UPMC Master M1 de mathématiques 13-14
D. Bertrand *4M 020 - Théorie des nombres*

Examen du 7 Mai 2014
Durée: 3 heures

L'usage du polycopié du cours et des feuilles d'exercices est autorisé.
Les 3 énoncés sont indépendants. Le barême (sur 20 pts) est indicatif.

I (7 pts)

Soient p un nombre premier impair, et $f(T) \in \mathbf{F}_p[T]$ un polynôme à coefficients dans $\mathbf{F}_p$. On note $N = N(f)$ le nombre de solutions $(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ de l'équation $y^2 = f(x)$, et $\overline{N}$ la classe de N modulo p, vue comme un élément de $\mathbf{F}_p$.

1°/ On suppose ici que $f(T) = aT^2 + bT + c$ est de degré 2.

i) Montrer que l'ensembe $R_1 = \{y^2\,, y \in \mathbf{F}_p\}$ a $\frac{p-1}{2} + 1$ éléments, et que l'ensemble $R_2 = \{f(x)\,, x \in \mathbf{F}_p\}$ a également $\frac{p-1}{2} + 1$ éléments.

ii) En déduire que $N(f) \geq 1$.

2°/ On ne fait plus d'hypothèse sur f.

i) Montrer que $N = \Sigma_{x \in \mathbf{F}_p}((\frac{f(x)}{p}) + 1)$, où $(\frac{-}{p})$ désigne le symbole de Legendre.

ii) En déduire que $\overline{N} = \Sigma_{x \in \mathbf{F}_p} f(x)^{(p-1)/2}$ (égalité dans $\mathbf{F}_p$).

iii) Soit i un entier > 0. Montrer que dans le corps $\mathbf{F}_p$, on a :

$$\Sigma_{x \in \mathbf{F}_p} x^i = -1 \text{ si } p-1 \text{ divise } i \; ; \quad \Sigma_{x \in \mathbf{F}_p} x^i = 0 \text{ si } p-1 \text{ ne divise pas } i.$$

3°/ On suppose ici que f est un polynôme de degré 3, et on note $A \in \mathbf{F}_p$ le coefficient du terme de degré $p-1$ du polynôme $f(T)^{(p-1)/2} = ... + AT^{p-1} + ...$

i) Déduire de 2^o/ que $\overline{N} = -A$.

ii) On suppose que $f(T) = T(T-1)(T-\lambda)$, où $\lambda \in \mathbf{F}_p$, et on pose $m = (p-1)/2$. Montrer que

$$A = (-1)^m \, \Sigma_{j=0,...,m} \binom{m}{j}^2 \lambda^j,$$

où $\binom{m}{j}$ désigne le coefficient binomial C_m^j.

II (6 pts)

1°/ i) Soient p un nombre premier, et ζ une racine primitive p-ième de l'unité dans $\mathbf{C}$. Montrer qu'il n'existe pas d'entier algébrique α tel que $\zeta - 1 = 3\alpha$.

ii) Soit ζ une racine de l'unité dans $\mathbf{C}$. On suppose qu'il existe un entier algébrique α tel que $\zeta - 1 = 3\alpha$. Montrer que $\zeta = 1$.

2°/ Soient n un entier > 0, et X un élément d'ordre fini du groupe multiplicatif $GL_n(\mathbf{Z})$. On suppose qu'il existe une matrice A à coefficients entiers telle que $X - \mathbf{I}_n = 3A$.

i) Montrer que les valeurs propres (complexes) de X sont toutes des racines de l'unité, puis qu'elles sont toutes égales à 1.

ii) Montrer que le polynôme minimal de la matrice X est séparable. En déduire que $X = \mathbf{I}_n$.

3°/ Soit G un sous-groupe fini de $GL_n(\mathbf{Z})$. Montrer que l'ordre $|G|$ de G est $< 3^{n^2}$. (On pourra considérer l'homomorphisme de réduction modulo 3 : $\pi : GL_n(\mathbf{Z}) \to GL_n(\mathbf{Z}/3\mathbf{Z})$.)

III (8 pts)

Soient L le corps de décomposition dans $\mathbf{C}$ du polynôme $P(T) = T^3 + T + 1 \in \mathbf{Q}[T]$, et K le corps $\mathbf{Q}(\sqrt{-31})$.

