ENS Lyon 2011 - 2012
Master 1

Algèbre Approfondie

21.10.2011

TD 6

Correspondance de Galois

Si K un corps et n un entier premier à la caractéristique de K, on note μ_n^* l'ensemble des racines primitives n-èmes de l'unité dans une clôture algébrique de K. On appelle n-ème polynôme cyclotomique de K le polynôme :

$$\Phi_{n,K}(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta).$$

Exercice 1.

1. Soient m et n deux entiers ≥ 1. Notons d leur pgcd, et M leur ppcm. Montrer :

$$\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_M) \quad \text{et} \quad \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_d).$$

2. Soient n et m deux entiers tels que $1 \leq n \leq m$. Montrer que $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)$ si et seulement si on est dans l'un des deux cas suivants :
   (a) $m = n$;
   (b) ou bien n est impair et $m = 2n$.

Exercice 2. Cyclotomie sur $\mathbb{F}_p$.

Soit n un entier positif et soit p un nombre premier ne divisant pas n. Soit ζ une racine primitive n-ème de l'unité de $\mathbb{F}_p$, dans le corps de décomposition de $X^n - 1$. On note d l'ordre de p vu comme élément de $(\mathbb{Z}/n\mathbb{Z})^*$.

1. Montrer que le polynôme minimal de ζ sur $\mathbb{F}_p$ est de degré d.
2. En déduire que le polynôme cyclotomique $\Phi_{n,\mathbb{F}_p}$ est irréductible si et seulement si $d = \varphi(n)$. Si $d < \varphi(n)$, montrer que $\Phi_{n,\mathbb{F}_p}$ est un produit de polynômes de degré d.
3. Décrire les groupes $(\mathbb{Z}/8\mathbb{Z})^*$ et $(\mathbb{Z}/12\mathbb{Z})^*$. En déduire que les polynômes $\Phi_{8,\mathbb{F}_p} = X^4 + 1$ et $\Phi_{12,\mathbb{F}_p} = X^4 - X^2 + 1$ ne sont pas irréductibles.
4. Montrer que l'extension $\mathbb{F}_p(\zeta_n)/\mathbb{F}_p$ est galoisienne de groupe de Galois isomorphe au sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$ engendré par la classe de p. Montrer aussi l'identité $\mathbb{F}_p(\zeta_n) = \mathbb{F}_{p^d}$.

Exercice 3.

1. Montrer que tout groupe cyclique est isomorphe au groupe de Galois d'une extension galoisienne de $\mathbb{Q}$.
2. Montrer que tout groupe abélien fini est isomorphe au groupe de Galois d'une extension galoisienne de $\mathbb{Q}$. *Indication : on pourra utiliser la propriété que pour tout nombre entier $n \geq 1$ il existe une infinité de nombres premiers p tels que $p \equiv 1$ (mod n).*

Exercice 4.

Soit $L \subset \mathbb{C}$ une extension normale d'un corps K. Soit a un élément de L ; on note $P(X) = \sum_{0 \leq k \leq n} a_k X^k$ le polynôme minimal de a sur K, et L' la clôture normale de $K[a]$ dans L. On note $m : L \to L$ l'application définie par $m(x) = ax$, et on pose $m' = m'_{|L'}$.

1. Vérifier que l'application m est K-linéaire.
2. (a) Exprimer la norme de a, $N_{L'/K}(a)$, en fonction des coefficients de P.

(b) Montrer $N_{L'/K}(a) = \det(m')$, puis $N_{L/K}(a) = \det(m)$.

Exercice 5.

Soit L/K une extension finie galoisienne, de groupe de Galois G. On suppose que G agit fidèlement et transitivement sur l'ensemble $\{1, ..., n\}$ pour un certain entier $n \geq 1$.

1. Montrer qu'il existe une extension intermédiaire F/K de degré n telle que L soit la clôture normale de F. *On pourra considérer le stabilisateur H de 1 dans G.*
2. Montrer qu'il existe un polynôme $P \in K[X]$ de degré n, irréductible et séparable, tel que le groupe de Galois de P sur K, noté $\mathrm{Gal}_K(P)$, soit isomorphe à G.
3. Soit $\mathcal{R}$ l'ensemble des racines de P dans L. Montrer qu'il existe une unique bijection de $\mathcal{R}$ dans $\{1, ..., n\}$ telle que l'action de $\mathrm{Gal}_K(P)$ sur $\mathcal{R}$ corresponde, via l'isomorphisme précédent, à l'action donnée de G sur $\{1, ..., n\}$.

Exercice 6.

On pose $\zeta = e^{2i\pi}/15$, $\eta = e^{2i\pi/5}$ et $j = e^{2i\pi/3}$. On rappelle que $\cos(2\pi/5) = \frac{-1+\sqrt{5}}{4}$.

1. Calculer le degré de l'extension $\mathbb{Q}(\zeta)$ sur $\mathbb{Q}$, et déterminer le polynôme minimal $\Phi_1 5$ de ζ sur $\mathbb{Q}$.
2. On pose $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Lorsqu'il existe, on note σ_k l'élément de G tel que $\sigma_k(\zeta) = \zeta^k$: quelles sont les valeurs de k possible ?
3. Montrer que G est isomorphe à un produit de deux groupes cycliques.
4. Montrer que $\mathbb{Q}(\zeta)$ est une extension de degré 2 de $\mathbb{Q}(\cos(2\pi/15))$.
5. Montrer que $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\eta)$, puis que les corps $\mathbb{Q}(j)$, $\mathbb{Q}(\eta)$, $\mathbb{Q}(\sqrt{5})$ et $\mathbb{Q}(j, \sqrt{5})$ sont des sous-extensions de $\mathbb{Q}(\zeta)/\mathbb{Q}$.
   Pour chacun des quatre corps K ci-dessus, déterminer le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta)/K)$. On donnera les éléments σ_k de ces groupes.
6. (a) Déterminer le corps des invariants du sous-groupe $< \sigma_{14} >$ de G.
   (b) Résoudre la même question pour le sous-groupe $< \sigma_2 >$. On montrera d'abord qu'il s'agit d'un sous-corps de $\mathbb{Q}(j, \sqrt{5})$.
7. Expliciter la correspondance de Galois pour l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$.
8. En considérant le groupe $\mathrm{Gal}(\mathbb{Q}(\cos(2\pi/15))/\mathbb{Q}(\sqrt{5})$, trouver un polynôme de degré 2, à coefficients dans $\mathbb{Q}(\sqrt{5})$, dont une racine est dans $\mathbb{Q}(\cos(2\pi/15))$. En déduire une expression par radicaux de $\cos(2\pi/15)$.