Feuille 3 :

Dans toute cette feuille, si l'on ne précise rien, p est un nombre premier.

Exercice 1 Soit $K = \mathbb{Q}(S)$ le corps engendré par $S = \{\sqrt{p} \mid p \text{ premier }\}$.

1. Montrer que $K/\mathbb{Q}$ est galoisien. Déterminer son groupe de Galois et l'écrire comme une limite projective.
2. Soit V un $\mathbb{F}_2$-espace-vectoriel de dimension infinie. Montrer que : pour tout entier $n \geq 0$, il existe un sous-espace vectoriel $V_n \subset V$ de codimension n.
3. Déduire de ce qui précède qu'il existe dans $\mathrm{Gal}(K/\mathbb{Q})$ des sous-groupes non-ouverts d'indice 2^n pour tout entier $n \geq 0$.
4. En déduire l'existence dans $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ de sous-groupes distingués non-ouverts d'indice 2^n pour tout entier $n \geq 0$.

Exercice 2 (Extensions cyclotomiques I) Soient $K/\mathbb{Q}$ un corps de nombres et $\mathcal{O}_K$ la clôture intégrale de $\mathbb{Z}$ dans K, *i.e.* l'anneau des entiers de $\mathcal{O}_K$. C'est un anneau de Dedekind. Soient L une extension finie séparable de degré n d'un corps de nombres K et B la clôture intégrale de $\mathcal{O}_K$ dans L. Soient $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ et $\mathfrak{p}B = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_g^{e_g}$ sa décomposition en idéaux premiers dans B. Soit $f_i = [B/\mathcal{P}_i : \mathcal{O}_K/\mathfrak{p}]$, $1 \leq i \leq g$ le degré d'inertie. On rappelle que

$$\sum_{i=1}^{g} e_i f_i = n.$$

On note $r \geq 1$, p premier, ζ une racine primitive p^r-ième de l'unité, $K = \mathbb{Q}[\zeta]$ et $\mathcal{O}_K$ son anneau d'entiers.

1. Montrer que K est une extension normale et que l'on a un morphisme injectif du groupe de Galois G_K vers le groupe $(\mathbb{Z}/p^r\mathbb{Z})^\times$ des inversibles de $\mathbb{Z}/p^r\mathbb{Z}$. Montrer également que $\mathbb{Z}[\zeta] \subset \mathcal{O}_K$ et que $[\mathbb{Q}[\zeta] : \mathbb{Q}] \leq \varphi(p^r) = p^{r-1}(p-1)$.
2. On appelle *polynôme cyclotomique* Φ_{p^r} le polynôme $\prod_{\zeta \in \mu_{p^r} \text{ primitive}} (X - \zeta)$. Montrer que
$$\Phi_{p^r} = \prod_{[i] \in (\mathbb{Z}/p^r\mathbb{Z})^\times} (X - \zeta^i) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1}.$$
3. Soit ξ une autre racine primitive p^r-ième de l'unité. Montrer que $\frac{1-\zeta}{1-\xi}$ est une unité de $\mathcal{O}_K$ (*i.e.* est inversible dans $\mathcal{O}_K$).
4. Soit $\pi = 1 - \zeta$. En calculant $\Phi_{p^r}(1)$, montrer l'égalité d'idéaux dans $\mathcal{O}_K$, $(p) = (\pi)^{\varphi(p^r)}$. En déduire que le corps $\mathbb{Q}[\zeta]$ est de degré $\varphi(p^r)$ sur $\mathbb{Q}$ et que l'élément π est premier dans $\mathcal{O}_K$. Quels sont les premiers ramifiés dans $K/\mathbb{Q}$? Donner le degré résiduel f et l'indice de ramification e.

Exercice 3 (Extension $\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}$) Dans la suite on utilisera librement que si $n \in \mathbb{N}$, et si ζ_n est une racine primitive n-ieme de 1, alors $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. On rappelle également le *théorème de Kronecker-Weber* : "si $K/\mathbb{Q}$ est une extension finie abélienne, alors il existe $n \geq 1$ tel que $K \subset \mathbb{Q}(\zeta_n)$." On note $\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}$ l'extension abélienne maximale de $\mathbb{Q}$.

Montrer que cette extension est galoisienne et décrire explicitement son groupe de Galois.

Exercice 4 Soit G un groupe topologique compact et $\{N_i \mid i \in I\}$ une famille de sous-groupes distingués, fermés d'indice fini dans G telle que

$$\bigcap_{i \in I} N_i = \{1\}.$$

On a alors G est un groupe profini, homéomorphe à la limite projective des G/N_i.

Exercice 5

1. Montrer que si H est un sous-groupe fermé de $\mathbb{Z}_p$ alors il existe $i \in \mathbb{N}$ tel que $p^i\mathbb{Z}_p = H$.
2. Montrer que $p\mathbb{Z}_p$ est l'unique sous groupe fermé maximal de $\mathbb{Z}_p$.
3. Montrer que si $\alpha : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ est un morphisme surjectif, et si H est un sous-groupe fermé tel que $\alpha(H) = \alpha(\mathbb{Z}_p)$, alors $H = \mathbb{Z}_p$.

Exercice 6 Prouver que $\widehat{\mathbb{Z}}$ est homéomorphe à $\prod_{p \text{ premier}} \mathbb{Z}_p$. Soit S un sous-ensemble non-vide de l'ensemble des nombres premiers. Donner un énoncé analogue avec la limite projective $\mathbb{Z}_S$ des $\mathbb{Z}/n\mathbb{Z}$ quand n décrit l'ensemble

$$\{n \in \mathbb{N} \mid \text{ les diviseurs premiers de } p \text{ sont dans } S\}.$$

Exercice 7 (Extensions quadratiques)
Soit K une extension quadratique de $\mathbb{Q}$. On note $\mathcal{O}$ la clôture intégrale de $\mathbb{Z}$ dans K :

$$\mathcal{O} = \{x \in K, x \text{ solution d'un polynôme unitaire à coefficients dans } \mathbb{Z}\}.$$

1. Montrer que K est de la forme $\mathbb{Q}(\sqrt{\Delta})$ avec $\Delta \in \mathbb{Z} - \{0, 1\}$ sans facteur carré.
2. Pour $z = x + y\sqrt{\Delta} \in \mathbb{Q}(\sqrt{\Delta})$, $\bar{z} = x - y\sqrt{\Delta}$. Montrer que

$$z \in \mathcal{O} \text{ si et seulement si } \begin{cases} N_{K/\mathbb{Q}}(z) = N(z) := z\bar{z} \in \mathbb{Z} \\ \mathrm{T}_{K/\mathbb{Q}}(z) = T(z) := z + \bar{z} \in \mathbb{Z} \end{cases}$$

3. En déduire $\mathcal{O}$.