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

Examen du 13 Mai 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

Soient p un nombre premier, $\boldsymbol{\mu}_p$ le groupe des racines p-ièmes de l'unité dans $\mathbf{C}$, K un sous-corps de $\mathbf{C}$ contenant $\boldsymbol{\mu}_p$, et L une extension galoisienne finie de K. On suppose qu'il existe un homomorphisme *surjectif* χ du groupe $G = Gal(L/K)$ sur le groupe $\boldsymbol{\mu}_p$.

1°/ Montrer que L contient une extension galoisienne M de K, de degré $[M : K] = p$.

2°/ À tout élément x de L, on associe l'élement $y = y(x)$ de L défini par $y = \Sigma_{\sigma\in G}\, \chi(\sigma)\, \sigma(x)$.
i) Montrer que pour tout élément τ de G, on a: $\tau(y) = \chi(\tau)^{-1}y$.
ii) On suppose que $y \neq 0$. Calculer le degré de y sur K, et le degré de y^p sur K.

3°/ Soit n l'ordre du groupe G.
i) Montrer qu'il existe un élément x de L de degré n sur K.
ii) Montrer que l'un des nombres $y(1)$, $y(x), ..., y(x^{n-1})$ est non nul.

4°/ Précisez l'énoncé du 1^o/ en montrant que L contient un extension galoisienne M de K de degré p, de la forme $M = K(\sqrt[p]{z})$, où z appartient à K.

II

On se propose de montrer par l'absurde que l'équation

$$(E) \qquad x^4 = 2y^2 + 17z^4$$

n'a pas de solution en entiers rationnels (x, y, z) non tous nuls. Soit donc (x, y, z) une telle solution.

1°/ Montrer qu'on peut, sans perte de généralité, supposer x et y premiers entre eux.

2°/ Vérifier que $(\frac{2}{17}) = 1$, et trouver les racines carrées $\{u, -u\}$ de 2 modulo 17.

3°/ i) Calculer $(\frac{u}{17})$ et $(\frac{-u}{17})$.
ii) En déduire que y n'est pas un carré modulo 17.

4°/ i) Soit p un nombre premier divisant y. Montrer que 17 est un carré modulo p. Que peut-on alors dire de $(\frac{p}{17})$?
ii) Conclure.

TSVP

III

Soient K le corps $\mathbf{Q}(\sqrt{-26})$, $\mathbf{O}$ son anneau d'entiers, et D son discriminant.

1°/ Donner une base de $\mathbf{O}$ sur $\mathbf{Z}$. Calculer D, et vérifier que la constante de Minskowski M_K de K est < 7.

2°/ Montrer qu'il existe un unique idéal premier $\mathbf{p}$ de $\mathbf{O}$ de norme 2, et que $\mathbf{p}$ n'est pas principal. Calculer l'ordre de $\mathbf{p}$ dans le groupe des classes $C\ell_K$ de K.

3°/ i) Montrer qu'il existe deux idéaux premiers $\mathbf{q}$, $\mathbf{q}'$ de norme 3, et qu'ils ne sont pas principaux.

ii) Montrer que $\mathbf{q}^3$ est principal, et calculer l'ordre de $\mathbf{q}$ dans $C\ell_K$.

4°/ Déterminer combien $\mathbf{O}$ admet d'idéaux de norme ≤ 6.

5°/ Déterminer le nombre de classes h_K de K et la structure du groupe $C\ell_K$.

IV

À toute suite de nombres complexes $\mathbf{u} = \{u(n), n \geq 1\}$, on associe la série de Dirichlet $\zeta_{\mathbf{u}}(s) = \Sigma_{n\geq 1} \frac{u(n)}{n^s}$.

1°/ On suppose que la suite $\mathbf{u}$ est à croissance au plus polynômiale, c-à-d. qu'il existe deux nombres réels $c, \gamma > 0$ telles que $|u(n)| \leq cn^\gamma$ pour tout $n \geq 1$. Montrer que la série de Dirichlet $\zeta_{\mathbf{u}}(s)$ converge pour tout nombre complexe s tel que $Re(s) > \gamma + 1$.

