ENS de Lyon
M1 Introduction à la théorie des nombres

Corrigé de l'examen partiel du 5 mars 2019

Exercice 1 — Soit p un nombre premier congru à 3 modulo 4.

1. Il s'agit d'un résultat vu en cours (début de la démonstration du théorème 2.22). Rappelons l'argument pour mémoire. L'extension $\mathbf{Q}(\zeta_p)/\mathbf{Q}$ est galoisienne, de groupe de Galois cyclique d'ordre $p-1$. Puisque $2|p-1$, ce groupe admet un unique quotient d'ordre 2 et il existe donc une unique extension quadratique K de $\mathbf{Q}$ contenue dans $\mathbf{Q}(\zeta_p)$. Le discriminant du corps de nombres $\mathbf{Q}(\zeta_p)$ étant une puissance de p, seul le nombre premier p peut être ramifié dans ce corps ; on en déduit que seul p peut-être ramifié dans K, donc $|D_K|$ est également une puissance de p. Si l'on écrit $K = \mathbf{Q}(\sqrt{d})$ avec $d \in \mathbf{Z}$ sans facteur carré, alors $D_K = d$ si $d \equiv 1 \pmod 4$ et $D_K = 4d$ si $d \equiv 3 \pmod 4$. On en déduit $d = -p$ et $K = \mathbf{Q}(\sqrt{-p})$.

2. Il s'agit d'un résultat vu en TD (Fiche 1, exercice 2). Rappelons l'argument pour mémoire. Soit Σ_L l'ensemble des plongements de L dans $\mathbf{C}$ et soit Σ_K l'ensemble des plongements de K dans $\mathbf{C}$. Pour tout $\alpha \in L$,

$$\mathrm{N}_{L/\mathbf{Q}}(\alpha) = \prod_{\sigma\in\Sigma_L} \sigma(\alpha) = \prod_{\tau\in\Sigma_K} \prod_{\substack{\sigma\in\Sigma_L \\ \sigma_{|K}=\tau}} \sigma(\alpha) = \prod_{\tau\in\Sigma_K} \tau(\mathrm{N}_{L/K}(\alpha)) = \mathrm{N}_{K/\mathbf{Q}}\left(\mathrm{N}_{L/K}(\alpha)\right).$$

3. L'application $\mathrm{N}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}(\sqrt{-p})}$ envoie $\mathbf{Z}[\zeta_p]$ dans $\mathcal{O}_{\mathbf{Q}(\sqrt{-p})}$. D'après la question précédente, on a donc

$$\mathrm{N}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\mathbf{Z}[\zeta_p]) = \mathrm{N}_{\mathbf{Q}(\sqrt{-p})/\mathbf{Q}}\left(\mathrm{N}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}(\sqrt{-p})}(\mathbf{Z}[\zeta_p])\right) \subset \mathrm{N}_{\mathbf{Q}(\sqrt{-p})/\mathbf{Q}}(\mathcal{O}_{\mathbf{Q}(\sqrt{-p})}).$$

Comme $-p \equiv 1 \pmod 4$, l'anneau $\mathbf{Q}(\zeta_p)$ est $\mathbf{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ et

$$\begin{aligned}\mathrm{N}_{\mathbf{Q}(\sqrt{-p})/\mathbf{Q}}\left(x + y\frac{1+\sqrt{-p}}{2}\right) &= \left(x + y\frac{1+\sqrt{-p}}{2}\right)\left(x + y\frac{1-\sqrt{-p}}{2}\right) = \left(x+\frac{y}{2}\right)^2 + \frac{p}{4}y^2 \\ &= x^2 + xy + \frac{p+1}{4}y^2.\end{aligned}$$

pour tous $x, y \in \mathbf{Z}$. Tout élément de $\mathrm{N}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\mathbf{Z}[\zeta_p])$ s'écrit donc sous cette forme.

4. La factorisation de ℓ dans $\mathbf{Z}[\zeta_p]$ reflète celle de Φ_p dans $\mathbf{F}_\ell[T]$. Puisque $\ell \equiv 1 \pmod p$, le polynôme $T^p - 1$ divise $T^{\ell-1} - 1$ et Φ_p est scindé sur $\mathbf{F}_\ell$. Le nombre premier ℓ est donc totalement décomposé dans $\mathbf{Q}(\zeta_p)$. Considérons un diviseur premier $\mathfrak{q}$ de ℓ dans $\mathbf{Z}[\zeta_p]$. Si l'anneau $\mathbf{Z}[\zeta_p]$ est principal, alors il existe α dans $\mathbf{Z}[\zeta_p]$ tel que $\mathfrak{q} = \alpha\mathbf{Z}[\zeta_p]$ et

$$\ell = \mathrm{N}(\mathfrak{q}) = \mathrm{N}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\alpha).$$

