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 $\mathbf{Q}_p$.

Corrigé :

1) Soit $z \in K \smallsetminus \mathbf{Q}_p$. Alors $K = \mathbf{Q}_p(z)$ et il existe deux nombre p-adiques a et b tels que $z^2 = az + b$. Remarquons alors que $(z - \frac{a}{2})^2 \in \mathbf{Q}_p$. Posons $d = (z - \frac{a}{2})^2$. On a nécessairement $d \neq 0$ puisque $z \notin \mathbf{Q}_p$ et $K = \mathbf{Q}_p(\sqrt{d})$.
2) Si $d_2 = u^2 d_1$, on a $\sqrt{d_2} = \pm u\sqrt{d_1}$ de sorte que $\mathbf{Q}_p(\sqrt{d_1}) = \mathbf{Q}_p(\sqrt{d_2})$. Réciproquement supposons $\mathbf{Q}_p(\sqrt{d_1}) = \mathbf{Q}_p(\sqrt{d_2})$. Si $\sqrt{d_1} \in \mathbf{Q}_p$, alors $\sqrt{d_2} \in \mathbf{Q}_p$ et le résultat est évident. Supposons donc $\sqrt{d_1} \notin \mathbf{Q}_p$. Il existe $a, b \in \mathbf{Q}$ tels que $\sqrt{d_2} = a\sqrt{d_1} + b$ et $d_2 = a^2 d_1 + 2ab\sqrt{d_1} + b^2$. Puisque $d_2 - a^2 d_1 - b^2 \in \mathbf{Q}_p$, on a $ab = 0$. Par ailleurs, puisque $\sqrt{d_2} \notin \mathbf{Q}_p$, on a $a \neq 0$ de sorte que $b = 0$. On peut alors choisir $u = a$ et $d_2 = u^2 d_1$.
3) Soit $a \in 1 + p\mathbf{Z}_p$. La réduction modulo p du polynôme $X^2 - a$ est le polynôme $X^2 - 1$ qui est scindé à racines simples. D'après le lemme de Hensel, il existe donc un unique élément $\alpha \in 1 + p\mathbf{Z}_p$ tel que $\alpha^2 = a$.
4) Les extensions de degré 2 de $\mathbf{Q}_p$ dans $\overline{\mathbf{Q}_p}$ sont en bijection avec les éléments non triviaux de $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2$. Or on sait que $\mathbf{Q}_p^\times \simeq p^{\mathbf{Z}} \times \mathbf{Z}_p^\times$. En utilisant le relèvement de Teichmüller, on a

$$\mathbf{Q}_p^\times \simeq p^{\mathbf{Z}} \times (\mathbb{F}_p)^\times \times (1 + p\mathbf{Z}_p).$$

Ainsi

$$(\mathbf{Q}_p^\times)^2 \simeq p^{2\mathbf{Z}} \times (\mathbb{F}_p^\times)^2 \times (1 + p\mathbf{Z}_p).$$

Comme $\mathbb{F}_p^\times$ est un groupe cyclique de cardinal $p-1$, on en conclut que $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ est un groupe de cardinal 2 et $\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^2 \simeq p^{\mathbf{Z}}/p^{2\mathbf{Z}} \times (\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2)$. Il y a donc exactement 3 extensions quadratiques de $\mathbf{Q}_p$. Il s'agit de $\mathbf{Q}_p(\sqrt{p})$, $\mathbf{Q}_p(\sqrt{[a]})$ et $\mathbf{Q}_p(\sqrt{p[a]})$ où a est un élément de $\mathbb{F}_p^\times$ qui n'est pas un carré.
Soit K l'une des extensions précédentes et soit $x \in \{p, [a]p, [a]\}$ tel que $K = \mathbf{Q}_p(\sqrt{x})$. Alors $\mathbf{Z}_p[\sqrt{x}] \subset \mathcal{O}_K$. De plus, le discriminant de la famille $(1, \sqrt{x})$ est égal $(4x)$. Si Δ désigne le discriminant de $\mathcal{O}_K$ sur $\mathbf{Z}_p$, on a $(4x) = (u^2)\Delta$ pour un élément $u \in \mathbf{Z}_p$. On en conclut que $\Delta = (4x) = (x)$ puisque $2 \in \mathbf{Z}_p^\times$.
Ainsi la seule extension non ramifiée est $\mathbf{Q}_p(\sqrt{[a]})$.

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 $\mathcal{O}_K$.

Corrigé :

1) Le groupe de Galois de $L/\mathbf{Q}$ est isomorphe à $(\mathbf{Z}/31\mathbf{Z})^\times$. Comme 31 est premier, ce groupe est cyclique de cardinal 30. Il possède donc un unique sous-groupe d'indice 3, ce qui prouve qu'il existe une unique sous extension de degré 3 dans L.
2) Soit r_1 le nombre de places réelles de K et r_2 le nombre de places complexes. On a $r_1 + 2r_2 = 3$ de sorte que $(r_1, r_2) = (3, 0)$ ou $(r_1, r_2) = (1, 1)$. Soit σ un plongement de K dans $\mathbb{C}$. Comme K est une extension galoisienne de $\mathbf{Q}$, la conjugaison complexe induit un automorphisme de K d'ordre un diviseur 2. Comme $[K : \mathbf{Q}] = 3$, le corps K ne possède pas d'automorphisme d'ordre pair, on en conclut que K est fixé par la conjugaison complexe et donc que $K \subset \mathbb{R}$. Tous les plongements de K dans $\mathbb{C}$ sont réels, on a donc $r_1 = 3$ et $r_2 = 0$.
3) Soit f le degré résiduel d'une place de L au-dessus de 2 et soit g le nombre de places de L au-dessus de 2. Comme $2 \nmid 31$, 2 est non ramifié dans L.

