UPMC Master M1 de mathématiques 14-15
D. Bertrand *4M020 - Théorie des nombres*

Examen du 16 Juin 2015
Durée: 3 heures

L'usage du polycopié du cours et des feuilles d'exercices est autorisé.
Les calculettes ne sont pas autorisées.
Les 4 énoncés sont indépendants.

I

1°/ Soit p un nombre premier de la forme $p = 2^n + 1$, où $n \geq 2$.
i) Calculer la classe de p modulo 3.
ii) Montrer que 3 n'est pas résidu quadratique modulo p.
iii) Soit ν l'ordre de $\bar{3}$ dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. Montrer que $\nu = 2^n$.

2°/ Ici, p est un nombre premier $\equiv 3$ modulo 8 et tel que $q = \frac{p-1}{2}$ est encore un nombre premier. Soit μ l'ordre de $\bar{2}$ dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. Montrer que $\mu = 2q$.

3°/ Donner la décomposition en produits d'éléments irréductibles du polynôme cyclotomique $\Phi_{17}(T)$ dans $\mathbb{F}_3[T]$, et celle du polynôme cyclotomique $\Phi_{11}(T)$ dans $\mathbb{F}_2[T]$.

II

Pour tout nombre réel $\alpha > 0$, on désigne par $\sqrt{-\alpha}$ le nombre complexe $i\sqrt{\alpha}$. On considère les nombres $x = \sqrt{1+\sqrt{3}}$, $y = \sqrt{1-\sqrt{3}}$, et les corps

$$K = \mathbb{Q}(\sqrt{3}, \sqrt{-2}) \ , M = \mathbb{Q}(x) \ , L = \mathbf{Q}(x, y).$$

1°/ Montrer que le polynôme $P(T) = T^4 - 2T^2 - 2$ est irréductible sur $\mathbb{Q}$, et calculer le degré de x sur $\mathbb{Q}$.

2°/ Calculer xy. Montrer que L contient K, que $y \notin M$, et calculer le degré de L sur $\mathbb{Q}$.

3°/ Montrer que $L/\mathbb{Q}$ est une extension galoisienne, et que son groupe de Galois n'est pas abélien.

4°/ Pour tout corps de nombres k, soit U_k le groupe des unités de l'anneau des entiers de k. Calculer les rangs de U_K, de U_L et de U_M.

III

Soient K le corps quadratique imaginaire $\mathbb{Q}(\sqrt{-10})$, et $\mathbf{O}$ son anneau d'entiers.

1°/ Donner une base de $\mathbf{O}$ sur $\mathbb{Z}$, calculer son discriminant D, et vérifier que la constante de Minkowski M_K de K est < 6.

2°/ i) Montrer qu'il existe un unique idéal **p** de **O** de norme 2, et qu'il n'est pas principal.
ii) Montrer qu'il existe un unique idéal **q** de **O** de norme 5, et qu'il n'est pas principal.
iii) Montrer que **pq** est principal.

3°/ Montrer que **O** n'admet pas d'idéal de norme 3.

4°/ Déterminer le nombre de classes h_K de K.

IV

Soient p et q deux nombres premiers impairs et distincts.

1°/ Soient α et β deux entiers rationnels. Montrer que l'ensemble $L = L_{\alpha,\beta}$ des triplets $(x, y, z) \in \mathbb{Z}^3$ satisfaisant le système de congruences:

$$(*) \quad \begin{cases} x \equiv \beta z \pmod{q} \\ y \equiv \alpha z \pmod{p} \\ x \equiv z \pmod{2} \\ y \equiv 0 \pmod{2} \end{cases}$$

est un sous-groupe de $\mathbb{Z}^3$ d'indice fini, égal à $4pq$.

2°/ On suppose désormais que p est un carré modulo q, et que $p \equiv 1 \pmod{4}$.
i) Montrer que q est un carré modulo p.
ii) Montrer qu'il existe des entiers rationnels α et β tels que $p\beta^2 + q\alpha^2 \equiv 1 \pmod{pq}$.
iii) Montrer qu'avec ce choix de α, β, les congruences $(*)$ entraînent:

$$px^2 + qy^2 \equiv z^2 \pmod{4pq}.$$

3°/ Calculer le volume de l'ellipsoïde **K** de $\mathbb{R}^3$ défini par l'inégalité

$$px^2 + qy^2 + z^2 < 4pq.$$

(On rappelle que le volume de la sphère unité vaut $\frac{4}{3}\pi$.)

4°/ Montrer que l'équation $px^2 + qy^2 = z^2$ admet une solution en entiers rationnels (x, y, z) non tous nuls.

Esquisse de corrigé

I. 1/ i) Comme $2 \equiv -1 \bmod 3$, on a $p \equiv (-1)^n + 1 \equiv 2 \bmod 3$ (car $p \not\equiv 0 \bmod 3$; en fait, n est forcément une puissance de 2 : nombres premiers de Fermat). -ii) Ainsi, $(\frac{p}{3}) = (\frac{2}{3}) = -1$, d'où $(\frac{3}{p}) = -1$ par la LRQ. -iii) ν divise $|\mathbb{F}_p^*| = p-1$, donc vaut $2^k, k \leq n$. Mais $\bar{3}^{2^{n-1}} = \bar{3}^{\frac{p-1}{2}} = (\frac{3}{p}) = -1$, donc $2^k > 2^{n-1}$ et $\nu = 2^n$. (Donc $\bar{3}$ engendre $(\mathbb{Z}/p\mathbb{Z})^*$.)