5. Raisonnons par l'absurde. Si l'anneau $\mathbf{Z}[\zeta_{23}]$ est principal, alors le nombre premier 47 est la norme d'un élément de $\mathbf{Z}[\zeta_{23}]$ d'après la question 4, donc peut s'écrire sous la forme $x^2+xy+6y^2 = (x+y/2)^2+\frac{23}{4}y^2$ avec $x, y \in \mathbf{Z}$. Cette condition implique $y^2 < 9$, donc $|y| \leqslant 2$, et on vérifie directement que les trois équations

$$x^2 = 47, \quad (2x \pm 1)^2 + 23 = 188 \quad \text{et} \quad (x \pm 1)^2 + 23 = 47$$

n'ont pas de solution entière. L'anneau $\mathbf{Z}[\zeta_{23}]$ n'est donc pas principal.

Exercice 2 — L'indice de $\mathbf{Z}[\alpha]$ dans $\mathcal{O}_K$ divise le discriminant de f en vertu de l'identité

$$\mathrm{disc}(f) = (\mathcal{O}_K : \mathbf{Z}[\alpha])D_K$$

donc p ne divise pas cet indice et la factorisation de p dans $\mathcal{O}_K$ reflète celle de f dans $\mathbf{F}_p[T]$ en vertu de la proposition 2.12 du cours. L'hypothèse d'irréductibilité de f dans $\mathbf{F}_p[T]$ se traduit donc par le fait que p est inerte dans $\mathcal{O}_K$, c'est-à-dire que l'idéal $\mathfrak{p} = p\mathcal{O}_K$ est premier.

Puisque $\mathfrak{p}$ est l'unique idéal premier de $\mathcal{O}_K$ divisant p, il est stabilisé par l'action du groupe de Galois et donc

$$\mathrm{Gal}(K|\mathbf{Q}) = \mathrm{D}(\mathfrak{p}/p).$$

Comme p est non ramifié dans K, le groupe $\mathrm{D}(\mathfrak{p}/p)$ est (canoniquement) isomorphe au groupe de Galois de l'extension de corps finis $\kappa(\mathfrak{p})/\mathbf{F}_p$, donc cyclique et engendré par l'élément de Frobenius $(\mathfrak{p}, K/\mathbf{Q})$. Nous en déduisons que le groupe $\mathrm{Gal}(K|\mathbf{Q})$ est cyclique.

Exercice 3 — 1. Si $\mathfrak{a} = (a)$ est un idéal principal de $\mathcal{O}_K$ contenant (π), alors il existe $b \in \mathcal{O}_K$ tel que $\pi = ab$. Puisque π est irréductible, ceci implique $\pi|a$, et donc $\mathfrak{a} = (\pi)$, ou $\pi|b$, et donc $a \in \mathcal{O}_K^\times$, $\mathfrak{a} = \mathcal{O}_K$. L'idéal (π) est donc maximal parmi les idéaux principaux de $\mathcal{O}_K$.

2. Considérons la factorisation de l'idéal (π) en produit d'idéaux premiers de $\mathcal{O}_K$:

   $$(\pi) = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_m.$$

   Cet idéal n'étant pas premier, $m \geqslant 2$.
   Les deux idéaux premiers $\mathfrak{p}_1$ et $\mathfrak{p}_2$ contiennent strictement l'idéal (π), donc ils ne sont pas principaux en vertu de la question 1. Leurs classes $\overline{\mathfrak{p}_1}, \overline{\mathfrak{p}_2}$ dans le groupe $\mathrm{Cl}(\mathcal{O}_K)$ sont ainsi non triviales, donc

   $$\overline{\mathfrak{p}_1\mathfrak{p}_2} = \overline{\mathfrak{p}_1} \cdot \overline{\mathfrak{p}_2} = 1$$

   en vertu de l'hypothèse $\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbf{Z}/2\mathbf{Z}$ et $\mathfrak{p}_1\mathfrak{p}_2$ est par conséquent un idéal principal.
   Il découle alors de la question 1 que l'inclusion $(\pi) \subset \mathfrak{p}_1\mathfrak{p}_2$ est une égalité.

3. L'ensemble $\mathcal{I}$ est le monoïde libre sur l'ensemble $\mathcal{P}$ des idéaux premiers de $\mathcal{O}_K$, donc l'application

   $$f : \mathcal{P} \to \mathbf{N}, \quad \mathfrak{p} \mapsto \begin{cases} 2 & \text{si } \mathfrak{p} \text{ est principal} \\ 1 & \text{sinon} \end{cases}$$

   se prolonge de manière unique en un morphisme de monoïdes $f : \mathcal{I} \to \mathbf{N}$.