On en conclut que $eg = [L : \mathbf{Q}] = 30$. Par ailleurs soit $(2, L/\mathbf{Q})$ l'élément de Frobenius associé à 2. L'entier f s'identifie à l'ordre de $(2, L/\mathbf{Q})$ dans $\mathrm{Gal}(L/\mathbf{Q})$. Comme $(2, L/\mathbf{Q})$ s'envoie sur la classe de 2 via l'isomorphisme $\mathrm{Gal}(L/\mathbf{Q}) \simeq (\mathbf{Z}/31\mathbf{Z})^\times$, on en conclut que f est l'ordre de 2 dans $(\mathbf{Z}/31)^\times$. Comme $2^5 = 32$ et $2^i < 31$ pour $i < 5$, on a $f = 5$ et $g = 6$.

4) On sait que $(2, K/\mathbf{Q})$ est l'image de $(2, L/\mathbf{Q})$. Par ailleurs le noyau de $\mathrm{Gal}(L/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q})$ s'identifie au sous-groupe des cubes de $(\mathbf{Z}/31\mathbf{Z})^\times$. Comme $(\mathbf{Z}/31\mathbf{Z})^\times$ est cyclique d'ordre 30 et que $2^{10} = 1$, l'élément 2 est un cube de $(\mathbf{Z}/31\mathbf{Z})^\times$. On en conclut que $(2, K/\mathbf{Q}) = 1$. Ainsi $f_\mathfrak{p} = 1$ et $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_2$.

5) Supposons que $\mathcal{O}_K = \mathbf{Z}[\alpha]$. Soit P le polynôme minimal de α sur $\mathbf{Q}$. On a $P \in \mathbf{Z}[X]$. De plus
$$\mathcal{O}_K/(2) \simeq \mathbb{F}_2[X]/(\overline{P})$$
où $\overline{P}$ désigne la réduction de P modulo 2. Comme il y a 3 idéaux maximaux de $\mathcal{O}_K$ au-dessus de 2, le polynôme $\overline{P}$ se factorise en produit de 3 polynômes unitaires distincts de $\mathbb{F}_2[X]$. Comme il y a exactement 2 polynômes unitaires de degré 1 dans $\mathbb{F}_2[X]$, on obtient une contradiction.

6) Soit p un nombre premier qui n'est pas un cube modulo 31. Par exemple $p = 3$ ($3^{10} = 25$ dans $\mathbb{F}_{31}$). Alors l'élément $(3, K/\mathbf{Q})$ est non trivial dans $\mathrm{Gal}(K/\mathbf{Q})$ donc est d'ordre 3. Il y a donc un unique idéal maximal de $\mathcal{O}_K$ au-dessus de 3. Comme 3 est de plus non ramifié dans K, on en déduit que (3) est premier dans $\mathcal{O}_K$.

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 $\mathcal{O}_F^\times$.

Corrigé :

1) Les éléments de torsion de $F^\times$ sont des racines de l'unité. Comme F est isomorphe à un sous-corps de $\mathbb{R}$, les seules racines de l'unité de F sont ± 1.

Si $-1 \in 1+p\mathcal{O}_F$, il existe $a \in \mathcal{O}_F$ tel que $-1 = 1+pa$, c'est-à-dire $-2 = pa$. On en déduit que $4 = p^2 N_{F/\mathbf{Q}}(a)$ dans $\mathbf{Z}$, ce qui est absurde vu que p est impair.

2) On montre par récurrence sur $n \geqslant 1$ que, pour tout $a \in \mathcal{O}_F$, $(1+pa)^{p^n} \in 1+p^{n+1}\mathcal{O}_F$. On en déduit que les éléments du groupe quotient $(1+p\mathcal{O}_F)\cap \mathcal{O}_F^\times/(1+p^n\mathcal{O}_F)\cap\mathcal{O}_F^\times$ sont d'ordre un diviseur de p^{n-1}. Comme de plus le groupe $(1+p\mathcal{O}_F)\cap\mathcal{O}_F^\times$ est un sous-groupe de $\mathcal{O}_F^\times$ qui est de type fini d'après le théorème de Dirichlet, on en déduit que $(1+p\mathcal{O}_F)\cap\mathcal{O}_F^\times$ est un groupe abélien de type fini dont tous les éléments sont de torsion d'ordre une puissance de p, c'est donc un p-groupe.

