

Correction de l'examen

1.

- a) **(2 points)** Soit $\varepsilon > 0$. Puisque la série $\sum_{n \geq 1} \frac{|b(n)|}{n}$ converge, il existe $N_1 \geq 1$ tel que, pour tout $N \geq N_1$, $\sum_{n > N} \frac{|b(n)|}{n} < \frac{\varepsilon}{2}$. Pour $N > N_1$, découpons notre somme en deux morceaux :

$$\begin{aligned} \frac{1}{N} \sum_{n=1}^N |b(n)| &= \frac{1}{N} \sum_{n=1}^{N_1} |b(n)| + \frac{1}{N} \sum_{n=N_1+1}^N |b(n)| \\ &\leq \frac{1}{N} \sum_{n=1}^{N_1} |b(n)| + \sum_{n=N_1+1}^N \frac{|b(n)|}{n} \\ &\leq \frac{1}{N} \sum_{n=1}^{N_1} |b(n)| + \sum_{n > N_1} \frac{|b(n)|}{n} \\ &< \frac{1}{N} \sum_{n=1}^{N_1} |b(n)| + \frac{\varepsilon}{2} \end{aligned}$$

Si on choisit $N \geq \max(N_1, N_2)$, où $N_2 = \left\lceil \frac{2}{\varepsilon} \sum_{n=1}^{N_1} |b(n)| \right\rceil$ alors on obtient l'inégalité $\frac{1}{N} \sum_{n=1}^N |b(n)| < \varepsilon$. On a donc prouvé que $\frac{1}{N} \sum_{n=1}^N |b(n)|$ converge vers 0 lorsque N tend vers ∞ .

Par définition de $c(n) : \frac{1}{N} \sum_{n=1}^N c(n) = \frac{1}{N} \sum_{n=1}^N \sum_{1 \leq d|n} b(d)$. En échangeant les deux sommes, on a $\frac{1}{N} \sum_{n=1}^N c(n) = \frac{1}{N} \sum_{d=1}^N \sum_{n=1, d|n}^N b(d)$. Or le nombre de multiples de d compris entre 1 et N est $\left\lfloor \frac{N}{d} \right\rfloor$ donc $\frac{1}{N} \sum_{n=1}^N c(n) = \frac{1}{N} \sum_{d=1}^N \left\lfloor \frac{N}{d} \right\rfloor b(d)$. La différence $\sum_{n=1}^N \frac{b(n)}{n} - \frac{1}{N} \sum_{n=1}^N c(n) = \frac{1}{N} \sum_{n=1}^N \left(\frac{N}{n} - \left\lfloor \frac{N}{n} \right\rfloor \right) b(n)$ converge vers 0 car $\frac{1}{N} \sum_{n=1}^N \left(\frac{N}{n} - \left\lfloor \frac{N}{n} \right\rfloor \right) |b(n)| < \frac{1}{N} \sum_{n=1}^N |b(n)|$. L'hypothèse selon laquelle $\sum_{n \geq 1} \frac{b(n)}{n}$ converge montre donc que $\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N c(n) = \lim_{N \rightarrow \infty} \sum_{n=1}^N \frac{b(n)}{n}$.

- b) **(2 points)** Soit $s \in \mathbb{C}$ tel que $\operatorname{Re}(s) > 1$. On a $\sum_{n=1}^N \left| \frac{b(n)}{n^s} \right| \leq \sum_{n=1}^N \left| \frac{b(n)}{n} \right|$ car $|n^s| = n^{\operatorname{Re}(s)} > n$, si bien que $\sum_{n \geq 1} \frac{b(n)}{n^s}$ converge absolument, d'après l'hypothèse sur $(b(n))$.

Puisque les séries $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$ et $\sum_{n \geq 1} \frac{b(n)}{n^s}$ convergent absolument, la série produit $\sum_{n \geq 1} \left(\sum_{n_1 n_2 = n} \frac{1}{n_1^s} \frac{b(n_2)}{n_2^s} \right) = \sum_{n \geq 1} \frac{c(n)}{n^s}$ converge absolument vers le produit : $\zeta(s) \sum_{n \geq 1} \frac{b(n)}{n^s} = \sum_{n \geq 1} \frac{c(n)}{n^s}$.