1°/ Résoudre (pas nécessairement dans l'ordre proposé) les questions suivantes.

a) Montrer que P est irréductible sur $\mathbf{Q}$, qu'il admet une racine réelle α et deux racines complexes conjuguées $\beta, \overline{\beta}$.

b) Calculer le degré de L sur $\mathbf{Q}$.

c) Déterminer le groupe de Galois $G = Gal(L/\mathbf{Q})$ de L sur $\mathbf{Q}$.

d) Montrer que $[(\alpha - \beta)(\alpha - \overline{\beta})(\beta - \overline{\beta})]^2 = -31$.

e) Montrer que G possède 4 sous-groupes propres (c'est-à-dire distincts de G et de $\{id_L\}$), et déterminer les sous-corps de L correspondants. Parmi ceux-ci, lesquels sont galoisiens sur $\mathbf{Q}$?

Pour tout corps de nombres k, on note respectivement $\mathbf{O}_k$, D_k, M_k et h_k l'anneau des entiers de k, son discriminant, la constante de Minkowski de k et le nombre de classes d'idéaux de k.

2°/ a) Déterminer D_K, $\mathbf{O}_K$ et M_K pour le corps quadratique imaginaire K.

b) Montrer que $\mathbf{O}_K$ admet deux idéaux $\mathbf{p}, \mathbf{p}'$ de norme 2, et aucun idéal de norme 3.

c) Montrer que $\mathbf{p}$ et $\mathbf{p}^2$ ne sont pas principaux, et calculer h_K.

d) L'idéal (67) de $\mathbf{O}_K$ est-il premier? (Justifier votre réponse.)

3°/ Soit F le corps $\mathbf{Q}(\alpha)$.

a) Calculer le discriminant de la base $\{1, \alpha, \alpha^2\}$ de F sur $\mathbf{Q}$. En déduire que $\mathbf{O}_F = \mathbf{Z}[\alpha]$.

b) Déterminer D_F et M_F, et montrer que $\mathbf{O}_F$ est un anneau principal.

c) Montrer qu'il existe deux éléments irréductibles et non associés u, v de $\mathbf{O}_F$ tels que $31 = uv^2$. (On pourra noter que 3 est une racine simple de $T^3 + T + 1 \in \mathbf{F}_{31}[T]$.)

d) Montrer que 2 est un élément irréductible de $\mathbf{O}_F$.

Corrigé

I $1^o/$ i) Toute valeur atteinte du polynôme T^2 l'est en deux points $\{y, -y\}$, qui sont distincts si $y \neq 0$ (NB: $p \neq 2$). Il prend donc $1 + (card\mathbf{F}_p - 1)/2$ valeurs distinctes. Toute valeur atteinte du polynôme $f(T)$ l'est en deux points $\{x_1, x_2 = -\frac{b}{a} - x_1\}$, qui sont distincts si $x_1 \neq -\frac{b}{2a}$ (NB: $2a \neq 0$). Il prend donc $1+(card\mathbf{F}_p-1)/2$ valeurs distinctes. - ii) Comme $card(R_1)+card(R_2) > card\mathbf{F}_p$, R_1 et R_2 admettent au moins un point commun, et ce point fournit une solution de $y^2 = f(x)$.

$2^o/$ i) Tout point $x \in \mathbf{F}_p$ tel que $f(x)$ est un carré non nul (resp. nul, resp. n'est pas un carré) fournit deux (resp. une, resp. aucune) solutions de l'équation $y^2 = f(x)$, c'est-à-dire dans chaque cas $(\frac{f(x)}{p}) + 1$ solutions. Leur somme sur tous les x vaut donc N. - ii) La deuxième égalité résulte alors des relations $p = 0$ et $(\frac{a}{p}) = a^{(p-1)/2}$ dans $\mathbf{F}_p$. - iii) Dans le premier cas, $\Sigma_x\, x^i = p-1 = -1$ (NB: $i \neq 0$). Dans le deuxième cas, on choisit un generateur ξ de $\mathbf{F}_p^*$; alors $\xi^i \neq 1, \xi^{i(p-1)} = 1$ et la somme s'ecrit $\Sigma_{k=0,\dots,p-2}\xi^{ik} = (\xi^{i(p-1)}-1)/(\xi^i-1) = 0$. [Autre méthode : comme $i \neq 0$, la somme sur $\mathbf{F}_p$ est égale à la somme sur $G = \mathbf{F}_p^*$. Or $\chi_i : x \mapsto x^i$ est un caractère de G (à valeurs dans le groupe multiplicatif du corps $\mathbf{F}_p$). Dès que ce caractère est non trivial, $\Sigma_{x\in G}\chi_i(x) = 0$.]

