Théorie de Galois - Interro 1

Vous pouvez traiter les exercices dans l'ordre qui vous convient. Prenez soin de bien justifier vos réponses et de bien présenter votre démarche; la qualité de la rédaction sera prise en compte dans la notation. Les calculatrices sont interdites. Le barème est donné à titre indicatif seulement. Des réponses partielles peuvent vous accorder une partie des points de la question en question. N'oubliez pas de numéroter vos pages.

1 Calcul d'un groupe de Galois

Soit $\mathbb{K}$ le corps de décomposition de $X^3 - 2 \in \mathbb{Q}[X]$.

1. (2 points) Justifier que $\mathbb{K}/\mathbb{Q}$ est une extension galoisienne et donner son degré.
2. (2 points) A quel groupe usuel est isomorphe $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$?

2 Vrai ou faux

Répondre en justifiant votre réponse par une preuve/un contre-exemple.

1. (2 points) On a $\mathrm{Gal}(\mathbb{Q}(e^{2i\pi/n})/\mathbb{Q}) \simeq \mathbb{Z}/\varphi(n)\mathbb{Z}$.

   Solution: On a vu en TD que l'on a

   $$\mathrm{Gal}(\mathbb{Q}(e^{2i\pi/n})/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$$

   de sorte que la question revient à savoir s'il y a un élément d'ordre $\varphi(n)$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ puisque ce groupe est d'ordre $\varphi(n)$.

   De plus, pour $n = 3 \times 5$, on a, d'après le lemme chinois

   $$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times.$$

   On remarque que $(\mathbb{Z}/3\mathbb{Z})^\times$ est un groupe d'ordre $\varphi(3) = 2$: il s'agit donc de $\mathbb{Z}/2\mathbb{Z}$. De plus, le groupe $(\mathbb{Z}/5\mathbb{Z})^\times$ est d'ordre $\varphi(5) = 4$. Ainsi, tous les éléments de $(\mathbb{Z}/15\mathbb{Z})^\times$ sont d'ordre divisant 4, de sorte que ce groupe ne saurait être cyclique (d'ordre 8).

2. (2 points) Il existe un entier n_0 tel que, pour tout $n \geqslant n_0$, il existe un nombre premier p et une extension $\mathbb{K}/\mathbb{F}_p$ de groupe de Galois $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Solution: Par l'absurde, supposons l'énoncé vrai. Fixons $n = n_0 + 2 \geqslant 2$, p et $\mathbb{K}$ comme énoncés. Puisque $\mathbb{K}$ est une extension finie de $\mathbb{F}_p$, on sait qu'il existe $q = p^e$ tel que $\mathbb{K} = \mathbb{F}_q$. On a vu en TD que l'on a $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ est cyclique. Or, dans le groupe $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ - qui est d'ordre n^2 - tous les éléments sont d'ordre divisant $n < n^2$, ce qui empêche ce dernier groupe d'être cyclique.

3. (3 points) Soit $\mathbb{L}/\mathbb{K}$ une extension galoisienne de degré 2^n. Il existe des sous-corps de $\mathbb{L}$ que l'on note $\mathbb{K}_0 = \mathbb{K} \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_n = \mathbb{L}$ tels que

$$\forall i \in [\![0, n[\![, \quad [\mathbb{K}_{i+1} : \mathbb{K}_i] = 2.$$

(On rappelle que le centre d'un 2-groupe est non trivial.)

Solution: Avec plein de sagesse, on suit sagement l'indication. Puisque $\mathbb{L}/\mathbb{K}$ est galoisienne finie, on a

$$|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$$

de sorte que $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est un 2-groupe. Par l'indication, le centre Z de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est non trivial. Remarquons que Z est un sous-groupe normal de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. La correspondance galoisienne assure qu'il existe $\mathbb{M}$ un corps intermédiaire tel que $Z = \mathrm{Gal}(\mathbb{L}/\mathbb{M})$ et tel que $\mathbb{M}/\mathbb{K}$ est galoisienne. On distigue maintenant deux cas.

Si $Z \neq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, c'est-à-dire si $\mathbb{M} \neq \mathbb{L}$, on constate que $[\mathbb{M} : \mathbb{K}]$ divise strictement $[\mathbb{L} : \mathbb{K}] = 2^n$. Ainsi, $\mathrm{Gal}(\mathbb{M}/\mathbb{K})$ et $\mathrm{Gal}(\mathbb{L}/\mathbb{M})$ sont des 2-groupes de cardinal plus petit que 2^n et on voit une récurrence apparaître naturellement. (Il conviendrait de réécrire cette preuve en commençant par dire que l'on travaille par récurrence forte, que le cas $n = 1$ est évident et que l'on s'attache maintenant à montrer la propriété "pour toute extension galoisienne $\mathbb{M}_2/\mathbb{M}_1$ de degré 2^n il existe une chaine de corps comme énoncé" mais par soucis pédagogique, je préférais vous montrer comment la récurrence apparaissait d'elle-même et on va faire comme si j'avais écrit tout ça en début de preuve.) Par récurrence, il existe donc deux chaînes d'extensions quadratiques

$$\mathbb{K} = \mathbb{K}_0 \subset \cdots \mathbb{K}_? = \mathbb{M}$$
$$\mathbb{M} = \mathbb{M}_0 \subset \cdots \mathbb{M}_{??} = \mathbb{L}$$

et il suffit de concaténer ces deux chaînes pour obtenir le résultat que l'on souhaitait avoir. Autrement dit, on pose

$$\forall i \in [\![? + 1, n]\!], \quad \mathbb{K}_i = \mathbb{M}_{i-?}.$$

Il convient de remarquer que l'on a $?+?? = n$ car le théorème de la base télescopique fournit

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}][\mathbb{M} : \mathbb{K}].$$

Si $Z = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, alors le groupe $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est abélien. Par le lemme de Cauchy, il existe un sous-groupe $H \leq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. De plus, le sous-groupe H est normal dans $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ puisque ce dernier est abélien. Ainsi, on peut de nouveau faire appel à l'hypothèse de récurrence en invoquant les mêmes arguments que précédemment après avoir remplacé Z par H.