- c) **(2 points)** Si l'on ne se soucie pas des problèmes de convergences, le développement formel du produit infini $\zeta(2s)^{-1} = \prod_p (1 - p^{-2s})$ donne $\sum_{n \geq 1} \frac{b(n)}{n^s}$ avec $b(n) = (-1)^r$ si $n = \prod_{i=1}^r p_i^2$ est le carré d'un entier sans facteur carré (i.e. les p_i sont deux à deux distincts) et $b(n) = 0$ sinon.

Si l'on prend cette définition de $b(n)$, on a, en posant $n = m^2$, $\sum_{n \geq 1} \left| \frac{b(n)}{n^s} \right| = \sum_{m \geq 1} \frac{1}{m^{2\operatorname{Re}(s)}}$ où la somme $\sum_{m \geq 1}'$ porte sur les entiers $m \geq 1$ sans facteur carré. L'inégalité $\sum_{n \geq 1} \left| \frac{b(n)}{n^s} \right| = \sum_{m \geq 1}' \frac{1}{m^{2\operatorname{Re}(s)}} < \sum_{m \geq 1} \frac{1}{m^{2\operatorname{Re}(s)}} = \zeta(2\operatorname{Re}(s))$ montre la convergence absolue de la série $\sum_{n \geq 1} \frac{b(n)}{n^s}$ pour $\operatorname{Re}(s) > \frac{1}{2}$.

- d) **(2 points)** Pour $\operatorname{Re}(s) > 1$, la majoration $\sum_{n \in A} \left| \frac{1}{n^s} \right| = \sum_{n \in A} \frac{1}{n^{\operatorname{Re}(s)}} \leq \sum_{n \in A} \frac{1}{n^{\operatorname{Re}(s)}} = \zeta(\operatorname{Re}(s))$ montre que la série de Dirichlet $\sum_{n \in A} \frac{1}{n^s}$ est absolument convergente.

Dans l'expression de la fonction ζ de Riemann sous forme de produit de Dirichlet $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p (1 + p^{-s} + p^{-2s} + \dots) = \prod_p \frac{1}{1 - p^{-s}}$, il est clair que si l'on tronque les séries $1 + p^{-s} + p^{-2s} + \dots$ pour ne garder que les deux premiers termes $1 + p^{-s}$, cela revient, côté série de Dirichlet à restreindre la somme aux $n \in A$: $\sum_{n \in A} \frac{1}{n^s} = \prod_p (1 + p^{-s})$.

- e) **(2 points)** Reprenons le résultat de la question précédente pour le pousser plus loin : $\sum_{n \in A} \frac{1}{n^s} = \prod_p (1 + p^{-s}) = \prod_p \frac{1 - p^{-2s}}{1 - p^{-s}} = \left(\prod_p \frac{1}{1 - p^{-s}} \right) \left(\prod_p (1 - p^{-2s}) \right) = \zeta(s) \zeta(2s)^{-1}$. En utilisant les résultats de c) et b), on a donc $\sum_{n \in A} \frac{1}{n^s} = \zeta(s) \sum_{n \geq 1} \frac{b(n)}{n^s} = \sum_{n \geq 1} \frac{c(n)}{n^s}$. On en déduit donc, par unicité des coefficients d'une série de Dirichlet, $c(n) = 1$.
Maintenant, en utilisant la deuxième relation obtenue en a), il vient : $\lim_{N \rightarrow \infty} \frac{1}{N} \text{Card} \{n \in A : n \leq N\} = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N c(n) = \lim_{N \rightarrow \infty} \sum_{n=1}^N \frac{b(n)}{n} = \zeta(2)^{-1}$.

2.

