M2R Université de Paris-Sud
2006-2007 21 novembre 2006

Partiel d'une durée de 2h30.

Les notes de cours et de TD sont autorisées à l'exclusion de tout autre document. Les calculatrices sont interdites. Écrivez lisiblement (en français ou en anglais).

Soit $f \in \mathbb{Z}[X]$ unitaire de degré $d \geq 1$. On note $\mathcal{R}$ l'ensemble des racines de f dans $\mathbb{C}$ et $\mathbb{E} = \mathbb{Q}(\mathcal{R})$ le corps de décomposition de f dans $\mathbb{C}$. On identifie $G = \mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ à un sous-groupe du groupe symétrique $S(\mathcal{R})$. On rappelle que le sous-corps fixé par $G \cap A(\mathcal{R})$ (où $A(\mathcal{R})$ est le groupe des permutations paires de $\mathcal{R}$) est $\mathbb{Q}(\sqrt{d})$ où d est le discriminant de f. On choisit α dans $\mathcal{R}$ et on pose $K = \mathbb{Q}(\alpha)$.

Partie 1 On suppose f irréductible sur $\mathbb{Q}$.

1. Montrer qu'un nombre premier p non ramifié dans $K/\mathbb{Q}$ l'est aussi dans $\mathbb{E}/\mathbb{Q}$.
2. Soit p un nombre premier tel que $f \mod p$ est le produit de r polynômes unitaires irréductibles disctincts de $\mathbb{Z}/p\mathbb{Z}[X]$. Si $d_1, \ldots, d_r$ sont les degrés de ces polynômes, prouver que G contient un produit de r cycles disjoints de longueur $d_1, \ldots, d_r$ (on pourra considérer un idéal maximal $\mathfrak{p}$ de $\mathbb{E}$ au-dessus de p, et l'action de $\mathrm{Frob}(\mathfrak{p}/p)$ sur $f \mod \mathfrak{p}$).

Partie 2 On considère maintenant le cas particulier où $f = X^4 + 4X + 2$, de discriminant $-2^8 \times 19$.

1. Justifier l'irréductibilité de f, par exemple en factorisant $2\mathcal{O}_K$.
2. Prouver que G agit transitivement sur $\mathcal{R}$ et que 4 divise $|G|$.
3. Calculer le nombre de racines réelles de f. En utilisant la conjugaison complexe $z \mapsto \overline{z}$, prouver que G contient une transposition.
4. Factoriser $f \mod 7$ dans $\mathbb{Z}/7\mathbb{Z}[X]$. En déduire que G contient un cycle d'ordre 3.
5. Prouver que G est $S(\mathcal{R})$ tout entier.
6. Décrire toutes les possibilités de décomposition dans $K/\mathbb{Q}$ d'un nombre premier $p = \prod_{\mathfrak{p}/p} \mathfrak{p}^{e(\mathfrak{p}/p)}$, c'est à dire les possibilités pour le nombre d'idéaux $\mathfrak{p}/p$, et pour les indices $e(\mathfrak{p}/p)$ et $f(\mathfrak{p}/p)$. Pour chaque cas, donner la densité correspondante (On décrira précisément le principe du calcul et on donnera les résultats, les détails ne sont pas demandés).
7. Quels sont les nombres premiers ramifiés dans $K/\mathbb{Q}$? Donner leur décomposition (on pourra remarquer que $f \mod 19$ a pour racines $3 \mod 19$, $-7 \mod 19$ et $-8 \mod 19$).
8. Prouver que $\mathbb{Z}[\alpha]$ est d'indice 2^β dans $\mathcal{O}_K$ avec $\beta \leq 4$. Montrer que l'inclusion de $\mathbb{Z}[\alpha]$ dans $\mathcal{O}_K$ induit un isomorphisme de $\mathbb{Z}[\alpha]/\alpha\mathbb{Z}[\alpha]$ sur $\mathcal{O}_K/\alpha\mathcal{O}_K$, et un isomorphisme de $\mathbb{Z}[\alpha]/2\mathbb{Z}[\alpha]$ sur $\mathcal{O}_K/2\mathcal{O}_K$. Conclure que $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
9. Soit Q_{19} un idéal maximal de $\mathcal{O}_\mathbb{E}$ au-dessus de 19, et D le sous-groupe de décomposition de $Q_{19}/19$. Notant H le sous-groupe $\mathrm{Gal}(\mathbb{E}/K)$ de G, déduire de la question 7. que D a 3 orbites dans son action sur G/H, dont on donnera la longueur. En déduire que D est engendré par une transposition (on pourra remarquer que G/H s'identifie à $\mathcal{R}$, comme ensemble muni d'une action de G).
10. Montrer que $\mathbb{E}$ contient une unique sous-extension quadratique F sur $\mathbb{Q}$ et que $2\mathcal{O}_F$ est premier.
11. La résolvante cubique g de f est $g = X^3 - 8X - 16$; si $\alpha = \alpha_1, \alpha_2, \alpha_2, \alpha_4$ sont les racines de f dans $\mathbb{E}$, celles de g sont $\beta_2 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $\beta_3 = \alpha_1\alpha_3 + \alpha_2\alpha_4$, $\beta_4 = \alpha_1\alpha_4 + \alpha_2\alpha_3$. Identifier dans $S(\mathcal{R})$ le sous-groupe $\mathrm{Gal}(\mathbb{E}/\mathbb{L})$ où $\mathbb{L}$ est le sous-corps $\mathbb{Q}(\beta_2, \beta_3, \beta_4)$.
12. Considérant $g(2Y)$, montrer que 2 est totalement ramifié dans $\mathbb{Q}(\beta_2)/\mathbb{Q}$. En déduire les groupes de décomposition et d'inertie du nombre premier 2 dans $\mathbb{E}/\mathbb{Q}$ et $\mathbb{L}/\mathbb{Q}$.