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

Examen partiel du 27 Février 2015
Durée: 2 heures

L'usage du polycopié du cours et des feuilles d'exercices est autorisé.
Les calculettes ne sont pas autorisées.
Les 3 énoncés sont indépendants.

I

Pour tout entier $n \geq 1$, on note $\Phi_n \in \mathbb{Z}[X]$ le polynôme cyclotomique d'ordre n.

1°/ Montrer que si p est un nombre premier, $\Phi_{p^2}(X) = \Phi_p(X^p)$.

2°/ i) Vérifier que $\Phi_2(X) = -\Phi_1(-X)$, et montrer que $\Phi_{2n}(X) = \Phi_n(-X)$ pour tout entier *impair* $n > 1$.

ii) Calculer le polynôme $\Phi_{18}(X)$.

3°/ Pour chacun des éléments u du groupe multiplicatif $(\mathbb{Z}/18\mathbb{Z})^*$, donner l'ordre k_u de u.

4°/ i) Trouver le plus petit nombre premier $p \neq 2, 3$ tel qu'en réduction modulo p, le polynôme Φ_{18} de $\mathbb{F}_p[X]$ se décompose en facteurs linéaires dans $\mathbb{F}_p[X]$.

ii) Trouver le plus petit nombre premier $p' \neq 2, 3$ tel qu'en réduction modulo p', le polynôme Φ_{18} de $\mathbb{F}_{p'}[X]$ soit irréductible dans $\mathbb{F}_{p'}[X]$.

II

[On rappelle que le groupe alterné $\mathbf{A}_4$ est l'unique sous-groupe d'indice 2 du groupe symétrique $\mathbf{S}_4$.]

1°/ Montrer que le polynôme $P(T) = T^4 - 3T - 3$ est irréductible sur $\mathbb{Q}$, et qu'il admet deux racines réelles x, y, et deux racines complexes conjuguées $z, \overline{z}$.

2°/ Soit $P(T) = (T^2 - \alpha T + \beta)(T^2 + \alpha T + \beta')$ la décomposition de P en produit de deux polynômes de degré 2 de $\mathbb{R}[T]$, avec $\alpha = x + y = -(z + \overline{z})$. Vérifier (ou admettre) que α est racine du polynôme $X^6 + 12X^2 - 9$, et déterminer le polynôme minimal de α^2 sur $\mathbf{Q}$.

On note $L = \mathbf{Q}(x, y, z, \overline{z})$ le corps de décomposition de P sur $\mathbb{Q}$, et G le groupe de Galois de L sur $\mathbb{Q}$. L'action de G sur l'ensemble $\{x, y, z, \overline{z}\}$ permet d'identifier G à un sous-groupe de $\mathbf{S}_4$.

3°/ Montrer que le degré de L sur $\mathbb{Q}$ est divisible par 12. En déduire que G contient $\mathbf{A}_4$.

4°/ Montrer qu'il existe un automorphisme de L permutant z et $\overline{z}$, et fixant x et y. En déduire que $G = \mathbf{S}_4$.

5°/ Calculer le degré de α sur $\mathbb{Q}$.

T.S.V.P.

III

Soit p un nombre premier, $p \equiv 1 \pmod{4}$.

1°/ Montrer qu'il existe un entier t tel que $t^2 + 1 \equiv 0 \pmod{p}$.

2°/ On considère le sous-groupe $L = \{(x, y) \in \mathbb{Z}^2, y \equiv tx \pmod{p}\}$ de $\mathbb{Z}^2 \subset \mathbb{R}^2$. Montrer que L est un réseau de $\mathbb{R}^2$.

3°/ Montrer que $\epsilon_1 = (1, t)$ et $\epsilon_2 = (0, p)$ engendrent le groupe L et calculer le co-volume $d(L)$ de L dans $\mathbb{R}^2$.

4°/ Soit r un nombre réel $> \sqrt{\frac{3p}{2}}$. Montrer qu'il existe un élement (a, b) non nul de L tel que $a^2 + b^2 < r^2$.

