UPMC Master M1 de mathématiques 13-14
D. Bertrand *4M020 - Théorie des nombres*

Partiel du 28 Février 2014
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

On note G le groupe multiplicatif $\mathbb{F}_{41}^*$. On rappelle qu'il est cyclique, et on se propose de déterminer l'ensemble S de tous les générateurs de G.

1°/ i) Déterminer l'ordre de G, et le nombre d'éléments de S.
ii) Calculer le symbole de Legendre $(\frac{2}{41})$. En déduire que $2 \notin S$.
iii) Calculer $(\frac{3}{41}), (\frac{5}{41}), (\frac{-1}{41})$.

2°/ Soit $\Phi_8 \in \mathbb{F}_{41}[T]$ le polynôme cyclotomique d'ordre 8.
i) Montrer que l'équation $\Phi_8(x) = 0$ admet 4 racines $x_1, ..., x_4$ dans $\mathbb{F}_{41}^*$.
ii) Déterminer ces racines. (On pourra remarquer que $-1 \equiv 9^2$ mod. 41.)

3°/ Soit $\Phi_5 \in \mathbb{F}_{41}[T]$ le polynôme cyclotomique d'ordre 5.
i) Montrer que l'équation $\Phi_5(y) = 0$ admet 4 racines $y_1, ..., y_4$ dans $\mathbb{F}_{41}^*$.
ii) Vérifier que $y_1 = -4$ est l'une de ces racines.

4°/ i) Montrer que pour tout $1 \leq i, j, \leq 4$, le produit $x_i y_j$ appartient à S.
ii) Déterminer l'ensemble S.

II

Soient $m_1, ..., m_n$ des entiers rationnels > 0, premiers entre eux deux à deux, et $a_1, ..., a_n$ des entiers rationnels.

1°/ Soient s un entier ≥ 1 et $f : \mathbb{R}^s \to \mathbb{R}^s$ une application $\mathbb{R}$-linéaire de déterminant $\Delta \neq 0$. Pour tout $i = 1, ..., s$, on désigne par y_i la i-ième coordonnée du vecteur $y \in \mathbb{R}^s$. Montrer que le volume de l'ensemble $\mathbf{K} = \{x \in \mathbb{R}^s,\ \forall\ i = 1, ..., s\ :\ |(f(x))_i| \leq 1\ \}$ vaut $\frac{2^s}{|\Delta|}$.

2°/ Montrer que le système de $n + 2$ inégalités en $n + 2$ inconnues

$$\begin{cases} |z| < m_1 ... m_n \\ |u| < \frac{3}{2} \\ |z - a_i u - m_i k_i| < 1 \qquad (1 \leq i \leq n) \end{cases}$$

admet une solution en entiers $(z, u, k_1, ..., k_n) \in \mathbb{Z}^{n+2}$ non tous nuls.

3°/ Montrer que pour une telle solution, u ne peut pas être nul.

4°/ En déduire qu'il existe un entier rationnel z tel que $\forall i = 1, ..., n\ : z \equiv a_i \bmod m_i$. Ce résultat vous était-il connu ?

III

Soient p_1, p_2, p_3 trois nombres premiers distincts.

1°/ i) Calculer le degré de l'extension $\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}$.
ii) Calculer le degré de l'extension $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})/\mathbb{Q}(\sqrt{p_1})$.

2°/ i) Déterminer le groupe $G := Aut(L/\mathbb{Q})$, où $L = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$.
ii) Donner le nombre des sous-groupes d'indice 2 de G.
iii) Donner la liste des sous-corps $\{M_i, i \in I\}$ de L tels que $[M_i : \mathbb{Q}] = 2$. On explicitera chacun d'eux sous la forme $M_i = \mathbb{Q}(\sqrt{x_i})$, pour un nombre rationnel x_i convenablement choisi.

3°/ i) Montrer que $\sqrt{p_3}$ n'appartient à aucun de ces corps M_i.
ii) Calculer le degré de l'extension $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})/\mathbb{Q}$.

Corrigé

I 1°/ i) G a $\phi(41) = 40$ éléments. S est l'ensemble des générateurs d'un groupe cyclique isomorphe à $\mathbf{Z}/40\mathbf{Z}$, donc a $\phi(40) = \phi(8)\phi(5) = 16$ éléments.

ii) $(\frac{2}{41}) = 2^{42.40/8} = 1$; donc 2, carré d'un élément de G, est d'ordre au plus 20.

iii) $(\frac{3}{41}) = (-1)^{1.20}(\frac{41}{3}) = (\frac{2}{3}) = -1$. $(\frac{5}{41}) = (-1)^{2.20}(\frac{41}{5}) = 1$. $(\frac{-1}{41}) = (-1)^{20} = 1$.

2°/ i) Comme 8 divise 40, G admet un unique sous-groupe cyclique d'ordre 8, et ses $\phi(8) = 4$ générateurs $x_1, ..., x_4 \in \mathbb{F}_{41}^*$ sont par définition les racines de Φ_8.

ii) $\Phi_8(T) = \frac{T^8-1}{T^4-1} = T^4 + 1$. Ses racines sont les solutions de $(x^2)^2 = -1 = 9^2$, soit $x^2 = 9$ et $x_1 = 3, x_2 = -3$, ou $x^2 = -9 = (9.3)^2$ et $x_3 = 27 = -14, x_4 = 14$.

3°/ i) Comme 5 divise 40, G admet un unique sous-groupe cyclique d'ordre 5, et ses $\phi(5) = 4$ générateurs $y_1, ..., y_4 \in \mathbb{F}_{41}^*$ sont les racines de Φ_5.

ii) $(-4)^2 = 16, 16^2 = 10$ et $-4.10 = 1$, donc $y_1 = -4$ est d'ordre 5 dans G. Les autres racines sont donc $y_2 = 16, y_3 = y_1^3 = -64 = 18, y_4 = -72 = 10$.

