Feuille d'exercices 8

Exercice 1 Soit K un tel corps de nombre et $P = ax^2 + bx + c \in \mathbb{Q}[X]$ un polynôme dont K est le corps de décomposition. Soit D le discriminant de P, puisque K est de degré 2 alors $\sqrt{D} \notin \mathbb{Q}$ et clairement $K = \mathbb{Q}(\sqrt{D})$. Quitte à multiplier P par un facteur on peut supposer que a, b, c et donc D sont entiers. SI maintenant $D = n^2 m$ avec m, n entier, alors clairement $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{m})$ donc on peut supposer D sans facteur carré. Si maintenant D_1, D_2 sont deux entiers sans facteurs carrés tels que $\mathbb{Q}(\sqrt{D_1}) = \mathbb{Q}(\sqrt{D_2})$ alors il existe $x, y \in \mathbb{Q}$ tels que $D_2 = (x + y\sqrt{D_1})^2$. En développant et en utilisant le fait que D_1, D_2 sont sans facteurs carrés on en déduit $D_1 = D_2$.

Exercice 2 Soit p premier impair, ζ_p une racine primitive p-ième de l'unité et $\tau = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a$. On rappelle (cours) que $\tau^2 = \left(\frac{-1}{p}\right) p$.

1. Calcul direct.
2. La formule ci-dessous montre que pour tout premier impair, $\mathbb{Q}(\zeta_p)$ contient $\mathbb{Q}\left(\sqrt{\left(\frac{-1}{p}\right) p}\right)$ et la question précédente implique que $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$. Par ailleurs $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ est déjà une extension cyclotomique. DOnc si $K = \mathbb{Q}(\sqrt{m})$ avec m sans facteur carré (donc tous ses facteurs premiers p_i apparaissant avec multiplicité 1), alors il suffit de choisir N tel que
   — chacun des p_i impair divise N de tel sorte que le groupe des racines N-ième de l'unité contiennent une racine primitive p_i-ième
   — si $2|m$ alors on demande que $8|N$ de tel sorte que ce groupe contient une racine primitive 8-ième de 1
   — suivant le signe de m et des $\left(\frac{-1}{p_i}\right)$ il suffit ensuite d'inclure éventuellement i, càd demander que $2|N$.

Exercice 3 1. Clair.

2. Soit I l'idéal (α). Soient $x = a + b\alpha$ et $y = c + d\alpha$. Si $xy \in I$, d'après la question précédente alors $ac - pbd = 0 \mod p$, donc $ac = 0 \mod p$, donc $a = 0 \mod p$ ou $c = 0 \mod p$ puisque $\mathbb{F}_p$ est intègre. Donc $x \in I$ ou $y \in I$, donc α est premier.

Exercice 4 On vérifie facilement que c'est vrai pour $k = -1, -2$. Montrons que c'est faux pour les autres. On peut supposer $k = -p$ avec p premier impair. En effet si $k = -ab$ avec a, b entiers différents de ± 1, alors dans l'anneau on a $k = -ab = (\sqrt{k})^2$ et donc deux factorisations distinctes. Or, si p est impair, $p + 1$ est pair, et donc

$$(1 - \sqrt{-p})(1 + \sqrt{-p}) = 1 + p = 2n$$

pour un certain n entier.