Feuille 6

Exercice 1 (Borne de Minkowski et ramification) Soient K une extension de degré n de $\mathbb{Q}$, d_K le discriminant de $K/\mathbb{Q}$, $2s$ le nombre de plongements complexes non réels de K. On rappelle le résultat suivant appelé *borne de Minkowski* : il existe un ensemble de représentants du groupe des classes de K composé d'idéaux entiers $\mathfrak{a}$ de K tels que

$$\mathrm{N}(\mathfrak{a}) \leq \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^s |d_K|^{1/2}$$

1. Trouver le nombre de classes des corps suivants : $K = \mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{-5}]$.
2. Soient $x = (11)^{1/3}$ et $K = \mathbb{Q}(x)$. Notons $\mathcal{O}_K$ l'anneau des entiers de K, U_K son groupe d'unités et C_K son groupe des classes d'idéaux.
   Montrer[1] que $\mathcal{O}_K = \mathbb{Z}[x]$. Montrer que C_K est engendré par au plus deux éléments (on pourra étudier la décomposition en premiers de $2\mathcal{O}_K, \ldots, 13\mathcal{O}_K$). En considérant l'idéal $\mathfrak{p}_2 = (2, x-1)$, montrer que $x^2 - 5$ est dans $\mathfrak{p}_2^2$ et de norme 4. En déduire que $|C_K| \leq 2$.
3. Montrer[2] qu'il n'existe pas d'extension non ramifiée de $\mathbb{Q}$.

Exercice 2 (Nombre de classes de $\mathbb{Q}[\zeta_{23}]$)

1. Décrire le groupe de Galois $\mathrm{Gal}(\mathbb{Q}[\zeta_{23}]/\mathbb{Q})$. En déduire l'unique extension quadratique K de $\mathbb{Q}$ contenue dans K.
2. On admet que le nombre de classes de K vaut 3. En déduire que le nombre de classes de $\mathbb{Q}[\zeta_{23}]$ est strictement supérieur à 1 (on pourra étudier l'idéal $2\mathcal{O}_K$).

---

[1] On rappelle le résultat suivant :

Théorème 0.1 Si A est un anneau de valuation discrète (DVR), d'idéal maximal $\mathfrak{p}$, de corps résiduel k ; si $f \in A[X]$ est de degré $n \geq 1$ et est d'Eisenstein pour $\mathfrak{p}$, alors, l'anneau $B := A[X]/(f)$ est DVR, d'idéal maximal engendré par x (image de X dans B), de corps résiduel k.

[2] Ceci n'est en général plus vrai pour des corps autres que $\mathbb{Q}$: c'est la notion de corps de classes de Hilbert.