M2R Université de Paris-Sud
2006-2007 Séance 12 du 15 janvier 2007

Feuille 10 : Corps de classes

Exercice : On considère le corps de nombres $F = \mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$. On sait que $\mathcal{O}_F = \mathbb{Z}[i]$ est un anneau principal et que ses unités sont $1, -1, i, -i$. On pose $\pi = i - 1$. L'extension $F/\mathbb{Q}$ est non ramifiée hors de 2 et on a $2\mathcal{O}_F = (\pi)^2$. On note F_π le complété de F pour la valuation associée à l'idéal π.

3.1 On considère les extensions abéliennes finies de F (dans $\mathbb{C}$) dont le groupe de Galois est annulé par 2 et qui sont non ramifiées hors de $\pi\mathcal{O}_F$.
Prouver qu'il existe une telle extension E/F qui contient toutes les autres, qu'elle est de degré 4 sur F et galoisienne sur $\mathbb{Q}$.
Décrire $F^* N_{E/F}(\mathbb{A}_E^*)$ sous la forme $F^* \Pi_v H_v$ où H_v est un sous-groupe ouvert de F_v^*, avec $H_v = U_v$ pour presque tout v.
Exprimer également E sous la forme $F(\sqrt{a}, \sqrt{b})$ avec $a, b \in F^*$ bien choisis.

3.2 Montrer que E est le corps de décomposition sur $\mathbb{Q}$ du polynôme $X^8 + 4$. Décrire l'action sur E de la conjugaison complexe c.
Montrer que E est cyclique sur $K = \mathbb{Q}(\sqrt{-2})$.

On notera σ un générateur de $\mathrm{Gal}(E/K)$ et encore c l'image dans $\mathrm{Gal}(E/\mathbb{Q})$ de la conjugaison complexe. On a $c\sigma c^{-1} = \sigma^3 = \sigma^{-1}$.

3.3 Montrer que $L = KF$ est la sous-extension abelienne maximale de E sur $\mathbb{Q}$.
Décrire $\mathbb{Q}^* N_{E/\mathbb{Q}}(\mathbb{A}_E^*)$.

3.4 Selon la classe de p modulo 8, discuter la ramification (i.e le nombre d'idéaux de $\mathcal{O}_L$ au-dessus de p, avec le degré d'inertie correspondant) d'un nombre premier impair p, dans l'extension $L/\mathbb{Q}$.
Lorsque $p \not\equiv 1 \mod 8$, discuter la ramification de p premier impair dans l'extension $E/\mathbb{Q}$.

3.5 Montrer que $N_\pi = F_\pi^* \cap F^* N_{E/F}(\mathbb{A}_E^*)$ est engendré par F_π^{*2} et l'image dans F_π des éléments de F^* qui sont des unités hors de π.
Déterminer l'image dans F_π^*/N_π du groupe des unités de F_π.
En déduire que $E/\mathbb{Q}$ est totalement ramifiée en 2.
Notant v la place de L au-dessus de 2 et w la place de E au-dessus de v, prouver que $N_{E_w/\mathbb{Q}_2}(E_w^*)$ est égal à $N_{L_v/\mathbb{Q}_2}(L_v^*)$.
Montrer que $N_{L_v/\mathbb{Q}_2}(L_v^*)$ est engendré par 2 et $1 + 8\mathbb{Z}_2$.

3.6 On suppose maintenant que p est un nombre premier congru à 1 modulo 8, et on écrit $p = X^2 + Y^2$, avec X et Y entiers. Prouver qu'on peut prendre X congru à 1 modulo 4 et Y divisible par 4.
Montrer que p est totalement décomposé dans $E/\mathbb{Q}$ si et seulement si l'idéal maximal de $\mathbb{Z}(i)$ engendré par $a = X + iY$ est totalement décomposé dans E/F, ce qui équivaut encore au fait que a, vu comme uniformisante du complété F_a de F en cet idéal, est dans le groupe $F^* N_{E/F}(\mathbb{A}_E^*)$.
Prouver que cela arrive précisément quand il existe un élément y de F qui est une unité hors de π, tel que ay soit un carré dans F_π.
Prouver que enfin que cette dernière condition équivaut à $X + Y$ congru à 1 modulo 8. (Indication : remarquer que toute unité de F_π s'écrit sous la forme $i^r(1+2\pi\alpha)$, $r \in \mathbb{Z}, \alpha \in \mathcal{O}_{F_\pi}$).