5°/ Montrer que $a^2 + b^2 \equiv 0 \pmod{p}$. Pour un choix convenable de r, en déduire que $p = a^2 + b^2$.

Corrigé

I. **1°**/ Comme p est premier, les diviseurs de p^2 sont p^2 et les diviseurs de p, donc $\Phi_{p^2}(X) = \frac{X^{p^2}-1}{X^p-1}$, tandis que $\Phi_p(X) = \frac{X^p-1}{X-1}$, d'où $\Phi_p(X^p) = \Phi_{p^2}(X)$.
2°/ i) Comme n est impair, l'application $\zeta \mapsto \zeta' := -\zeta$ établit une bijection de l'ensemble des racines de l'unité ζ d'ordre égal à n vers l'ensemble des racines de l'unité ζ' d'ordre égal à $2n$. Les polynômes $\Phi_{2n}(X)$ et $\Phi_n(-X)$ ont ainsi les mêmes racines, toutes simples, et sont donc égaux dès que $n \neq 1$ (puisque $\phi(n)$ étant alors pair, ils sont tous deux unitaires). [Autre méthode : comme $(n, 2) = 1$, les diviseurs de $2n$ forment la réunion disjointe des diviseurs de n et des doubles des diviseurs de n, donc $\Pi_{d|n}\Phi_{2d}(X) = \frac{X^{2n}-1}{X^n-1} = X^n + 1$. Or $\Pi_{d|n}\Phi_d(-X) = (-X)^n - 1 = -(X^n + 1)$. Une récurrence sur n permet alors de vérifier l'assertion "$\Phi_{2n}(X) = \pm\Phi_n(-X)$", et la parité de $\phi(n)$ fournit les égalité recherchées.]
ii) $\Phi_{18}(X) = \Phi_9(-X) = \Phi_3((-X)^3) = \Phi_3(-X^3)$, et $\Phi_3(T) = T^2 + T + 1$. Par conséquent, $\Phi_{18}(X) = X^6 - X^3 + 1$.
3°/ Les $\phi(18) = \phi(9) = 3.2 = 6$ éléments de $(\mathbb{Z}/18\mathbb{Z})^*$ sont (les classes modulo 18 de) $u = 1$, d'ordre $k_1 = 1$, $u = 5$, d'ordre $k_5 = 6$ (car $5^2 \equiv 7, 5^3 \equiv -1$), $u = 7 \equiv 5^2$, d'ordre $k_7 = 3$, $u = 11 \equiv -7$, d'ordre $k_{11} = 6$, $u = 13 \equiv -5$, d'ordre $k_{13} = 3$, $u = 17 \equiv -1$, d'ordre $k_{17} = 2$.
4°/ On sait (voir feuille de TD no 2, ex. 10.c) que pour tout nombre premier p ne divisant pas n, le polynôme Φ_n se décompose dans $\mathbb{F}_p[X]$ en un produit de polynômes irréductibles de même degré, égal à l'orde k_p de la classe de p dans $(\mathbb{Z}/n\mathbb{Z})^*$. Pour (i), on cherche donc p tel que $k_p = 1$, c-à-d. $p \equiv 1$ mod. 18, et $p = 19$ répond à la question. Pour (ii), on cherche p' tel que $k_{p'} = 6$, c-à-d. $p' \equiv 5$ ou 11 mod. 18 et $p' = 5$ répond à la question.

