_1(i) = i \\ \theta_1(t') = t' \end{cases} \quad \begin{cases} \theta_2(t) = t \\ \theta_2(i) = -i \\ \theta_2(t') = -t' \end{cases} \quad \begin{cases} \theta_3(t) = -t \\ \theta_3(i) = i \\ \theta_3(t') = -t' \end{cases} \quad \begin{cases} \theta_4(t) = -t \\ \theta_4(i) = -i \\ \theta_4(t') = t' \end{cases}$$

$$\begin{cases} \theta_5(t) = t' \\ \theta_5(i) = i \\ \theta_5(t') = t \end{cases} \quad \begin{cases} \theta_6(t) = t' \\ \theta_6(i) = -i \\ \theta_6(t') = -t \end{cases} \quad \begin{cases} \theta_7(t) = -t' \\ \theta_7(i) = i \\ \theta_7(t') = -t \end{cases} \quad \begin{cases} \theta_8(t) = -t' \\ \theta_8(i) = -i \\ \theta_8(t') = t \end{cases}$$

On doit encore travailler pour déterminer de quel type est G. Il ya 5 classes de groupes d'ordre 8 :

- 3 sont abéliens

$$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}), \quad (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}), \quad \mathbb{Z}/8\mathbb{Z},$$

- 2 ne sont pas abéliens

$$D_8 = \langle a, b \mid a^2 = b^2 = 1, \quad (ab)^4 = 1 \rangle \qquad \text{groupe dihédral d'ordre 8}$$
$$Q = \langle -1, i, j, k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle \qquad \text{groupe des quaternions.}$$

On remarque rapidement que G n'est pas abélien puisque

$$(\theta_4 \circ \theta_5)(t) = \theta_4(\theta_5(t)) = \theta_4(t') = t'$$
$$(\theta_5 \circ \theta_4)(t) = \theta_5(\theta_4(t)) = \theta_5(-t) = -t'$$

Ainsi G est soit le groupe dihédral soit le groupe des quaternions. Le groupe dihédral se présente sous la forme suivante

$$D_8 = \{1, a, b, ab, ba, aba, bab, abab\} \qquad \text{où } a^2 = b^2 = 1 \text{ et } (ab)^4 = 1.$$

Il y a 5 éléments d'ordre 2, et 2 éléments d'ordre 4.

le groupe des quaternions se présente sous la forme suivante

$$Q = \{1, -1, i, -i, j, -j, k, -k\} \qquad \text{où } (-1)^2 = 1,\ i^2 = j^2 = k^2 = ijk = -1,$$

Il y a 1 élément d'ordre 2, et 6 éléments d'ordres 4.

On peut donc déterminer G en calculant l'ordre de ses éléments. Un calcul élémentaire montre que θ_2, θ_3, θ_4, θ_5, et θ_7 sont d'ordre 2 et donc $G \cong D_8$.

On peut vérifier que $a \mapsto \theta_5$ and $b \mapsto \theta_4$ définit un isomorphisme de D_8 dans G.

4. D_8 a 8 sous-groupes (dès lors qu'un sous-groupe H contient a et b alors $H = D_8$). Il y a 3 sous-groupe d'ordre 4, et 5 d'ordre 2. On trouve ainsi tous les sous-groupes de G :

$$H_{2a} = \langle \theta_5 \rangle = \{1, \theta_5\}$$
$$H_{2b} = \langle \theta_4 \rangle = \{1, \theta_4\}$$
$$H_{2c} = \langle \theta_2 \rangle = \{1, \theta_2\}$$
$$H_{2d} = \langle \theta_7 \rangle = \{1, \theta_7\}$$
$$H_{2e} = \langle \theta_3 \rangle = \{1, \theta_3\}$$
$$H_{4a} = \langle \theta_8 \rangle = \{1, \theta_3, \theta_6, \theta_8\}$$
$$H_{4b} = \langle \theta_5, \theta_7 \rangle = \{1, \theta_3, \theta_5, \theta_7\}$$
$$H_{4c} = \langle \theta_2, \theta_4 \rangle = \{1, \theta_2, \theta_3, \theta_4\}.$$

Soit

$$L_{2a} = \mathrm{Fix}(H_{2a}), \quad L_{2b} = \mathrm{Fix}(H_{2b}), \quad L_{2c} = \mathrm{Fix}(H_{2c}), \quad \text{etc...}$$

les sous-corps de E fixés par ces sous-groupes. On rappelle que

$$[\mathrm{Fix}(H) : \mathbb{Q}] = |G|/|H|.$$

Calcul de L_{4c} Puisque H_{4c} est un groupe d'ordre 4, on sait que $L_{4c} : \mathbb{Q}$ est une extension de degré 2. De plus t^2 est fixé par tout $\theta \in H_{4c}$ et donc $\mathbb{Q}(t^2) \subset L_{4b}$. Mais $t^2 = 1 + \sqrt{2}$ et donc $[\mathbb{Q}(t^2) : \mathbb{Q}] = 2$. Ainsi