Dans la suite du problème, toutes les suites sont à croissance au plus polynômiale. On ne demande pas de le vérifier, et on s'autorisera à traiter les séries de Dirichlet de façon formelle, sans préciser leur domaine de convergence ni le domaine de validité des identités étudiées.

2°/ Soient $\mathbf{u} = \{u(n)\}, \mathbf{v} = \{v(n)\}$ deux suites, et $\zeta_{\mathbf{u}}(s), \zeta_{\mathbf{v}}(s)$ les séries de Dirichlet associées. Pour tout $n \geq 1$, on pose $w(n) = \Sigma_{d|n} u(d)v(\frac{n}{d})$. Montrer que la suite $\mathbf{w} = \{w(n), n \geq 1\}$ vérifie : $\zeta_{\mathbf{u}}(s)\zeta_{\mathbf{v}}(s) = \zeta_{\mathbf{w}}(s)$.

3°/ Soient μ la fonction de Möbius et ζ la fonction zeta de Riemann. Établir la relation : $\Sigma_{n\geq 1} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$.

4°/ Soit ϕ la fonction indicatrice d'Euler. Établir la relation : $\Sigma_{n\geq 1} \frac{\phi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$.

5°/ (Question facultative) Pour tout $n \geq 1$, on note ν_n le nombre d'idéaux de l'anneau $\mathbb{Z}[i]$ de norme n. On note par ailleurs $\chi : \mathbb{Z} \to \{-1, 0, 1\}$ la fonction définie par $\chi(d) = \pm 1$ si $d \equiv \pm 1$ mod. 4, et $\chi(d) = 0$ si d est pair. On se propose de montrer que pour tout $n \geq 1$, on a : $\nu_n = \Sigma_{d|n}\chi(d)$.

i) Vérifier la formule quand $n = p$ est un nombre premier.

ii) Montrer que $\Sigma_{n\geq 1} \frac{\chi(n)}{n^s} = \Pi_{p\in\mathcal{P}} \frac{1}{1-\chi(p)/p^s}$, où $\mathcal{P}$ désigne l'ensemble de tous les nombres premiers.

iii) Montrer que $\Sigma_{n\geq 1} \frac{\nu_n}{n^s} = \Pi_{\wp\in\mathfrak{P}} \frac{1}{1-1/N(\wp)^s}$, où $\mathfrak{P}$ désigne l'ensemble de tous les idéaux premiers $\wp$ de $\mathbb{Z}[i]$.

iv) Montrer que $\Sigma_{n\geq 1} \frac{\nu_n}{n^s} = \zeta(s)\Pi_{p\in\mathcal{P}} \frac{1}{1-\chi(p)/p^s}$, et conclure.

Corrigé

I.1/ Le noyau H de χ est un sous-groupe normal de G d'indice $|\mu_p| = p$, donc l'extension intermédiaire $M := L^H$ est galoisienne sur K, et de degré $|G/H| = p$.

2/ i) Comme $\tau \in Gal(L/K)$ fixe les éléments de $\mu_p \subset K$, $\tau(y) = \Sigma_{\sigma\in G}\ \chi(\sigma)\ \tau(\sigma(x))$, qui vaut $\chi(\tau)^{-1}\Sigma_{\sigma\in G}\ \chi(\tau\sigma)\ \tau\sigma(x) = \chi(\tau)^{-1}y$. - ii) Le degré de y sur K est égal au nombre de ses conjugués distincts, donc L/K étant galoisienne, au cardinal de l'ensemble $\{\tau(y), \tau \in G\}$. Comme χ est surjective, et $y \neq 0$, il y en a p, donc $[K(y) : K] = p$. Par ailleurs, $\tau(y^p) = \chi(\tau)^{-p}y^p = y^p$ pour tout $\tau \in G$, donc $y^p \in L^G = K$.

3/ i) Comme $n = |G| = [L : K]$, il suffit d'invoquer le théorème de l'élément primitif. - ii) Si tous étaient nuls, le système de n équations à n inconnues : $\Sigma_{\sigma\in G}\sigma(x^i)t_\sigma = 0; i = 0, ..., n-1$, aurait une solution $(t_\sigma = \chi(\sigma); \sigma \in G)$ non triviale. Or son déterminant est un Van der Monde non nul (égal au discriminant de la base $\{1, x, ..., x^{n-1}\}$ de L sur K).