$3^o/$ i) Comme $deg(f) = 3$, le seul monôme A_iT^i de degré i non nul et divisible par $p-1$ apparaissant dans le développement de $f(T)^{(p-1)/2}$ est celui de degré $p-1$. D'après $2^o/$, on a donc $\overline{N} = A_0(\Sigma_{x\in\mathbf{F}_p}1)+A\,(\Sigma_x\, x^{p-1}) = pA_0-A = -A$. - ii) Pour un tel f, A est le coefficient du terme de degré m de $(T-1)^m(T-\lambda)^m$, c'est-à-dire $\Sigma_{j=0,\dots,m}\binom{m}{m-j}(-1)^{m-j}\binom{m}{j}(-\lambda)^j = (-1)^m\Sigma_j\binom{m}{j}^2\lambda^j$.

II $1^o/$ i) Le polynomal minimal $\Phi_p(T+1) = (T+1)^p-1)/T$ de $\zeta-1$ a pour terme constant p, donc $N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta-1) = (-1)^{p-1}p$. La norme d'un tel α serait un entier rationnel a, et $N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(3\alpha) = 3^{p-1}a$, donc 3^{p-1} diviserait p. Que p soit ou non égal à 3, c'est impossible. - ii) Soit m l'ordre de ζ. Si $m > 1$, il existe un diviseur m' de m tel que m/m' soit un nombre premier p. Alors, $\zeta' = \zeta^{m'}$ est d'ordre p, et vérifie : $\zeta' - 1 = (\zeta-1)\times$ {un entier algébrique β} $= 3\alpha\beta$. Ceci contredit (i). Donc $m = 1$, et $\zeta = 1$.

$2^o/$ i) Soit m l'ordre de X dans $GL_n(\mathbf{Z})$, de sorte que $X^m = \mathbf{I}_n$, et toute valeur propre ζ de X est une racine m-ième de l'unité. Comme le polynôme caractéristique de la matrice A est à coefficients entiers, ses valeurs propres sont toutes des entiers algébriques α. La relation $X - \mathbf{I}_n = 3A$ entraîne $\zeta - 1 = 3\alpha$, et on déduit de $1/$(ii) que toutes les valeurs propres ζ de X sont égales à 1. - ii) Comme X vérifie la relation $T^m-1 = 0$, son polynôme minimal $P(T)$ divise $T^m - 1$, qui n'a que des racines simples dans $\mathbb{C}$. Donc P est lui aussi séparable. Par conséquent, la matrice X est diagonalisable, donc égale à $\mathbf{I}_n$ d'après le (i).

$3^o/$ L'application π est bien un homomorphisme de groupes. Son noyau H est constitué des matrices X de $GL_n(\mathbf{Z})$ telles que $X - \mathbf{I}_n \in 3Mat_{nn}(\mathbf{Z})$. Comme tout élément X du groupe fini G est d'ordre fini, on déduit de $2/$ que $G \cap H = \{\mathbf{I}_n\}$. Donc G est isomorphe à son image $\pi(G)$, et son ordre $|G|$ divise $|GL_n(\mathbf{F}_3)| < 3^{n^2}$.

III $1^o/$ a) Par le lemme de Gauss, P aurait sinon un facteur de la forme $T\pm1$, or $P(\mp1) \neq 0$. On conclut par un tableau de variations, ou par le fait (cf. cours, III, p. 30; TD VI, exo

13) que le discriminant $D = -4p^3 - 27q^2 = -31$ de $P(T) = T^3 + pT + q$ n'est pas un carré dans $\mathbf{R}$. - b, c) α est de degré 3, et β de degré au plus 2 sur $F = \mathbf{Q}(\alpha)$, donc égal à 2 car $F \subset \mathbf{R}$. Comme $\overline{\beta} = -\alpha - \beta$, $[L : \mathbf{Q}] = 6$. Le groupe de Galois G est d'ordre 6, et s'identifie à un sous-groupe du groupe S_3 des permutations des 3 racines, donc $G = S_3$. - d) Cette expression est le discriminant D de P (cf. cours, V, preuve de la Prop. 2.ii, et TD III, exo 3). - e) Les sous-groupes propres de S_3 sont le groupe alterné A_3, qui est normal dans G, et les sous-groupes d'ordre 2 engendré par les 3 transpositions, qui ne le sont pas. Les corps correspondants sont $K = \mathbf{Q}(\sqrt{D})$, unique sous-corps de L galoisien sur $\mathbf{Q}$ (et $\neq \mathbf{Q}$), et les trois extensions cubiques de $\mathbf{Q}$ engendré par chaque racine de P.