4. Soit π un élément irréductible de $\mathcal{O}_K$. Si l'idéal (π) est premier, alors $f(\pi) = 2$; sinon, on peut écrire $(\pi) = \mathfrak{p}_1\mathfrak{p}_2$ avec $\mathfrak{p}_1$ et $\mathfrak{p}_2$ deux idéaux premiers non principaux (question 2), et alors

   $$f(\pi) = f(\mathfrak{p}_1) + f(\mathfrak{p}_2) = 1 + 1 = 2.$$

   Ainsi, $f(\pi) = 2$ pour tout élément irréductible π de $\mathcal{O}_K$.

   Si $\pi_1, \ldots, \pi_n, \pi'_1, \ldots, \pi'_m$ sont des éléments irréductibles de $\mathcal{O}_K$ tels que

   $$\pi_1 \cdot \ldots \cdot \pi_n = \pi'_1 \cdot \ldots \cdot \pi'_m$$

   alors

   $$2n = f(\pi_1) + \ldots + f(\pi_n) = f(\pi_1 \cdot \ldots \cdot \pi_n) = f(\pi'_1 \cdot \ldots \cdot \pi'_n) = f(\pi'_1) + \ldots + f(\pi'_n) = 2m$$

   et donc $m = n$.

5. Comme $-31 \equiv 1 \pmod 4$, l'anneau $\mathcal{O}_K$ est $\mathbf{Z}\left[\frac{1+\sqrt{-31}}{2}\right]$ et

$$\mathrm{N}_{K/\mathbf{Q}}\left(a+b\frac{1+\sqrt{-31}}{2}\right) = \left(a+\frac{b}{2}\right)^2 + \frac{31}{4}b^2 = a^2+ab+8b^2.$$

6. Si $2 = xy$ avec $x, y \in \mathcal{O}_K$, alors

$$4 = \mathrm{N}_{K/\mathbf{Q}}(x)\mathrm{N}_{K/\mathbf{Q}}(y)$$

et donc $\mathrm{N}_{K/\mathbf{Q}}(x), \mathrm{N}_{K/\mathbf{Q}}(y) \in \{1,2,4\}$. Il découle immédiatement de la formule explicite de la question précédente que 2 n'est pas la norme d'un élément de $\mathcal{O}_K$, donc $\mathrm{N}_{K/\mathbf{Q}}(x) = 1$ ou $\mathrm{N}_{K/\mathbf{Q}}(y) = 1$ et x ou y est inversible dans $\mathcal{O}_K$. Ainsi, 2 est un élément irréductible de $\mathcal{O}_K$.

7. On peut écrire

$$8 = \mathrm{N}_{K/\mathbf{Q}}\left(\frac{1+\sqrt{-31}}{2}\right) = \frac{1+\sqrt{-31}}{2}\cdot\frac{1-\sqrt{-31}}{2}.$$

On justifie comme précédemment l'irréductibilité de $\frac{1\pm\sqrt{-31}}{2}$ dans $\mathcal{O}_K$: si tel n'était pas le cas, il existerait dans $\mathcal{O}_K$ un élément de norme 2 et ceci est exclu par la question 5.

8. L'identité

$$2^3 = \frac{1+\sqrt{-31}}{2}\cdot\frac{1-\sqrt{-31}}{2}$$

montre qu'il n'y a pas unicité du nombre de facteurs irréductibles des éléments de l'anneau $\mathcal{O}_K$. Celui-ci n'est donc pas factoriel, et son groupe des classes n'est pas d'ordre 2 en vertu de la première partie.

Exercice 4 — Soit p un nombre premier impair tel que $p \equiv 1 \pmod 4$.

1. Si 2 est une puissance quatrième dans $\mathbf{F}_p$, alors 2 est un carré dans $\mathbf{F}_p$ et donc $p \equiv \pm 1 \pmod 8$ en vertu de la loi de réciprocité quadratique (deuxième loi complémentaire). Puisque $p \equiv 1 \pmod 4$, on a $p \equiv 1 \pmod 8$.

2. Soit p un nombre premier congru à 1 modulo 8.
   (i) Comme $p \equiv 1 \pmod 4$, p est décomposé dans $\mathbf{Q}(i)$. L'anneau $\mathbf{Z}[i]$ étant principal, il contient un élément de norme p et donc

$$p = \mathrm{N}_{\mathbf{Q}(i)/\mathbf{Q}}(a+ib) = a^2+b^2$$

   avec $a, b \in \mathbf{Z}$. Les deux entiers a et b doivent être de parité différente, donc on peut supposer a impair et b pair. On a $a^2 \equiv 1 \pmod 8$, donc $b^2 \equiv 0 \pmod 8$ et $4|b$.