4/ Pour i tel que $y' := y(x^i)$ soit non nul, posons $z = y'^p$. D'après 2/, $z \in K$ et y' engendre une extension de degré p de K. Comme $Min_{y',K}(T)$ divise $T^p - z$, il lui est donc égal, $T^p - z$ est irréductible sur K et $K(y') = K[T]/(T^p - z)$. Comme $\mu_p \in K$, ce polynôme se décompose en facteurs linéaires dans $K(y') = K(\sqrt[p]{z})$, qui est donc bien un extension galoisienne M de K, de degré p.

II.1/ Soit p un nombre premier divisant x et y. Alors p^2 divise $x^4 - 2y^2 = 17z^4$, donc p divise z (même si $p = 17$), donc p^4 divise $x^4 - 17z^4 = 2y^2$, donc p^2 divise y (même si $p = 2$). Ainsi, (E) admet la solution "plus petite" $(\frac{x}{p}, \frac{y}{p^2}, \frac{z}{p})$. En itérant, on aboutit à une solution (x', y', z') où x' et y' n'ont pas de diviseur commun autre que 1.

2/ i) Comme $(17^2 - 1)/8 = 16 \times 18/8$ est pair, $(\frac{2}{17}) = 1$. - ii) Comme $6^2 \equiv 2$ mod. 17, les racines de 2 sont $\pm u = \pm 6$ mod. 17.

3/ i) $(\frac{u}{17}) = (\frac{2}{17}) \times (\frac{3}{17}) = 1 \times (\frac{17}{3})(-1)^{2.16/4} = (\frac{17}{3}) = (\frac{2}{3}) = -1$. Donc $(\frac{-u}{17}) = (\frac{-1}{17})(\frac{u}{17}) = (-1)^{16/2} \times (-1) = -1$. - ii) y n'est pas divisible par 17, sans quoi 17 diviserait x^4, donc aussi x. Soit y' tel que $yy' \equiv 1$ mod. 17. De (E), on tire $2 \equiv x^4y'^2$ mod. 17. Si y était un carré mod. 17, y' le serait aussi, et 2 serait une puissance 4-ième mod. 17. Mais alors, l'une au moins de ses racines carrées $u, -u$ serait un carré mod. 17, ce qui contredit le i).

4/ i) Le diviseur premier p de y ne peut pas diviser z, sans quoi il diviserait aussi x^4, donc x. De (E) modulo p, on tire que 17 est une puissance 4-ième, donc aussi un carré modulo p. Pour p impair, on a donc $(\frac{17}{p}) = 1$ et comme $(17 - 1)/4$ est pair, la LRQ donne $(\frac{p}{17}) = (\frac{17}{p}) = 1$. Quant à $p = 2$, on a vu que $(\frac{2}{17}) = 1$. -ii) Ainsi, tout diviseur premier de y est un carré modulo 17. Donc y est aussi un carré modulo 17. Joint à la conclusion de 3/ii), cela donne la contradiction recherchée.

III.1/ $-26 \equiv 2$ mod 4. Donc $\mathbf{O}$ admet $\{1, \sqrt{-26}\}$ comme base sur $\mathbf{Z}$, $D = -104$, et $M_K = \frac{4}{\pi}\frac{2!}{2^2}\sqrt{4 \times 26} = \frac{4}{\pi} \times 5 \times (1 + \frac{1}{25})^{\frac{1}{2}} < \frac{20}{\pi}(1 + \frac{1}{50}) < \frac{21}{\pi} < 7$.

2/ Les idéaux de norme 2 (qui sont automatiquement premiers) divisent (2). Comme -26 est pair, 2 est ramifié dans K (cf. cours, chap. VI, prop. 1). Il existe donc un unique idéal premier $\mathbf{p}$ divisant (2), avec $(2) = \mathbf{p}^2$. En particulier, $N(\mathbf{p}) = 2$ et $\mathbf{p}$ est le seul idéal

de norme 2. Si $\mathbf{p} = (a + b\sqrt{-26})$ était principal, les entiers rationnels a, b vérifieraient $a^2 + 26b^2 = 2$, impossible. Comme $\mathbf{p}^2$ est principal, la classe de $\mathbf{p}$ dans $C\ell_K$ est d'ordre 2.