2/ $p \equiv 3 \bmod 8 \Rightarrow 2$ n'est pas RQ dans $\mathbb{F}_p^*$, et $\bar{2}^q = -1$. Mais μ divise $p-1 = 2q$, donc vaut 2 ou $2q$. Comme $2^2 \not\equiv 1 \bmod p$ ($\neq 3$), il vaut $2q$. (Donc $\bar{2}$ engendre $(\mathbb{Z}/p\mathbb{Z})^*$.)

3/ $\bar{3}$ engendre $(\mathbb{Z}/17\mathbb{Z})^* \Rightarrow$ (TD 2, Ex. 10) Φ_{17} irréductible dans $\mathbb{F}_3[T]$. Idem pour l'autre.

II. 1/ P vérifie le critère d'Eisentein en $p = 2$. Comme $(x^2-1)^2 - 3 = P(x) = 0$, c'est $Min_{x;\mathbb{Q}}$, et x est de degré 4 sur $\mathbb{Q}$.

2/ On a $xy = \sqrt{-2}$, donc $K \subset L$, tandis que y, dont le carré est < 0, n'appartient pas $M \subset \mathbb{R}$. Comme $y^2 \in M$, y est donc de degré 2 sur M, et $[L : \mathbb{Q}] = 2.4 = 8$.

3/ Le polynôme $P(T) = (T-x)(T+x)(T-y)(T+y)$ admet L comme corps de décomposition sur $\mathbb{Q}$, donc $L/\mathbb{Q}$ est galoisienne. Comme $P = Min_{x,\mathbb{Q}}$, y est un conjugué de x sur $\mathbb{Q}$, donc $M/\mathbb{Q}$ n'est pas galoisienne et $Gal(L/\mathbb{Q})$ ne peut être abélien.

4/ L'image de K par chacun de ses plongements dans $\mathbb{C}$ contient $\sqrt{-2}$, donc $s_K = 0$ plongements réels, $2t_K = 4$ complexes, et le rang de U_K vaut $r_K = s_K + t_K - 1 = 1$. De même, $s_L = 0, 2t_L = 8$ et $r_L = 3$. Enfin, $s_M = 2, 2t_M = 2$, donc $r_M = 2$.

III. 1/ i) $\mathbf{O} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-10}, D = -40, M_K = \frac{4}{\pi}\frac{2!}{2^2}\sqrt{40} = \frac{4}{\pi}\sqrt{10} < 6$ (et même en fait < 5).

2/ i) D'après le poly, Chap. 6, Prop. 1, $2\mathbf{O} = \mathbf{p^2}$, donc $\mathbf{p}$ est le seul idéal de norme 2, et il n'est pas principal car $a^2 + 10b^2 \neq 2$. -ii) Idem pour $5|D$. -iii) Les idéaux $\mathbf{pq}$ et $(\sqrt{-10})$ sont égaux, puisqu'ils ont les mêmes carrés.

3/ Puisque $(\frac{-10}{3}) = -1$, la même référence entraîne que $3\mathbf{O}$ est un idéal premier de $\mathbf{O}$. Il est de norme 9, donc $\mathbf{O}$ n'a pas d'idéal de norme 3.

4/ Les idéaux de norme < 6 sont $\mathbf{O}, \mathbf{p}, \mathbf{p}^2, \mathbf{q}$, et leurs classes dans $C\ell_K$ sont celles de $\mathbf{O} \sim \mathbf{p}^2$ et de $\mathbf{q} \sim \mathbf{p}^{-1} \sim \mathbf{p} \not\sim \mathbf{O}$. Donc $h_K = 2$.

IV. 1/ Un changement de base de $\mathbb{Z}^3$ montre que les deux premières congruences $x - \beta z \equiv 0 \pmod q$, $y - \alpha z \equiv 0 \pmod p$ définissent un sous-groupe L' de $\mathbb{Z}^3$ d'indice pq. L est alors le noyau d'une application surjective de L' dans $(\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$, donc d'indice 4 dans L', et d'indice $4pq$ dans $\mathbb{Z}^3$.

2/ i) LRQ. -ii) Par hypothèse, il existe un carré β^2 dont la classe mod q est l'inverse de celle de p, donc un entier t tel que $p\beta^2 + qt = 1$. La classe de t mod p est l'inverse de celle de q, donc de la forme $t \equiv \alpha^2 \bmod p$, d'où $qt \equiv q\alpha^2 \bmod pq$ et $p\beta^2 + q\alpha^2 \equiv 1 \bmod pq$. - iii) Pour $(x, y, z) \in L_{\alpha,\beta}$, on a alors $px^2 + qy^2 \equiv z^2 \bmod pq$. Comme $p \equiv 1 \bmod 4$, les deux dernières congruences montrent que $px^2 - z^2$ et qy^2 sont divisible par 4. Comme $(4, pq) = 1$, on a bien $px^2 + qy^2 - z^2 \equiv 0 \bmod 4pq$.

3/ $Vol(\mathbf{K}) = \sqrt{\frac{1}{p}} \times \sqrt{\frac{1}{q}} \times \frac{4}{3}\pi \times (\sqrt{4pq})^3 = \frac{\pi}{3} \times 2^3 \times 4pq$.

4/ Avec les notations du poly, bas de la p. 36, on a $d(L) = [\mathbb{Z}^3 : L] = 4pq$, donc $Vol(\mathbf{K}) > 2^3 d(L)$ et le thm de Minkowski assure l'existence d'un point non nul (x, y, z) dans $L \cap \mathbf{K}$. Pour ce point, les entiers positifs ou nuls $px^2 + qy^2$ et z^2 sont de somme $< 4pq$, et diffèrent d'un multiple de $4pq$. Ils sont donc égaux.