Examen partiel de Théorie des nombres

Vendredi 12 novembre 2021. Durée : 3 heures.

Documents autorisés, appareils électroniques interdits.

La qualité de l'argumentation et la précision des arguments seront pris en compte dans l'évaluation.

Exercice 1 Soit p un nombre premier. On fixe $\overline{\mathbf{Q}_p}$ une clôture algébrique de $\mathbf{Q}_p$. On note $(\mathbf{Q}_p^\times)^2$ l'ensemble des éléments de la forme x^2 avec $x \in \mathbf{Q}_p^\times$.

1) Soit $K \subset \overline{\mathbf{Q}_p}$ une extension de degré 2 de $\mathbf{Q}_p$. Montrer qu'il existe $d \in \mathbf{Q}_p^\times \smallsetminus (\mathbf{Q}_p^\times)^2$ tel que $K = \mathbf{Q}_p(\sqrt{d})$.
2) Montrer que, pour d_1 et d_2 dans $\mathbf{Q}_p^\times$, on a $\mathbf{Q}_p(\sqrt{d_1}) = \mathbf{Q}_p(\sqrt{d_2})$ si et seulement si il existe $u \in \mathbf{Q}_p^\times$ tel que $d_2 = u^2 d_1$.

On suppose désormais que p est impair.

3) Montrer que l'application $x \mapsto x^2$ de $1 + p\mathbf{Z}_p$ dans lui-même est bijective.
4) En déduire la liste des sous-extensions $K \subset \overline{\mathbf{Q}_p}$ de $\mathbf{Q}_p$ telles que $[K : \mathbf{Q}_p] = 2$. En donner des générateurs et indiquer lesquelles sont ramifiées sur $\mathbf{Q}_p$.

Exercice 2 Soit $L = \mathbf{Q}(\zeta_{31})$.

1) Montrer que L contient un unique sous-corps K de dimension 3 sur $\mathbf{Q}$.
2) Déterminer le nombre de places réelles et complexes de K.

On rappelle que l'anneau des entiers $\mathcal{O}_L$ de L est l'anneau $\mathbf{Z}[\zeta_{31}]$.

3) Déterminer la décomposition de l'idéal $2\mathcal{O}_L$ en produit d'idéaux maximaux dans $\mathcal{O}_L$.
4) Soit $\mathcal{O}_K$ l'anneau des entiers de K et soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_K$ divisant $2\mathcal{O}_K$. Déterminer le corps résiduel $\mathcal{O}_K/\mathfrak{p}$.
5) En déduire que l'anneau $\mathcal{O}_K$ n'est pas de la forme $\mathbf{Z}[\alpha]$ pour un élément $\alpha \in \mathcal{O}_K$.
6) Donner (et justifier) un exemple de nombre premier p tel que $p\mathcal{O}_K$ est un idéal premier de $\mathcal{O}_K$.

Exercice 3 Soit F une extension quadratique réelle de $\mathbf{Q}$. Soit p un nombre premier impair.

1) Montrer que le sous-groupe $(1 + p\mathcal{O}_F) \cap \mathcal{O}_F^\times$ est sans torsion.
2) Soit $n \geqslant 1$. Montrer que le quotient de $(1 + p\mathcal{O}_F) \cap \mathcal{O}_F^\times$ par $(1 + p^n\mathcal{O}_F) \cap \mathcal{O}_F^\times$ est un p-groupe fini.

3) En déduire que pour tout entier $r \geqslant 1$, il existe un entier $n \geqslant 1$ tel que $a \in (1 + p^n\mathcal{O}_F) \cap \mathcal{O}_F^\times$ implique l'existence de $\alpha \in \mathcal{O}_F^\times$ tel que $\alpha^{p^r} = a$.
4) Montrer que pour tout entier $r \geqslant 1$, il existe un entier $n \geqslant 1$ tel que $a \in (1 + 2^n\mathcal{O}_F) \cap \mathcal{O}_F^\times$ implique l'existence de $\alpha \in \mathcal{O}_F^\times$ tel que $\alpha^{2^r} = a$.
5) Soit m un entier impair. Montrer qu'il existe $n \geqslant 1$ tel que tout élément de $(1 + n\mathcal{O}_F) \cap \mathcal{O}_F^\times$ soit une puissance m-ième d'un élément de $\mathcal{O}_F^\times$.

Exercice 4 Soit F un corps de nombres. On note I_F le groupe des idèles de F et I_f le groupe des idèles finis de F, c'est-à-dire le produit restreint des $F_v^\times$, pour $v \nmid \infty$, relativement aux sous-groupes $\mathcal{O}_{F_v}^\times$. On plonge $F^\times$ diagonalement dans I_f.

1) Si F est une extension quadratique imaginaire de $\mathbf{Q}$, montrer que $F^\times$ est fermé dans I_f.
2) Si F est une extension quadratique réelle de $\mathbf{Q}$, montrer que $F^\times$ muni de la topologie induite par I_f n'est pas discret.
3) En déduire que $F^\times$ n'est pas fermé dans I_f (on pourra utiliser le fait que la topologie de I_f est métrisable).