Fiche 1
21 janvier 2015

Exercice 1 (Corps quadratiques).

1. Fixons $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{N}$. Montrer que $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$.
2. Soit $d \in \mathbb{N} \setminus \{0, 1\}$. Montrer que les conditions suivantes sont équivalentes :
   (a) $\sqrt{d} \notin \mathbb{Q}$,
   (b) $\sqrt{d} \notin \mathbb{N}$,
   (c) il existe un nombre premier p tel que la puissance la plus élevée divisant d soit impaire,
   (d) $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$.
3. Soient $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{N}$ et $\alpha \in \mathbb{Q}(\sqrt{d}) \setminus \mathbb{Q}$. Déterminer le polynôme minimal de α sur $\mathbb{Q}$.
4. Soit maintenant L un corps intermédiaire entre $\mathbb{Q}$ et $\mathbb{C}$, en d'autres termes, $\mathbb{Q} \leq L \leq \mathbb{C}$. On suppose que $[L : \mathbb{Q}] = 2$. Montrer qu'il existe $d \in \mathbb{Z}$ tel que $L = \mathbb{Q}(\sqrt{d})$. Montrer qu'on peut choisir d sans facteurs carrés.
5. Déterminer à isomorphisme près $\mathrm{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$.
6. Soient d et d' deux éléments de $\mathbb{Z} \setminus \{0, 1\}$, sans facteurs carrés et distincts. Montrer que les corps $\mathbb{Q}(\sqrt{d})$ et $\mathbb{Q}(\sqrt{d'})$ ne sont <u>pas</u> isomorphes.

Exercice 2 (Eléments algébriques, éléments transcendants).

1. On considère l'extension $\mathbb{Q}(u)$ où u est racine de $X^3 - X^2 + X + 2$. Vérifier que ce polynôme est irréductible dans $\mathbb{Q}[X]$. Exprimer $(u^2 + u + 1)(u^2 - u)$ et $(u - 1)^{-1}$ comme une combinaison $\mathbb{Q}$-linéaire de 1, u et u^2.
2. Si K/k est une extension algébrique, en d'autres termes une extension dont tout élément est algébrique sur k. Montrer que tout sous-anneau de K contenant k est un sous-corps.
3. On définit $K = \mathbb{Q}(t), K_1 = \mathbb{Q}(t^2), K_2 = \mathbb{Q}(t^2 - t)$ avec t transcendant sur $\mathbb{Q}$.
   Montrer que K est algébrique sur K_1, algébrique sur K_2 mais non sur $K_1 \cap K_2$. (*Indication : vérifier que* $K_1 \cap K_2 = \mathbb{Q}$).
4. Soient K un corps et $L = K(u)$, où u est transcendant sur K. Soit M un sous-corps de L, qui contient K strictement. Montrer que u est algébrique sur M.

Exercice 3 (Extensions, automorphismes).

I.

1. Montrer que $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$.
2. En déduire $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$.
3. Soit $\alpha = \sqrt{2} + \sqrt{3}$. Montrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$.
4. Déterminer le polynôme minimal P de α sur $\mathbb{Q}$ et toutes les racines de P.
5. Déterminer les automorphismes de $\mathbb{Q}(\alpha)$.
6. Soit K un sous-corps de $\mathbb{Q}(\alpha)$; en remarquant que le polynôme minimal de α sur K divise P dans $K[X]$, montrer que
$$K = \mathbb{Q},\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{6}) \text{ ou } \mathbb{Q}(\alpha).$$

II. On définit $w = e^{i\frac{\pi}{6}}$. Déterminer le polynôme minimal et le degré de l'extension $\mathbb{Q}(w)/\mathbb{Q}$.

III. Soient p et q deux nombres premiers. On considère le polynôme $P = X^p - q$ sur $\mathbb{Q}$.

1. Montrer que P est irréductible dans $\mathbb{Q}[X]$. Vérifier que les racines de P sont de la forme $q^{\frac{1}{p}}\ r^i$ avec $0 \leq i \leq p-1$ où r est une racine primitive pième de l'unité.
2. Montrer que le corps de décomposition de P dans $\mathbb{C}$ est $\mathbb{Q}(q^{\frac{1}{p}},\ r)$. On le notera L. Déterminer $[L : \mathbb{Q}]$.
3. On fixe $0 \leq i \leq p-1$. Déterminer la structure de $\mathrm{Aut}(\mathbb{Q}(q^{\frac{1}{p}}\ r^i)/\mathbb{Q})$ suivant les valeurs de p.
4. Montrer que $\mathrm{Aut}(L/\mathbb{Q})$ stabilise $\mathbb{Q}(r)$.
5. Montrer que $|\mathrm{Aut}(L/\mathbb{Q})| = p(p-1)$. Expliciter ses éléments. Montrer que ce groupe a un sous-groupe distingué d'ordre p.

IV. Déterminer les corps de décomposition ainsi que les degrés de ceux-ci sur $\mathbb{F}_p$ pour les polynômes $X^{p^n} - 1$, avec $n \in \mathbb{N}$.

Exercice 4 (Eléments primitifs, une première rencontre).

Soit $K \leq E$ une extension de corps de degré fini et qui jouit de la propriété suivante : pour toute paire de sous-corps E_1 et E_2, soit $E_1 \leq E_2$ soit $E_2 \leq E_1$. Montrer qu'il existe un élément $\alpha \in E$ tel que $E = K(\alpha)$.