4^o/ i) L'ordre de chaque $z = x_i y_j$ divise 40. Comme $z^8 = y_j^8 = y_j^3 \neq 1$ et $z^{20} = x_i^4 \neq 1$, z est d'ordre 40, donc est un des générateurs de G.

ii) Ces z sont distincts, car un élément d'ordre divisant 8 ne peut être égal à un élément d'ordre divisant 5 que s'il vaut 1. Il y a donc $4 \times 4 = 16 = cardS$ tels produits, et $S = \{x_i y_j; 1 \leq i, j, \leq 4\}$.

[NB : 2 et 5 (et 4) n'appartiennent pas à S, d'après le 1^o/; 3 non plus, car d'ordre 8 par le 2^o/. Le "plus petit" élément de S est en fait $x_4 y_3 = 14 \times 18 = 252 = 6$.]

II 1°/ Le changement de variable $x = f^{-1}(y)$, de déterminant jacobien Δ^{-1}, fournit la relation: $\mu(\mathbf{K}) = \int_{\mathbf{K}} dx_1...dx_s = \int_{|y_1|\leq 1,...,|y_s|\leq 1} \frac{1}{|\Delta|} dy_1...dy_s = \frac{2^s}{|\Delta|}$.

2°/ La matrice $\begin{pmatrix} \frac{1}{m_1...m_n} & 0 & 0 & 0 \\ 0 & \frac{2}{3} & 0 & 0 \\ 1 & -a_1 & -m_1 & 0 \\ 1 & -a_n & 0 & -m_n \end{pmatrix}$ définit un endomorphisme f de $\mathbb{R}^{n+2}$ pour lequel $x = (z, u, k_1, ..., k_n)$ vérifie le système si et slt si $\forall i = 1, ..., n+2 : |(f(x))_i| \leq 1$. Par conséquent, le volume de la partie $\mathbf{K}$ de $\mathbf{R}^{n+2}$ définie par ces inégalités vaut $2^{n+2}(\frac{1}{m_1...m_n} \times \frac{2}{3} \times m_1...m_n)^{-1} = 2^{n+2} \times \frac{3}{2}$, qui est $> 2^{n+2} \times 1$. Comme $\mathbf{K}$ est convexe, bornée et symétrique par rapport à 0, et que le réseau $\mathbf{Z}^{n+2}$ de $\mathbf{R}^{n+2}$ a pour covolume 1, le théorème de Minkowski permet de conclure.

3°/ Un entier rationnel de valeur absolue < 1 est nul. Donc si $u = 0$, $z = m_i k_i$ pour tout i, et par coprimalité des m_i, z est divisible par $m_1...m_n$. La première inégalité entraîne alors $z = 0$, de sorte que tous les k_i sont nuls, et $(z, u, k_1, ..., k_n)$ serait la solution nulle.

4°/ Quitte à en prendre l'opposée, on peut donc supposer que la solution de 2^o/ vérifie $u = 1$. Les dernières inégalités montrent alors que $z - a_i$ est divisible par m_i pour tout i. Il s'agit là de la partie "surjectivité de l'application $\mathbf{Z}/(m_1...m_n) \to \Pi_{i=1,...,n}\mathbf{Z}/(m_i)$ " du lemme chinois.

III 1°/ i) $T^2 - p_1$ est irréductible sur $\mathbb{Q}$ (par exemple par Eisenstein), donc $[\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] = 2$. ii) Si $\sqrt{p_2} = a + b\sqrt{p_1}, a, b \in \mathbb{Q}$, appartenait à $\mathbb{Q}(\sqrt{p_1})$, on aurait $2ab = 0$, d'où $a = 0$

(car $\sqrt{p_2} \notin \mathbb{Q}$), d'où $\sqrt{p_1 p_2} \in \mathbb{Q}$, alors que $T^2 - p_1 p_2$ est irréductible sur $\mathbb{Q}$ (de nouveau par Eisenstein en p_1, puisque $p_1^2 \not| \, p_1 p_2$).

2°/ i) $L/\mathbb{Q}$, extension de décomposition de $(T^2 - p_1)(T^2 - p_2)$, est galoisienne de degré 4, donc $|G| = 4$. ii) G, qui contient au moins deux sous-groupes $Gal(L/\mathbb{Q}(\sqrt{p_i})), i = 1, 2$, d'indice 2, ne peut être le groupe cyclique $\mathbb{Z}/(4)$. C'est donc le groupe de Klein $(\mathbb{Z}/(2)) \times (\mathbb{Z}/(2))$, qui a 3 sous-groupes d'indice 2. iii) En explicitant l'élement $\neq id_L$ de chacun de ces sous-groupes, on voit que les sous-corps M_i de L fixés par ces sous-groupes (autrement dit, G étant abélien : les sous-corps de L quadratiques sur $\mathbb{Q}$) sont $M_1 = \mathbb{Q}(\sqrt{p_1}), M_2 = \mathbb{Q}(\sqrt{p_2})$ et $M_3 = \mathbb{Q}(\sqrt{p_1 p_2}) = \mathbb{Q}(\sqrt{\frac{p_2}{p_1}})$.

3°/ i) Pour $i = 1, 2, 3$, même preuve qu'en 1^o/.ii). ii) Si $\sqrt{p_3}$ appartenait à L, le corps $\mathbb{Q}(\sqrt{p_3})$, qui est quadratique sur $\mathbb{Q}$, serait l'un des corps M_i. Donc $\sqrt{p_3} \notin L$, et $[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}) : \mathbb{Q}] = 8$.