3/ i) De $(\frac{-26}{3}) = (\frac{1}{3}) = 1$, on déduit que 3 est décomposé: il existe deux idéaux premiers $\mathbf{q}, \mathbf{q}'$ distincts tels que $(3) = \mathbf{q}\mathbf{q}'$. Alors, $\mathbf{q}$ et $\mathbf{q}'$ sont les seuls idéaux de norme 3. L'équation diophantienne $a^2 + 26b^2 = 3$ n'ayant pas de solution, ils ne sont pas principaux. - ii) Les idéaux de norme 27 divisent $\mathbf{q}^3\mathbf{q}'^3$. Ce sont donc $\mathbf{q}^2\mathbf{q}' = 3\mathbf{q}, \mathbf{q}\mathbf{q}'^2 = 3\mathbf{q}'$, qui ne sont pas principaux, et $\mathbf{q}^3, \mathbf{q}'^3$. Or les idéaux principaux engendrés par les éléments (non associés) $1 \pm \sqrt{-26}$ de $\mathbf{O}$ sont de normes 27. Ils coïncident donc avec les idéaux $\mathbf{q}^3, \mathbf{q}'^3$, et ces derniers sont bien principaux. L'ordre de $\mathbf{q}$ dans $C\ell_K$ divise donc 3, et vaut exactement 3.

4/ $\mathbf{O}$ est le seul idéal de norme 1; $\mathbf{p}$ de norme 2; $\mathbf{q}$ et $\mathbf{q}'$ de norme 3. Donc les seuls idéaux de norme 4 (resp. 6) sont $\mathbf{p}^2 = (2)$ (resp. $\mathbf{p}\mathbf{q}, \mathbf{p}\mathbf{q}'$). De $(\frac{-26}{5}) = (\frac{4}{5}) = 1$, on déduit que 5 est décomposé, et il existe deux idéaux premiers $\mathbf{r}, \mathbf{r}'$ distincts de norme 5. Il y a donc en tout 9 idéaux de norme ≤ 6.

5/ Le groupe abélien $C\ell_K$ contient un élément d'ordre 2 et un élément d'ordre 3, donc admet un sous-groupe cyclique d'ordre 6. La constante de Minskowski étant < 7, tous les éléments de $C\ell_K$ sont représentés par les classes des idéaux $1 \sim \mathbf{p}^2, \mathbf{p}, \mathbf{q}, \mathbf{q}', \mathbf{p}\mathbf{q}, \mathbf{p}\mathbf{q}', \mathbf{r}, \mathbf{r}'$. Donc $h_K \leq 8$. Comme h_K est divisible par 6, il vaut 6 et $C\ell_K$ est un groupe cyclique d'ordre 6, engendré par exemple par la classe de $\mathbf{p}\mathbf{q}$ (ou celle de $\mathbf{r}$, d'ordre $\neq 1, 2, 3$).

IV.1/ $|u(n)/n^s| = |u(n)|/n^\sigma \leq c/n^{\sigma-\gamma}$. La série converge donc absolument pour $\sigma - \gamma > 1$.

2/ Le produit $\zeta_{\mathbf{u}}(s)\zeta_{\mathbf{v}}(s) = \big(\Sigma_{\ell\geq 1}\frac{u(\ell)}{\ell^s}\big)\big(\Sigma_{m\geq 1}\frac{v(m)}{ms}\big)$ est formellement donné par la série double $\Sigma_{\ell,m\geq 1}u(\ell)v(m)/(\ell m)^s$, qui après regroupement des termes tels que $\ell m = n$ s'écrit $\Sigma_{n\geq 1}\big(\Sigma_{\ell,m\geq 1,\ell m=n}u(\ell)v(m)\big)/n^s = \Sigma_{n\geq 1}\frac{w(n)}{n^s}$, où $w(n) = \Sigma_{\ell,m\geq 1,\ell m=n}u(\ell)v(m) = \Sigma_{d|n}u(d)v(\frac{n}{d})$. [La formule vaut pour $\sigma > sup(\gamma_{\mathbf{u}}, \gamma_{\mathbf{v}}) + 1$, où la série double est absolument sommable.]