- a) **(2 points)** Puisque E est un corps fini, on sait que son groupe des éléments inversibles $E^\times$ est un groupe cyclique. Soit $x \in E^\times$ un générateur de ce groupe.
Par finitude de E toujours, donc de $E^\times$, x est d'ordre fini, ce qui signifie exactement que x est une racine de l'unité.
Par ailleurs, l'extension $F[x]$ de F engendrée par x contient, par définition, l'élément nul 0, l'élément x et toutes ses puissances, c'est-à-dire 0 et $E^\times$. D'où $F[x] = E$ et E est l'extension cyclotomique engendrée par la racine de l'unité x .
- b) **(1 point)** Considérons la racine 8^e de l'unité $\zeta_8 = e^{\frac{i\pi}{4}} \in \mathbb{C}$.
L'égalité $\zeta_8 = \frac{1}{2}(\sqrt{2} + i\sqrt{2})$ montre que $\mathbb{Q}[\zeta_8] \subset \mathbb{Q}[\sqrt{2}, \sqrt{-2}]$. Les égalités $\sqrt{2} = \zeta_8 + (\zeta_8)^{-1}$, $i\sqrt{2} = \zeta_8 - (\zeta_8)^{-1}$ montrent l'inclusion inverse : $\mathbb{Q}[\sqrt{2}, \sqrt{-2}] \subset \mathbb{Q}[\zeta_8]$. Par conséquent, $\mathbb{Q}[\sqrt{2}, \sqrt{-2}]$ est l'extension cyclotomique engendrée par la racine 8^e de l'unité ζ_8 .
- c) **(3 points)** Considérons la racine p^e de l'unité $\zeta_p = e^{\frac{2i\pi}{p}} \in \mathbb{C}$ et la somme de Gauss $\tau = \sum_{x \in \mathbb{F}_p^\times} \left(\frac{x}{p} \right) (\zeta_p)^x$ (qui s'exprime aussi sous la forme $\tau = \sum_{x \in \mathbb{F}_p} (\zeta_p)^{x^2}$).
Par définition de τ , on a $\mathbb{Q}[\tau] \subset \mathbb{Q}[\zeta_p]$.
Selon le cours, τ vérifie la relation $\tau^2 = \left(\frac{-1}{p} \right) p$. Quelque soit la valeur de $\left(\frac{-1}{p} \right)$, on a donc $\tau \in \{ \pm \sqrt{p}, \pm i\sqrt{p} \}$, c'est-à-dire $\{ \pm \sqrt{p}, \pm i\sqrt{p} \} = \{ \pm \tau, \pm i\tau \}$. En termes d'extensions, on obtient $\mathbb{Q}[\sqrt{p}, \sqrt{-p}] = \mathbb{Q}[\sqrt{p}, i\sqrt{p}] = \mathbb{Q}[\tau, i\tau] = \mathbb{Q}[i, \tau] \subset \mathbb{Q}[i, \zeta_p]$.
La racine 4^e p^e de l'unité $\zeta_{4p} = e^{\frac{i\pi}{2p}} \in \mathbb{C}$ vérifie $(\zeta_{4p})^p = i$ et $(\zeta_{4p})^4 = \zeta_p$, donc $\mathbb{Q}[i, \zeta_p] \subset \mathbb{Q}[\zeta_{4p}]$.
Finalement, on a montré que $\mathbb{Q}[\sqrt{p}, \sqrt{-p}]$ est incluse dans l'extension cyclotomique $\mathbb{Q}[\zeta_{4p}]$ engendrée par la racine 4^e p^e de l'unité ζ_{4p} .
- d) **(2 points)** Soit K une extension quadratique de $\mathbb{Q}$. On sait que K est de la forme $\mathbb{Q}[\sqrt{d}]$ avec $d \in \mathbb{Z} \setminus \{ \pm 1, 0 \}$ sans facteur carré.
Écrivons $d = (-1)^\varepsilon \prod_{i=1}^r p_i$ la décomposition de d en produit de nombres premiers : $\varepsilon \in \{0, 1\}$, $r \geq 1$ et les p_i sont des nombres premiers 2 à 2 distincts. On a $(i^\varepsilon \prod_{i=1}^r \sqrt{p_i})^2 = d$ donc $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[i, \sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_r}]$.
D'après les deux questions précédentes, on a $\mathbb{Q}[\sqrt{p_i}] \subset \mathbb{Q}[\zeta_{4p_i}]$, si bien que $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[i, \sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_r}] \subset \mathbb{Q}[i, \zeta_{4p_1}, \zeta_{4p_2}, \dots, \zeta_{4p_r}]$. En posant $\zeta_{4d} = e^{\frac{i\pi}{2d}}$, les égalités $(\zeta_{4d})^d = i$ et $(\zeta_{4d})^{p_1 p_2 \dots p_k - 1 p_{k+1} \dots p_r} = \zeta_{4p_k}$ montrent que $\mathbb{Q}[i, \zeta_{4p_1}, \zeta_{4p_2}, \dots, \zeta_{4p_r}] \subset \mathbb{Q}[\zeta_{4d}]$.
Par conséquent, l'extension quadratique $\mathbb{Q}[\sqrt{d}]$ est incluse dans l'extension cyclotomique $\mathbb{Q}[\zeta_{4d}]$.

