Université Paris 7 **31 octobre 2016**
Algèbre

TD6 : morphismes et groupe de Galois

Exercice 1 :

Déterminer $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{R})$ et $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, i\sqrt{3}), \mathbb{C})$.

Exercice 2 :

Déterminer $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{R})$ et $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{C})$.

Exercice 3 :

Montrer que si $L = K(a_1, \ldots a_n)$, alors tout morphisme $\phi \in \mathrm{Hom}_K(L, L')$ est entièrement déterminé par les images $\phi(a_1), \ldots \phi(a_n)$.

Exercice 4 :

On considère le corps de décomposition L de $x^4 - 2$ sur $\mathbb{Q}$.

1. On note $\alpha = \sqrt[4]{2}$. Montrer que $L = \mathbb{Q}(\alpha, i)$.
2. On pose $K_1 = \mathbb{Q}(\alpha)$. Déterminer $\mathrm{Hom}_{\mathbb{Q}}(K_1, L)$.
3. Montrer que $K_1 \simeq K_2 = \mathbb{Q}(i\alpha)$, et déterminer $\mathrm{Hom}_{\mathbb{Q}}(K_1, K_2)$.
4. Déterminer $\mathrm{Gal}(L/\mathbb{Q})$.

Exercice 5 :

Soit L/K une extension finie de K un corps de caractéristique nulle. En utilisant le théorème de l'élément primitif, redémontrer que pour toute extension L'/K, $\#\,\mathrm{Hom}_K(L, L') \leqslant [L : K]$ et préciser le cas d'égalité. On donnera des exemples où l'on a égalité et inégalité stricte.

Exercice 6 :

On considère la racine de l'unité $\zeta = e^{\frac{2i\pi}{n}} \in \mathbb{C}$, et l'extension cyclotomique $\mathbb{Q}(\zeta)/\mathbb{Q}$.

1. Montrer que $\mathbb{Q}(\zeta)/\mathbb{Q}$ est le corps de décomposition d'un polynôme séparable.
2. Soit $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, montrer que $\sigma(\zeta)$ est de la forme ζ^k pour un certain $0 \leqslant k < n$.
3. Montrer que l'entier k de la question précédente est premier à n.
4. Montrer que l'application $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ qui à σ associe la valeur k ainsi définie est un morphisme de groupes, et que ce morphisme est injectif.
5. On rappelle que le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$ est appelé $\varphi(n)$. Montrer que $[\mathbb{Q}(\zeta) : \mathbb{Q}] \mid \varphi(n)$.
6. Montrer que si $n = p$ est premier, alors on a un isomorphisme $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^*$.

Exercice 7 :

Soit L/K le corps de décomposition d'un polynôme $P \in K[x]$ à racines simples.

1. On note $x_1, \ldots x_n$ les racines de P dans L. Montrer que pour tout $\phi \in \mathrm{Hom}_K(L, \bar{L})$ et tout i, il existe j tel que $\phi(x_i) = x_j$.
2. Soit $\phi \in \mathrm{Hom}_K(L, \bar{L})$. Montrer que $\phi(L) \subset L$.
3. Montrer que $\phi(L) = L$.
4. En déduire que $\#\,\mathrm{Gal}(L/K) = [L : K]$.

Exercice 8 :

On considère le corps de décomposition L de $x^n - 2$ sur $\mathbb{Q}$.

1. Montrer que $x^n - 2$ est irréductible.

2. Déterminer deux éléments α, β tels que $L = \mathbb{Q}(\alpha, \beta)$.

3. Montrer que si $n = p$ est premier, alors $[L : \mathbb{Q}] = p(p-1)$.

Exercice 9 :

On dit que deux éléments α, β sont sont conjugués sur K s'il existe une extension L/K contenant α et β, et $\phi \in \mathrm{Gal}(L/K)$ tel que $\phi(\alpha) = \beta$.

1. Montrer que i et $-i$ sont conjugués sur $\mathbb{R}$, et que $\sqrt{2}$ et $-\sqrt{2}$ sont conjugués sur $\mathbb{Q}$.

2. Montrer que si α et β sont conjugués sur K, alors on a égalité des polynômes minimaux P_α et P_β.

3. $\sqrt{3}$ et $i\sqrt{3}$ sont-ils conjugués sur $\mathbb{Q}$?

4. Réciproquement, on suppose que α, β sont deux racines d'un polynôme irréductible $P \in K[x]$, et soit L un corps de décomposition de P. Montrer qu'il existe un automorphisme de L qui envoie α sur β.

5. En déduire que deux éléments sont conjugués sur K si et seulement si ils ont même polynôme minimal sur K.

1 Groupe de Galois

Exercice 10 :

On considère l'extension de corps finis $\mathbb{F}_{p^n}/\mathbb{F}_p$.

1. Montrer que l'automorphisme de Frobenius $\phi_p : x \mapsto x^p$ est un élément de $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

2. Montrer que ϕ_p est d'ordre n dans $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

3. Montrer que $\mathbb{Z}/n\mathbb{Z} \simeq \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, via $k \mapsto \phi_p \circ \ldots \phi_p$ (k-fois).

Exercice 11 :

Soit L/K l'extension de décomposition de $P(x) \in K[x]$. On note $x_1, \ldots x_n \in L$ ses racines, que l'on suppose deux à deux distinctes.

1. Montrer que tout élément σ de $\mathrm{Gal}(L/K)$ induit une permutation de $x_1, \ldots x_n$.

2. En déduire un morphisme injectif $\mathrm{Gal}(L/K) \to \mathfrak{S}_n$.

3. En déduire que $[L : K] \mid n!$.