3) Si $(1+p\mathcal{O}_F)\cap\mathcal{O}_F^\times = \{1\}$, le résultat est évident. On suppose donc $(1+p\mathcal{O}_F)\cap\mathcal{O}_F^\times \neq \{1\}$. D'après le théorème de Dirichlet, le groupe $\mathcal{O}_F^\times$ est isomorphe à $\{\pm 1\}\times\mathbf{Z}$. Comme $(1+p\mathcal{O}_F)\cap\mathcal{O}_F^\times$ est un sous-groupe sans torsion et non trivial de $\mathcal{O}_F^\times$, il est isomorphe à $\mathbf{Z}$. Le groupe $(1+p\mathcal{O}_F)\cap\mathcal{O}_F^\times/(1+p^n\mathcal{O}_F)\cap\mathcal{O}_F^\times$ est donc un quotient fini de $\mathbf{Z}$ dont les éléments sont d'ordre une puissance de p, il est donc isomorphe à $\mathbf{Z}/p^{k_n}\mathbf{Z}$ pour un entier $k_n \geqslant 0$. On en conclut que le sous-groupe $(1+p^n\mathcal{O}_F)\cap\mathcal{O}_F^\times$ est exactement le sous-groupe des puissances p^{k_n} de $(1+p\mathcal{O}_F)\cap\mathcal{O}_F^\times$. Soit $a \in \bigcap_n (1+p^n\mathcal{O}_F)\cap\mathcal{O}_F^\times$. Alors $p^n \mid a-1$ dans $\mathcal{O}_F$ pour tout $n \geqslant 1$, c'est-à-dire $p^{2n} \mid N_{F/\mathbf{Q}}(a-1)$ pour tout $n \geqslant 1$, de sorte que $N_{F/\mathbf{Q}}(a-1) = 0$ et $a = 1$. On a prouvé que $\bigcap_n (1+p^n\mathcal{O}_F)\cap\mathcal{O}_F^\times = \{1\}$, ce qui implique $\lim_{n\to+\infty} k_n = +\infty$. On en déduit le résultat.

4) On raisonne de la même façon que précédemment en utilisant le fait que $1+4\mathcal{O}_F \cap \mathcal{O}_F^\times$ est sans torsion et que $(1+4a)^{2^n} \in 1+2^{n-2}\mathcal{O}_F$.

5) On décompose $m = p_1^{k_1}\cdots p_r^{k_r}$ en produit de facteurs premiers. Pour tout $1 \leqslant i \leqslant r$, il existe s_i tel que si $a \in \mathcal{O}_F^\times$ vérifie $a \equiv 1\,[p]_i^{s_i}$, il existe $\alpha_i \in \mathcal{O}_F^\times$ tel que $\alpha_i^{p^{k_i}} = a$. En posant $n = \prod_i p_i^{s_i}$, il existe $\alpha_i \in \mathcal{O}_F^\times$ tel que $a = \alpha_i^{p_i^{k_i}}$. On en déduit par récurrence sur r que a est une puissance m-ième dans $\mathcal{O}_F^\times$. En effet, si u et v sont deux entiers premiers entre eux et $a = \alpha^u\beta^v$, si $ku+\ell v = 1$ est une relation de Bezout, alors $a = (\alpha^\ell\beta^k)^{uv}$.

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).

Corrigé :

1) Montrons que $F^\times$ est un sous-groupe discret de I_f, il est donc fermé. En effet, si $\gamma \in F^\times \cap \prod_{v\neq\infty} \mathcal{O}_F^\times$, alors $\gamma \in \mathcal{O}_F^\times$. D'après le théorème de Dirichlet, le groupe $\mathcal{O}_F^\times$ est fini. Ainsi $F^\times$ possède un voisinage de l'identité fini pour la topologie induite par celle de I_F, c'est donc un sous-groupe discret.

2) Soit V un voisinage de l'identité dans I_f. Il existe un ensemble fini S de places finies de F, ainsi que des sous-groupes ouverts $U_v \subset \mathcal{O}_v^\times$ tels que

$$U \coloneqq \prod_{v\in S} U_v \times \prod_{v\notin S} \mathcal{O}_v^\times \subset V.$$

Le groupe quotient $\prod_{v\neq\infty} \mathcal{O}_F^\times / U$ est fini, et puisque $F^\times \cap \prod_{v\neq\infty} \mathcal{O}_v^\times = \mathcal{O}_F^\times$ est infini, le groupe $U \cap F^\times \subset \mathcal{O}_F^\times$ est d'indice fini dans $\mathcal{O}_F^\times$, et est donc infini. On en conclut que $F^\times$ n'est pas un sous-groupe discret de I_f.

3) Le groupe I_f est localement compact et métrisable, c'est donc un espace topologique complet. Supposons que $F^\times$ est fermé dans I_f, c'est donc un espace métrique complet. Comme $F^\times$ n'est pas discret, le singleton $\{1\}$ est un fermé d'intérieur vide dans $F^\times$. Comme $F^\times$ est un groupe topologique, il en est de même de $\{\gamma\}$ pour tout $\gamma \in F^\times$. Comme $F^\times$ est dénombrable, on déduit du théorème de Baire qu'il est d'intérieur vide dans lui-même. D'où la contradiction.