3.

- a) **(2 points)** Une unité fondamentale de l'anneau $\mathbb{Z}[\sqrt{15}]$ est donnée par la solution entière (x, y) de l'équation $x^2 - 15y^2 = \pm 1$ telle que $x, y \geq 1$ et x est minimal. Il est facile de voir que cette solution est $(4, 1)$, donc $\omega = 4 + \sqrt{15} \in \mathbb{Z}[\sqrt{15}]$ est une unité fondamentale.

Cette unité est de norme $(4 + \sqrt{15})(4 - \sqrt{15}) = 1$ ($(4, 1)$ est solution de $x^2 - 15y^2 = 1$) donc, selon le cours, les solutions de l'équation $x^2 - 15y^2 = 1$ correspondent, au signe près, au puissance de ω :

$$\{(x, y) \in \mathbb{Z}^2 : x^2 - 15y^2 = 1\} = \{(x, y) : \exists n \in \mathbb{Z}, x + y\sqrt{15} = \pm (4 + \sqrt{15})^n\}$$

- b) **(1 point)** L'unité fondamentale $\omega \in \mathbb{Z}[\sqrt{15}]$ étant de norme 1, aucune unité n'est de norme -1 et l'équation $x^2 + 15y^2 = -1$ n'a aucune solution.

4.

(3 points) Les caractères de Dirichlet modulo 8 correspondent aux caractères $\alpha: (\mathbb{Z}/8\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$. On sait que $(\mathbb{Z}/8\mathbb{Z})^\times = \{\pm 1, \pm 3\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$. En choisissant les générateurs -1 et 3 de $(\mathbb{Z}/8\mathbb{Z})^\times$, on obtient que les caractères de Dirichlet correspondent aux couples $(\alpha, \beta) \in \{\pm 1\}^2$: à un tel couple correspond le caractère

$$\begin{array}{ccc} (\mathbb{Z}/8\mathbb{Z})^\times & \longrightarrow & \mathbb{C}^\times \\ 1 & \longmapsto & 1 \\ -1 & \longmapsto & \alpha \\ 3 & \longmapsto & \beta \\ -3 = -1.3 & \longmapsto & \alpha\beta \end{array}$$

donc, le caractère de Dirichlet

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{C}^\times \\ a & \longmapsto & \begin{cases} 1 & \text{si } a \equiv 1 \pmod{8} \\ \alpha & \text{si } a \equiv -1 \pmod{8} \\ \beta & \text{si } a \equiv 3 \pmod{8} \\ \alpha\beta & \text{si } a \equiv -3 \pmod{8} \\ 0 & \text{sinon} \end{cases} \end{array}$$

De même, les caractères de Dirichlet modulo 12 correspondent aux caractères $\alpha: (\mathbb{Z}/12\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$. On sait que $(\mathbb{Z}/12\mathbb{Z})^\times = \{\pm 1, \pm 5\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$. En choisissant les générateurs -1 et 5 de $(\mathbb{Z}/12\mathbb{Z})^\times$, on obtient que les caractères de Dirichlet correspondent aux couples $(\alpha, \beta) \in \{\pm 1\}^2$: à un tel couple correspond le caractère

$$\begin{array}{ccc} (\mathbb{Z}/12\mathbb{Z})^\times & \longrightarrow & \mathbb{C}^\times \\ 1 & \longmapsto & 1 \\ -1 & \longmapsto & \alpha \\ 5 & \longmapsto & \beta \\ -5 = -1.5 & \longmapsto & \alpha\beta \end{array}$$

donc, le caractère de Dirichlet

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{C}^\times \\ a & \longmapsto & \begin{cases} 1 & \text{si } a \equiv 1 \pmod{12} \\ \alpha & \text{si } a \equiv -1 \pmod{12} \\ \beta & \text{si } a \equiv 5 \pmod{12} \\ \alpha\beta & \text{si } a \equiv -5 \pmod{12} \\ 0 & \text{sinon} \end{cases} \end{array}$$