Université de Paris
Master de Mathématiques

Théorie algébrique des nombres I
Année 2021-22
H. Chen, P. Molin, L. Merel

CORRIGÉ de l'EXAMEN du 3 novembre 2021

I

1. C'est l'ordre de $(\mathbf{Z}/N\mathbf{Z})^\times$: $N-1$.
2. Notons Tr la trace relativement à l'extension $\mathbf{Q}(\zeta)|\mathbf{Q}$. Comme le groupe $\mathbf{Z}[\zeta]$ est engendré par $(\zeta^i)_{1\leq i\leq N-1}$, le discriminant est, au signe près, $\det(\mathrm{Tr}(\zeta^{i+j})_{i,j})$. Or $\mathrm{Tr}(\zeta^k) = -1$ si $\zeta^k \neq 1$ et $\mathrm{Tr}(1) = N-1$. On a donc à calculer le déterminant d'une matrice $(N-1)\times(N-1)$ dont les termes sont égaux à -1 sauf les termes antidiagonaux qui valent $N-1$. Une manipulation sur les lignes et les colonnes donne le résultat. (On peut aussi procéder en calculant le discriminant du polynôme cyclotomique.)
3. Puisque p ne divise pas le discriminant, c'est un nombre premier non ramifié.
4. La substitution de Frobenius ϕ associée à un idéal $\mathcal{P}$ au dessus de p vérifie $\phi(x) \equiv x^p \pmod{\mathcal{P}}$ pour tout $x \in \mathbf{Z}[\zeta]$. Il suffit de vérifier pour $x = \zeta$. On a donc $\phi = \sigma_p$.
5. Comme $\mathbf{R}$ est dénué de racine primitive N-ème de 1, il n'y a pas de plongement de $\mathbf{Q}(\zeta)$ dans $\mathbf{R}$. Donc $r = 0$. Comme l'extension $\mathbf{Q}(\zeta)|\mathbf{Q}$ est de degré $2s + r$, on a $s = (N-1)/2$.
6. Cette norme est $\prod_{i=1}^{N-1}(1-\zeta^i) = \Phi_N(1) = N$.
7. Comme $1-\zeta$ divise N, l'anneau $\mathbf{Z}[\zeta]/(1-\zeta)$ est un anneau quotient de $\mathbf{Z}$ de caractéréristique résiduelle N. C'est donc un corps.
8. On a $N = \prod_{i=1}^{N-1}(1-\zeta^i)$. Chaque facteur engendre un idéal maximal. On a ainsi l'inventaire des idéaux premiers au dessus de N. Ils sont tous prinicpaux.
9. Le rang de ce groupe est $r + s - 1 = (N-3)/2$.
10. On a bien $-\zeta \in \mathbf{Z}[\zeta]^\times$ et $-\zeta$ est d'ordre $2N$. Soit $\alpha \in \mathbf{Z}[\zeta]^\times$ d'ordre M. Le groupe engendré par α et ζ contient un élément β d'ordre $L = \mathrm{ppcm}(M, 2N)$. Mais β est de degré $|(\mathbf{Z}/L\mathbf{Z})^\times|$, car c'est une racine du L-ème polynôme cyclotomique, qui est irréductible sur $\mathbf{Q}$. On a donc $|(\mathbf{Z}/L\mathbf{Z})^\times| = |(\mathbf{Z}/N\mathbf{Z})^\times|$, et donc $L = 2N$. Donc α est d'ordre divisant $2N$. Or il n'y a que $2N$ racines au polynôme $X^{2N} - 1$; ce sont les puissances de $-\zeta$.
11. On a $u_i = \sum_{j=0}^{i-1}\zeta^j \in \mathbf{Z}[\zeta]$, et $u_i^{-1} = \sum_{j=0}^{i^{-1}-1} u^{ji} \in \mathbf{Z}[\zeta]$.
12. On a $u_i/u_{-i} = (1-\zeta^i)(1-\zeta^{-i})^{-1} = -\zeta^i$.