3/ Soient $\mathbf{1}$ la suite $\mathbf{1}(n) = 1$, et $\boldsymbol{\mu}$ la suite $\mu(n)$. Alors $\zeta_{\mathbf{1}}(s)\zeta_{\boldsymbol{\mu}}(s) = \zeta_{\mathbf{w}}(s)$, où $w(n) = \Sigma_{d|n}\mu(d)\mathbf{1}(\frac{n}{d})$, qui, d'après le poly, Chap. I, vaut 1 si $n = 1$, et 0 sinon. Donc $\zeta(s) \times \Sigma_{n\geq 1}\frac{\mu(n)}{n^s} = 1$. [Cela vaut dès que $\sigma > 1$, et on peut alors diviser par $\zeta(s)$, qui y est $\neq 0$.]

4/ Soit $\boldsymbol{\phi}$ la suite $\phi(n)$. Alors, $\zeta_{\mathbf{1}}(s)\zeta_{\boldsymbol{\phi}}(s) = \zeta_{\mathbf{w}}(s)$, où $w(n) = \Sigma_{d|n}\phi(d)\mathbf{1}(\frac{n}{d}) = n$ (poly, Chap. I), donc $\zeta(s) \times \Sigma_{n\geq 1}\frac{\phi(n)}{n^s} = \Sigma_{n\geq 1}\frac{n}{n^s} = \zeta(s-1)$. [Cela vaut dès que $\sigma > 2$.]

5/ i) $p = 2$ est ramifié dans $\mathbb{Q}(i)$, donc il y a exactement un idéal de norme 2, et $\chi(1) + \chi(2) = 1 + 0 = 1$ est bien égal à ν_2. Un $p \equiv 1$ mod. 4 est décomposé, donc $\nu_p = 2$, bien égal à $\chi(1) + \chi(p)$. Un $p \equiv 3$ mod. 4 est inerte, donc $\nu_p = 0$, égal à $\chi(1) + \chi(p)$. - ii) La fonction χ est strictement multiplicative. On applique le Lemme 2.ii du chap. VII du poly. (En fait, χ est un caractère de Dirichlet mod. 4, et $\zeta_{\boldsymbol{\chi}}(s) := \Sigma_{n\geq 1}\frac{\chi(n)}{n^s} = L(s, \chi)$.) - iii) $Z(s) := \Pi_{\wp\in\mathfrak{P}}\frac{1}{1-1/N(\wp)^s} = \Pi_{\wp\in\mathfrak{P}}(\Sigma_{k\geq 0}N(\wp)^{-ks})$. En développant le produit, on déduit de la multiplicativité de la norme que $Z(s) = \Sigma_{\mathfrak{A}}N(\mathfrak{A})^{-s}$, où $\mathfrak{A}$ parcourt l'ensemble de tous les idéaux non nuls de $\mathbb{Z}[i]$, car chacun s'écrit de façon unique comme produit de puissances d'idéaux premiers. En regroupant les idéaux $\mathfrak{A}$ de norme n, on en déduit que $Z(s) = \Sigma_{n\geq 1}\frac{\nu_n}{n^s}$. - iv) $\Pi_{\wp\in\mathfrak{P}}\frac{1}{1-1/N(\wp)^s} = \Pi_{p\equiv 1(4)}\frac{1}{(1-1/p^s)^2} \times \Pi_{p\equiv 3(4)}\frac{1}{1-1/p^{2s}} \times \Pi_{p=2}\frac{1}{1-1/p^s} = \Pi_{p\equiv 1(4)}\frac{1}{(1-1/p^s)^2} \times \Pi_{p\equiv 3(4)}\frac{1}{(1-1/p^s)(1+1/p^s)} \times \Pi_{p=2}\frac{1}{1-1/p^s} = \Pi_{p\in\mathcal{P}}\frac{1}{1-1/p^s} \times \Pi_{p\in\mathcal{P}}\frac{1}{1-\chi(p)/p^s}$, donc $\zeta_{\boldsymbol{\nu}}(s) = Z(s) = \zeta_{\mathbf{1}}(s) \times \zeta_{\boldsymbol{\chi}}(s)$, et la suite $\boldsymbol{\nu}$ vérifie bien $\nu(n) = \Sigma_{d|n}\chi(d)$.