ENS Lyon 2011 - 2012
Master 1

Algèbre Approfondie

18.10.2011

TD 5

Correspondance de Galois

Exercice 1.

Expliciter la correspondance de Galois sur $\mathbb{Q}$ des polynômes $(X^2-2)(X^2-3)$ et X^4-2 étudiés dans la feuille de TD précédente.

Exercice 2.

On note $P(X)$ le polynôme X^3-5. Soit L son corps de décomposition sur $\mathbb{Q}$.

1. Déterminer le degré de l'extension $L/\mathbb{Q}$.
2. Décrire le groupe de Galois G de P sur $\mathbb{Q}$.
3. Donner une représentation de chaque élément de G par une permutation de l'ensemble des racines de$P$.

Exercice 3.

On considère le polynôme $P(X) = X^4 - 3$.

1. Montrer que $P(X)$ est irréductible sur $\mathbb{Q}(i)$.
2. Déterminer le corps de décomposition, L, et le groupe de Galois, G, de $P(X)$ sur le corps $\mathbb{Q}(i)$.
3. Donner la correspondance de Galois entre les sous-groupes de G et les sous-extensions de $L/\mathbb{Q}(i)$.
4. Pour chaque extension intermédiaire de $L/\mathbb{Q}(i)$, donner la factorisation du polynôme P.

Exercice 4.

1. Soit $M = \mathbb{Q}(\sqrt[3]{2})$. Montrer que le groupe $\mathrm{Aut}_{\mathbb{Q}}(M)$ est trivial.
2. Soit $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[5]{2})$. Montrer que le groupe $\mathrm{Aut}_{\mathbb{Q}}(L)$ est trivial, mais que l'extension $L/\mathbb{Q}$ admet des sous-extensions non triviales.

Exercice 5.

Soit K un corps, et soit L/K une extension galoisienne finie de groupe G. Soient M et M' sont deux extensions intermédiaires de L/K. On note H et H' les sous-groupes de G correspondant à M et M' respectivement, par la correspondance de Galois.

1. Montrer que le sous-groupe $H \cap H'$ de G correspond à l'extension composée MM'.
2. Montrer que le sous-groupe engendré par $H \cup H'$ correspond à l'extension $M \cap M'$.

Exercice 6.

Soit K un corps, et soit $\bar{K}$ une clôture algébrique de K. On considère une extension galoisienne finie L/K, et une extension finie quelconque F/K, contenues dans $\bar{K}$.

1. Montrer que l'extension LF/F est galoisienne.
2. Montrer que le degré $[LF : F]$ divise le degré $[L : K]$. Est-ce que cette assertion reste vraie si l'extension L/K n'est pas galoisienne ?

Exercice 7.

1. Si G est une groupe, et H un sous-groupe de G, on appelle *normalisateur de H dans G* l'ensemble
$$N_G(H) = \{\sigma \in G \,:\, \sigma H \sigma^{-1} = H\}.$$
Rappeler pourquoi $N_G(H)$ est un sous-groupe de G, et que c'est le plus grand sous-groupe de G dans lequel H soit un sous-groupe distingué.
2. Soit K un corps, et soit L/K une extension galoisienne finie de groupe G. Soit M une extension intermédiaire de L/K ; on note H le sous-groupe de G correspondant à M par la correspondance de Galois. Montrer que le normalisateur de H dans G est le sous-groupe de G formé des K-automorphismes qui laissent M *globalement* invariant.

Exercice 8.

Soit L/K une extension galoisienne de groupe G.

1. Pour tout $x \in L$, montrer l'identité : $L^{\mathrm{Stab}(x)} = K(x)$.
2. On suppose que L est corps de décomposition sur K d'un polynôme irréductible P de degré n. Notons $x_1,...,x_n$ les racines de P. Pour tout indice i, on pose $H_i = \mathrm{Stab}(x_i) \subset G$.
   (a) Montrer que les sous-groupes H_i sont conjugués dans G, et que pour tout i on a $[G : H_i] = n$. À quel sous-corps de L correspond le groupe H_i ?
   (b) Si le groupe G est abélien, montrer que $L = K(x_1)$.
3. Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible sur $\mathbb{Q}$. On suppose que P a au moins une racine réelle et une racine non réelle. Montrer que le groupe de Galois de P sur $\mathbb{Q}$ n'est pas abélien.

Exercice 9. Existence de polynômes sur $\mathbb{Q}$ de groupe de Galois $\mathfrak{S}_n$.

Soit $n \geq 2$ un entier.

1. Soit H un sous-groupe de $\mathfrak{S}_n$ contenant une transposition, un $(n-1)$-cycle et un n-cycle. Montrer l'égalité $H = \mathfrak{S}_n$.
2. Soit H un sous-groupe de $\mathfrak{S}_n$ contenant un $(n-1)$-cycle, un n-cycle et une permutation dont la décomposition en cycles à supports disjoints contient exactement un cycle de longueur 2 et tous les autres cycles ont des longueurs impaires. Montrer : $H = \mathfrak{S}_n$.
3. Soient :
   - $f_2 \in \mathbb{F}_2[X]$ un polynôme uniatire irréductible de degré n ;
   - $f_3 \in \mathbb{F}_3[X]$ un polynôme unitaire séparable, produit d'un polynôme de degré 1 et d'un polynôme irréductible de degré $n-1$;
   - $f_5 \in \mathbb{F}_5[X]$ un polynôme unitaire séparable, produit d'un polynôme irréductible de degré 2 et de polynômes irréductibles de degré impair.

   On note P_2, P_3 et P_5 des relèvements unitaires de f_2, f_3 et f_5 respectivement, en polynômes de $\mathbb{Z}[X]$. On pose
   $$P = -15P_2 + 10P_3 + 6P_5.$$
   Montrer que le groupe de Galois sur $\mathbb{Q}$ du polynôme P est isomorphe au groupe symétrique $\mathfrak{S}_n$.

   Remarque. Peut-on remplacer 2, 3 et 5 par trois nombres premiers distincts p_1, p_2 et p_3 ?