II

1. Cela résulte de l'identité $1/(1-\chi(p)p^{-s}) = \sum_{k=0}^{\infty}\chi(p^k)/p^{ks}$. On développe ensuite en utilisant la factorisation des entiers en produit de facteurs premiers.
2. On peut réordonner la somme $\sum_{n=1}^{\infty}\chi(n)/n^s$ par une sommation d'Abel. On obtient $\sum_{n=1}^{\infty}(\sum_{k=1}^{n}\chi(k))(1/n^s - 1/(n+1)^s)$. Remarquons que $(\sum_{k=1}^{n}\chi(k))$ est borné lorsque n varie, car $\chi \neq 1$ et donc $\sum_{n=m}^{m+N}\chi(n) = 0$. De plus, on a $|1/n^s - 1/(n+1)^s| = |n^{-s}(1-(1+1/n)^{-s})| < s/n^{s+1}$ (au moins pour n assez grand). Ainsi, la série converge absolument lorsque $\Re(s) > 0$. Ainsi, $\epsilon = 1$ convient.
3. On va montrer la formule facteur par facteur. Soit p un nombre premier. Si $p \neq N$, il suffit de montrer la formule $\prod_{\mathcal{P}} 1/(1-|\mathbf{Z}[\zeta]/|\mathcal{P}|^{-s}) = \prod_{\chi\in X_N} 1/(1-\chi(p)p^{-s})$, où $\mathcal{P}$