2^o/ a) D'après le cours, VI, §1, $D_K = -31$, $\mathbf{O}_K = \mathbf{Z} \oplus \mathbf{Z}\omega$ avec $\omega = \frac{1+\sqrt{-31}}{2}$, $M_K = \frac{4}{\pi}\frac{2!}{2^2}\sqrt{31} < 4$. - b) $-31 \equiv 1 \bmod 8$, donc (VI, Prop. 1.ii) 2 est décomposé dans K, i.e. il existe deux idéaux premiers distincts $\mathbf{p}, \mathbf{p}'$ de produit (2). - b) Tout idéal contient sa norme (V, Prop. 5.iii). Or $(\frac{-31}{3}) = (\frac{-1}{3}) = -1$, donc 3 est inerte, donc le seul idéal premier contenant 3 est (3), qui a pour norme 9. - c) Si $\mathbf{p}$, de norme 2, était principal, il aurait un générateur de norme 2. Or l'équation $N_{K/\mathbf{Q}}(x + y\omega) = x^2 + xy + 8y^2 = 2$ n'a pas de solutions en entiers rationnels x, y (car $xy \geq -\frac{1}{2}(x^2 + y^2)$). De même, supposons $\mathbf{p}^2$ principal. Comme les seules solutions de l'équation $x^2 + xy + 8y^2 = 4$ sont $x = \pm 2, y = 0$, $\mathbf{p}^2$ serait l'idéal (2), qui vaut $\mathbf{p}\mathbf{p}'$, d'où $\mathbf{p} = \mathbf{p}'$, contradiction. Enfin, d'après V, thm. 3, tout élément du groupe des classes Cl_K est représentable par un idéal de $\mathbf{O}_K$ de norme $\leq M_K$, donc ≤ 3, donc par (1), $\mathbf{p}$ ou $\mathbf{p}'$, et l'ordre h_K de Cl_K est ≤ 3. On vient de voir que la classe de $\mathbf{p}$ est d'ordre ≥ 3, donc $h_K = 3$. (On peut aussi dire que $\mathbf{p}$ n'est pas principal, et que d'après VI, Thm. 1, h_K n'est pas divisible par 2.) - d) D'après la loi de réciprocité quadratique, $(\frac{-31}{67}) = (\frac{-1}{67})(\frac{31}{67}) = (-1)^{33}(\frac{67}{31})(-1)^{15.33} = (\frac{5}{31}) = (\frac{31}{5})(-1)^{15.2} = 1$, donc 67 est décomposé, et (67) n'est pas un idéal premier de $\mathbf{O}_K$. (Cela découle aussi de la relation $67 = 6^2 + 31$, qui montre en plus que les idéaux premiers divisant 67 sont principaux.)

3^o/ a) Ce discriminant vaut celui de P (V, Prop. 2.ii), c.-à -d. -31, qui est sans facteur carré dans $\mathbf{Z}$, et on déduit de V, Prop. 2.iii, que $\mathbf{Z} \oplus \mathbf{Z}\alpha \oplus \mathbf{Z}\alpha^2 = \mathbf{O}_F$. Le discriminant D_F de F vaut donc -31. - b) $M_F = \frac{3!}{3^3}\sqrt{31} < 2$. D'où $h_F = 1$ par V, thm. 5. - c) D'après b), l'anneau $\mathbf{O}_F$ vérifie les hypothèses de V, Prop. 7. La décomposition de (31) est donc régie par celle de $P(T)$ modulo 31. Or $T^3 + T + 1 = (T - 3)(T - 14)^2$ dans $\mathbf{F}_{31}[T]$ (ses racines sont de somme nulle, et on sait qu'il a une racine au moins double), donc il existe deux idéaux premiers distincts $\mathbf{p}_1, \mathbf{p}_2$ de $\mathbf{O}_F$ tels que $(31) = \mathbf{p}_1\mathbf{p}_2^2$. Comme $\mathbf{O}_F$ est principal, on en déduit qu'il existe deux élements u et v de $\mathbf{O}_F$ irréductibles et non associés (cf. cours I, p. 11), et une unité ϵ de $\mathbf{O}_F$ tels que $31 = \epsilon u v^2$; on conclut en remplaçant u par ϵu. - d) Le polynôme $T^3 + T + 1 \in \mathbf{F}_2[T]$ étant irréductible, V. Prop. 7 entraîne que (2) est un idéal premier de $\mathbf{O}_F$, donc 2 est irréductible dans l'anneau $\mathbf{O}_F$.