   (ii) En utilisant le symbole de Jacobi, la loi de réciprocité quadratique permet d'écrire

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{b^2}{a}\right) = 1$$

   donc a est un carré modulo p.

   (iii) L'entier a est premier à p, donc inversible modulo p, et il existe ainsi $x \in \mathbf{Z}$ tel que $b \equiv ax \pmod p$. On en déduit

$$a^2(1+x^2) \equiv a^2+b^2 \equiv 0 \pmod p$$

   donc $x^2 \equiv -1 \pmod p$.

   (iv) On a

$$\left(\frac{a+b}{p}\right) \equiv (a+b)^{\frac{p-1}{2}} \equiv \left((a+b)^2\right)^{\frac{p-1}{4}} \equiv (2ab)^{\frac{p-1}{4}} \pmod p.$$

(v) L'entier $a+b$ est impair. En utilisant le symbole de Jacobi, la loi de réciprocité quadratique permet d'écrire

$$\left(\frac{a+b}{p}\right) = \left(\frac{p}{a+b}\right) = \left(\frac{2}{a+b}\right)\left(\frac{2p}{a+b}\right) = \left(\frac{2}{a+b}\right)\left(\frac{(a+b)^2+(a-b)^2}{a+b}\right) = \left(\frac{2}{a+b}\right)\left(\frac{(a-b)^2}{a+b}\right)$$

donc

$$\left(\frac{a+b}{p}\right) = \left(\frac{2}{a+b}\right) = (-1)^{\frac{(a+b)^2-1}{8}}.$$

(vi) En vertu de la question (iii),

$$(ab)^{\frac{p-1}{4}} \equiv (a^2x)^{\frac{p-1}{4}} \equiv a^{\frac{p-1}{2}} x^{\frac{p-1}{4}} \equiv \left(\frac{a}{p}\right) x^{\frac{p-1}{4}} \equiv x^{\frac{p-1}{4}} \pmod{p}.$$

En identifiant les seconds membres des identités (iv) et (v), il vient alors

$$2^{(p-1)/4}x^{(p-1)/4} \equiv 2^{(p-1)/4}(ab)^{(p-1)/4} \equiv (-1)^{((a+b)^2-1)/8} \equiv (-1)^{(p-1)/8}(-1)^{ab/4} \pmod{p}$$

et donc

$$2^{(p-1)/4} \equiv (-1)^{ab/4} \pmod{p}$$

puisque $x^2 \equiv -1 \pmod{p}$.

3. Soit p un nombre premier congru à 1 modulo 4. D'après la question 1, la condition $p \equiv 1 \pmod{8}$ est nécessaire pour que 2 soit une puissance quatrième modulo p. Supposons qu'elle soit satisfaite et écrivons p sous la forme $p = a^2 + b^2$ avec $2 \nmid a$ et $4|b$ en vertu de la question 2(i).

Si 2 est une puissance quatrième dans $\mathbf{F}_p$, alors $2^{(p-1)/4} \equiv 1 \pmod{p}$. Réciproquement, supposons que l'on ait $2^{(p-1)/4} \equiv 1 \pmod{p}$. Si ω est un générateur du groupe cyclique $\mathbf{F}_p^\times$ et si $2 \equiv \omega^m \pmod{p}$, alors $1 \equiv 2^{(p-1)/4} \equiv \omega^{m(p-1)/4} \pmod{p}$, donc $p-1|m(p-1)/4$ et $4|m$, ce qui prouve que 2 est une puissance quatrième dans $\mathbf{F}_p$. Ainsi,

$$2 \text{ est une puissance quatrième dans } \mathbf{F}_p \;\Leftrightarrow\; 2^{\frac{p-1}{4}} \pmod{p}.$$

En vertu de la question précédente, $2^{(p-1)/4} \equiv 1 \pmod{p}$ si et seulement si $8|ab$, donc si et seulement si $8|b$ puisque $2 \nmid a$. On en déduit que 2 est une puissance quatrième modulo p si et seulement si p est de la forme

$$a^2 + 8^2B^2 = A^2 + 64B^2$$

avec $A, B \in \mathbf{Z}$.

Remarque. La condition $p \equiv 1 \pmod{4}$ a été oubliée dans l'énoncé de l'exercice. Cela empêchait de traiter convenablement la question 1.