parcourt les idéaux premier au dessus de p. Soit f l'ordre de p dans $(\mathbf{Z}/N\mathbf{Z})^\times$. C'est le degré résiduel en $\mathcal{P}$ pour tout idéal premier au dessus de p. Alors $\chi(p)$ parcourt les racines f-èmes de l'unité avec multiplicité $(N-1)/f$, lorsque χ parcourt X_N. En passant aux inverses, le membre de gauche est donc $(1-p^{-fs})^{(N-1)/f}$ et le membre de gauche est $\prod_\theta(1-\theta p^{-s})^{(N-1)/f}$, où θ parcourt les racines f-ème de l'unité. On a donc c'est-à-dire $\prod_\theta(1-\theta p^{-s})^{(N-1)/f} = (1-p^{-fs})^{(N-1)/f}$. Pour $p=N$, les facteurs d'Euler sont tous deux égaux à $1/(1-N^{-s})$, puisqu'il n'y a qu'un seul idéal premier au dessus de N.
4. Les fonctions $Z_{\mathbf{Q}(\zeta)}$ et $Z_{\mathbf{Q}}$ sont méromorphes et ont un pôle simple en $s=1$. Comme les facteurs $L(\chi,s)$ sont holomorphes au voisinage de $s=1$, on a $L(\chi,1)\neq 0$ pour $\chi\neq 1$.
5. C'est l'application de la formule du nombre de classes. On a vu que $r=0$ et $s=(N-1)/2$, qu'il y a $2N$ racines de l'unité, que le discriminant est N^{N-2}.
6. Utilisons la formule $\log(1-\rho\zeta^{-a}) = -\sum_{k=1}^\infty \rho^k\zeta^{-ka}/k$, valide pour $\rho\in[0,1[$. On a donc $(-G(\chi)/N)\sum_{a=1}^{N-1}\bar\chi(a)\log(1-\rho\zeta^{-a}) = G(\chi)/N\sum_{k=1}^\infty\sum_{a=1}^{N-1}\bar\chi(a)\rho^k\zeta^{-ka}/k$. On trouve ensuite $G(\chi)/N\sum_{k=1}^\infty\bar G(\chi)\chi(k)\rho^k/k$. Lorsque ρ tend vers 1, cette quantité tend vers $G(\chi)/N\sum_{k=1}^\infty\bar G(\chi)\chi(k)/k$ (par sommation d'Abel). Les paramètres a, b et c dans les sommes qui suivent parcourent $(\mathbf{Z}/N\mathbf{Z})^\times$. Il reste à montrer que $G(\chi)\bar G(\chi)=N$. On a $G(\chi)\bar G(\chi) = (\sum_a\chi(a)\zeta^a)(\sum_b\bar\chi(b)\zeta^{-b}) = \sum_{a,b}\chi(a/b)\zeta^{a-b}$. Posons $c=a/b$. Ce changement de variable donne $G(\chi)\bar G(\chi) = \sum_c\chi(c)\sum_a\zeta^{a(1-c)}$. Or, si $c\neq 1$, on a $\sum_a\zeta^{a(1-c)}=-1$. Donc $G(\chi)\bar G(\chi) = (\sum_{c\neq1}-\chi(c)) + \sum_a 1 = 1+(N-1)=N$.
7. On a $\log(1-\zeta^a) = \log|1-\zeta^a| + i(\pi/2-\pi a/N)$ et $\log(1-\zeta^{-a}) = \log|1-\zeta^a| - i(\pi/2-\pi a/N)$. Puisque $\chi(-1)=-1$, on a la formule cherchée.
8. Cela résulte de la formule précédente et de la non-nullité de $L(\chi,1)$.
9. Cela résulte de $\chi(-1)=1$ et de l'identité $2\log|1-\zeta^{-a}| = \log(1-\zeta^{-a})+\log(1-\zeta^a)$.
10. Le $\mathbf{C}$-espace vectoriel $M\otimes\mathbf{C}$ hérite de la structure de G-module de M. Soit $\theta\in G$. On a $\theta(\sum_{\tau\in\hat G}\tau(m)\otimes\chi(\tau)) = \bar\chi(\theta)\sum_{\tau\in\hat G}\tau(m)\otimes\chi(\tau)$. Ainsi, les termes $\sum_{\tau\in\hat G}\tau(m)\otimes\chi(\tau)$ appartiennent à des sous-espaces en somme directe de $M\otimes\mathbf{C}$. Comme ces termes sont non nuls, ils engendrent un espace vectoriel de dimension $|G|$, qui à son tour est engendré, comme espace vectoriel, par $(\tau(m))_{\tau\in\hat G}$. Ainsi le sous-groupe engendré par $(\tau(m))_{\tau\in\hat G}$ est de rang $\geq|G|$, et donc de rang $|G|$.
11. On applique la proposition précédente au groupe $G=(\mathbf{Z}/N\mathbf{Z})^\times/\{\pm1\}$, et à $m=(1-\zeta)(1-\zeta^{-1})$. On a $\sigma_i((1-\zeta)(1-\zeta^{-1})) = (1-\zeta^i)(1-\zeta^{-i}) = |1-\zeta^i|^2$. La condition $\sum_{\tau\in\hat G}\tau(m)\otimes\chi(\tau)\neq 0$ se traduit via le logarithme par $\sum_{a=1}^{(N-1)/2}\bar\chi(a)\log|1-\zeta^{-a}|\neq 0$; elle est donc satisfaite. Ainsi les conjugués de m engendrent un groupe de rang $(N-1)/2$. De plus, pour $1\leq i\leq(N-1)/2$, on a $m_i = -(1-\zeta^i)^2\zeta^{-i}$. Donc le groupe engendré par les $(1-\zeta^i)$ est d'indice une puissance de 2, à torsion près, dans le sous-groupe engendré par les m_i. Il est donc aussi de rang $(N-1)/2$.
12. Comme les $1-\zeta^i$ engendrent un groupe de rang $(N-1)/2$, les u_i engendrent un groupe de rang $(N-1)/2-1$. Or le groupe $\mathbf{Z}[\zeta]^\times$ est de rang $(N-1)/2-1$. Ses sous-groupes de rang $(N-1)/2-1$ sont donc d'indice fini.

NB : On ne connaît pas de démonstration élémentaire de II.8. Le fait que le groupe engendré par les u_i (dites *unités cyclotomiques*) soit d'indice fini i_N dans le groupe des unités n'admet pas non plus de démonstration élémentaire. On peut poursuivre la théorie en reliant, par la formule du nombre de classes, le nombre de classe h_N à i_N.