II. **1°**/ Le critère d'Eisenstein avec $p = 3$ montre que P est irréductible sur $\mathbf{Q}$. Comme sa dérivée ne s'annule sur $\mathbf{R}$ qu'en $(\frac{3}{4})^{\frac{1}{3}}$, où P est < 0, P a exactement deux racines réelles.
2°/ On a $\beta\beta' = -3, \alpha(\beta' - \beta) = -3, \beta + \beta' - \alpha^2 = 0$, d'où $\alpha^2((\beta + \beta')^2 - 4\beta\beta') = 9$ et $\alpha^6 + 12\alpha^2 - 9 = 0$. Le polynôme unitaire $T^3 + 12T - 9$ n'a pas de racine dans $\mathbf{Z}$ (elles ne pourraient être egales qu'à $\pm 1, \pm 3 \pm 9$, où il ne s'annule pas), ni donc dans $\mathbf{Q}$ par le lemme de Gauss. Étant de degré 3, il est irréductible sur $\mathbf{Q}$. C'est donc le polynôme minimal de sa racine α^2.
3°/ Comme P est irréductible, x est de degré 4 sur $\mathbf{Q}$, et $4|[L : \mathbf{Q}]$. De même, $\alpha = x + y$, donc α^2, appartient à L, et $3 = [\mathbf{Q}(\alpha^2) : \mathbf{Q}]$ divise $[L : \mathbf{Q}]$. Donc $ppcm(3, 4)|[L : \mathbf{Q}]$. Par conséquent, le groupe de Galois de L sur $\mathbb{Q}$ est d'ordre ≥ 12, donc d'indice ≤ 2 dans $\mathbf{S_4}$. Vu le rappel, G est soit $\mathbf{A_4}$, soit $\mathbf{S_4}$ tout entier.
4°/ La conjugaison complexe induit sur L un automorphisme de corps σ, qui fixe x, y, et échange z et $\overline{z}$. Cet élément σ de G, lu dans $\mathbf{S_4}$, est une transposition (signature impaire), donc G n'est pas contenu dans $\mathbf{A}_4$, et $G = \mathbf{S}_4$.
5°/ Le degré de $\alpha = x + y$ sur $\mathbf{Q}$, qui, d'après 2^o/, vaut 3 ou 6, est égal au nombre de ses images sous l'action de G. Comme $G = \mathbf{S}_4$, ces images sont données par toutes les sommes de couples de racines de P. Or les nombres réels $x + y = \alpha$ et $z + \overline{z} = -\alpha$ sont distincts, et distincts des nombres imaginaires $x + z$ et $x + \overline{z}$, eux-mêmes complexes conjugués, donc distincts. Ainsi, α est de degré au moins 4, donc de degré 6, sur $\mathbf{Q}$.

III. **1°**/ Comme $p \equiv 1$ mod. 4, -1 est un résidu quadratique modulo p.
2°/ L est contenu dans $\mathbb{Z}^2$, donc est discret dans $\mathbb{R}^2$. Contenant deux éléments linéairement indépendants sur $\mathbb{R}$ (par exemple $(1,t)$ et $(1,t+p)$), il engendre $\mathbb{R}^2$ sur $\mathbb{R}$. C'est donc un réseau de $\mathbb{R}^2$.
3°/ Un point (x,y) appartient à L si et slt si d'une part, $x = m \in \mathbb{Z}$ et d'autre part, il existe un entier n tel que $y = mt + np$, autrement dit si et slt s'il existe deux entiers m, n tels $(x,y) = m(1,t) + n(0,p)$. Ainsi, $(1,t)$ et $(0,p)$ forment une base du réseau L, et $d(L) = det \begin{pmatrix} 1 & 0 \\ t & p \end{pmatrix} = p$.
4°/ Soit $\mathbf{K}$ le disque ouvert de centre 0 et de rayon r. C'est une partie convexe, symétrique par rapport à 0 et bornée de $\mathbb{R}^2$, d'aire $\mu(\mathbf{K}) = \pi r^2 > \frac{3\pi}{2} p > 2^2 d(L)$, car $3\pi > 8$. Le théorème de Minkowski assure alors l'existence d'un point (a,b) de L non nul et situé dans $\mathbf{K}$, donc tel que $a^2 + b^2 < r^2$.
5°/ Puisque $(a,b) \in L$, $b \equiv ta$ mod. p, donc $a^2 + b^2 \equiv a^2(1+t^2) \equiv 0$ mod. p. En choisissant r assez petit, on déduit de 4^o/ que $a^2 + b^2 \leq \frac{3}{2} p$. Ainsi, $a^2 + b^2$ est un entier non nul divisible par p, et strictement inférieur à $2p$. Il vaut donc p.