$$L_{4b} = \mathbb{Q}(1 + \sqrt{2}) = \mathbb{Q}(\sqrt{2}).$$

Calcul de L_{4b} Puisque H_{4b} est un groupe d'ordre 4, on sait que $L_{4b} : \mathbb{Q}$ est une extension de degré 2. De plus i est fixé par tout $\theta \in H_{4b}$ on en déduit que $\mathbb{Q}(i) \subset L_{4b}$ et donc $L_{4b} = \mathbb{Q}(i)$ puisque $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Calcul de L_{4a} Puisque H_{4a} est un groupe d'ordre 4, on sait que $L_{4a} : \mathbb{Q}$ est une extension de degré 2. Il est plus difficile ici de trouver un élément fixer par H_{4a}, mais on finit par trouver que $i\sqrt{2}$. Ainsi $L_{4a} = \mathbb{Q}(i\sqrt{2})$.

Calcul de L_{2e} On sait que $[L_{2e} : \mathbb{Q}] = 4$. Le groupe H_{2e} est engendré par θ_3 et i et $t^2 = 1 + \sqrt{2}$ sont stables par θ_3. Ainsi $\mathbb{Q}(i, \sqrt{2}) \subset L_{2e}$ ce qui implique, comme ces deux extensions sont de même degré, que

$$\mathbb{Q}(i, \sqrt{2}) = L_{2e}.$$

Calcul de L_{2d} On sait que $[L_{2d} : \mathbb{Q}] = 4$. Le groupe H_{2d} est engendré par θ_7 et i et $t - t'$ sont stables par θ_7. Ainsi $\mathbb{Q}(i, t - t') \subset L_{2e}$ ce qui implique,, comme ces deux extensions sont de même degré, que

$$\mathbb{Q}(i, t - t') = L_{2e}.$$

Calcul de L_{2c} On sait que $[L_{2c} : \mathbb{Q}] = 4$. Le groupe H_{2c} est engendré par θ_2 et $\sqrt{2}$ et t sont stables par θ_2. Ainsi $\mathbb{Q}(\sqrt{2}, t) \subset L_{2c}$ ce qui implique, comme ces deux extensions sont de même degré, que

$$\mathbb{Q}(\sqrt{2}, t) = L_{2c}.$$

Calcul de L_{2b} On sait que $[L_{2b} : \mathbb{Q}] = 4$. Le groupe H_{2b} est engendré par θ_4 et $\sqrt{2}$ et t' sont stables par θ_4. Ainsi $\mathbb{Q}(\sqrt{2}, t') \subset L_{2b}$ ce qui implique, comme ces deux extensions sont de même degré, que

$$\mathbb{Q}(\sqrt{2}, t') = L_{2b}.$$

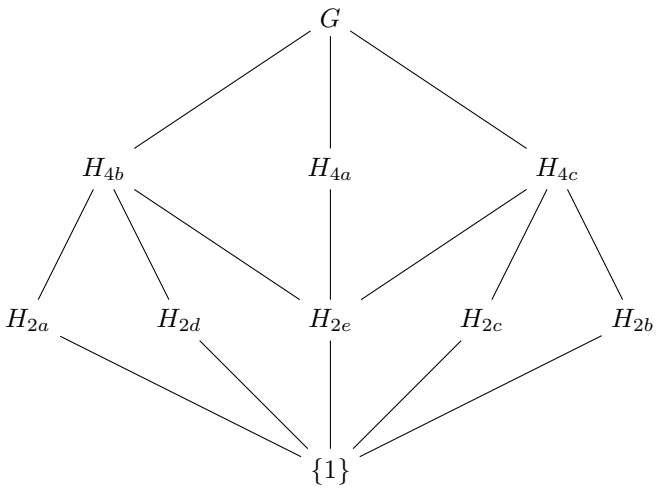
Calcul de L_{2a} On sait que $[L_{2a} : \mathbb{Q}] = 4$. Le groupe H_{2a} est engendré par θ_5 et i et $t + t'$ sont stables par θ_3. Ainsi $\mathbb{Q}(i, t + t') \subset L_{2a}$ ce qui implique, comme ces deux extensions sont de même degré, que

$$\mathbb{Q}(i, t + t') = L_{2a}.$$

En résumé, la correspondance de Galois est :

$$\begin{aligned}
H_{2a} &\longleftrightarrow \mathbb{Q}(i, t + t') & H_{2b} &\longleftrightarrow \mathbb{Q}(\sqrt{2}, t') \\
H_{2c} &\longleftrightarrow \mathbb{Q}(\sqrt{2}, t) & H_{2d} &\longleftrightarrow \mathbb{Q}(i, t - t') \\
H_{2e} &\longleftrightarrow \mathbb{Q}(\sqrt{2}, i) & H_{4a} &\longleftrightarrow \mathbb{Q}(i\sqrt{2}) \\
H_{4b} &\longleftrightarrow \mathbb{Q}(i) & H_{4c} &\longleftrightarrow \mathbb{Q}(\sqrt{2}).
\end{aligned}$$

Le graphe des sous-groupes de G est donné ci-dessous :



Le graphe correspondant des sous-corps L de E tel que $\mathbb{Q} \leq L \leq \mathbb{Q}(t, t')$: