Université de Paris
Master de Mathématiques

Théorie algébrique des nombres II
Année 2020-21
H. Chen, P. Molin, L. Merel

CORRIGÉ de l'EXAMEN du 6 janvier 2021

I

1. Soit I un idéal de $\mathcal{O}_K$. Montrer que la classe de I dans $\mathcal{C}\ell_K$ est un carré si et seulement si pour tout caractère quadratique $\tilde{\chi}$ de $\mathcal{C}\ell_K$ on a $\tilde{\chi}(I) = 1$.

Si $I = J^2$ est un carré, on a $\tilde{\chi}(I) = \tilde{\chi}(J^2) = (\tilde{\chi}(J))^2 = 1$. Réciproquement, le groupe quotient $\mathcal{C}\ell_K/\mathcal{C}\ell_K^2$ est un espace vectoriel de dimension finie (car $\mathcal{C}\ell_K$ est un groupe fini) sur le corps $\mathbf{F}_2$. Si I n'est pas un carré dans $\mathcal{C}\ell_K$, il existe une forme linéaire $\lambda : \mathcal{C}\ell_K/\mathcal{C}\ell_K^2 \to \mathbf{F}_2$ qui ne s'annule pas sur la classe de I. On pose alors, pour un idéal J de classe j dans $\mathcal{C}\ell_K/\mathcal{C}\ell_K^2$: $\tilde{\chi}(J) = (-1)^{\lambda(j)}$. C'est le caractère cherché et on a $\tilde{\chi}(I) = -1$.

2. Montrer que dans le noyau du morphisme canonique $\mathcal{C}\ell_K^+ \to \mathcal{C}\ell_K$ tout élément au carré est trivial.

Soit I un idéal fractionnaire dont la classe est dans ce noyau. Alors I est un idéal principal, engendré par, disons, $a \in K^\times$. L'idéal $I^2 = a^2\mathcal{O}_K$ admet un générateur totalement positif. Ainsi la classe de I^2 est triviale dans $\mathcal{C}\ell_K^+$.

3. Soit $\tilde{\chi}$ un caractère de $\mathcal{C}\ell_K^+$. Notons χ le caractère de Hecke unitaire associé. En quelles places finies v, la composante locale χ_v est-elle ramifiée ?

Le morphisme $\mathbf{A}_K^\times \to \mathcal{C}\ell_K^+$ a pour noyau $K^\times.(\prod_{v\in S_f} \mathcal{O}_v^\times \prod_{v\in S_\infty} K_v^+)$, où $K_v^+ = \mathbf{R}_+^\times$ si v est réelle et $\mathbf{C}^\times$ si v est archimédienne non-réelle. Comme le noyau contient $\mathcal{O}_v^\times$ pour toute place finie v, tout caractère qui se factorise par ce morphisme est non-ramifié en toute place finie.

4. Si v est une place finie, montrer qu'on a $\chi_v(\pi_v) = \tilde{\chi}(\mathcal{P}_v)$.

Notons $\alpha = (\alpha_w)_{w\in S_K}$ l'idèle dont toutes les composantes sont égales à 1 sauf la composante en v qui vaut π_v. On a $\tilde{\chi}(\mathcal{P}_v) = \chi(\alpha) = \prod_w \chi_w(\alpha_w) = \chi_v(\alpha_v) = \chi_v(\pi_v)$.

5. Montrer que, si $K_v = \mathbf{C}$, on a $\chi_v = 1$, et que, si $K_v = \mathbf{R}$, on a $\chi_v = 1$ ou la fonction signe. Montrer que si $\tilde{\chi}$ se factorise par $\mathcal{C}\ell_K^+ \to \mathcal{C}\ell_K$, on a $\chi_v = 1$ lorsque $K_v = \mathbf{R}$.

La première assertion résulte du fait que χ, et par conséquent χ_v, est d'image finie. Le caractère trivial est le seul caractère d'image finie de $\mathbf{C}^\times$. Les seuls caractères d'images finies de $\mathbf{R}^\times$ sont le caractère trivial et la fonction signe.

Dire que χ se factorise par $\mathcal{C}\ell_K^+ \to \mathcal{C}\ell_K$ revient à dire que le noyau de χ contient $K^\times.(\prod_{v\in S_f} \mathcal{O}_v^\times \prod_{v\in S_\infty} K_v^\times)$, c'est-à-dire que $\chi_v = 1$ pour toute place archimédienne.

6. Montrer que pour v place finie de K, on a $\eta_v(\mathcal{O}_v) = q_v^{n_v/2}$.

Partons de la formule $\eta_v(\mathcal{O}_v)\eta_v(\mathcal{D}_v) = 1$. Comme $\mathcal{D}_v$ est un sous-groupe d'indice $q_v^{n_v}$ de $\mathcal{O}_v$ et que η_v est une mesure de Haar, on a $\eta_v(\mathcal{D}_v) = q_v^{-n_v}\eta_v(\mathcal{O}_v)$ et donc $\eta_v(\mathcal{O}_v)^2 = q_v^{n_v}$, d'où le résultat.

7. Montrer que $\epsilon(\chi, s) = (-i)^t\overline{\tilde{\chi}(\mathcal{D}_K)}/|\mathcal{D}_K|^{1/2-s}$, en explicitant t.

Observons que $\chi_v(\mathcal{D}_K) = \chi_v(\mathcal{D}_v) = \chi_v(\pi_v^{n_v})$. Notons t le nombre de places réelles v telles que $\chi_v(-1) = -1$. D'après la formule donnée dans les rappels ci-dessus, on a $\epsilon(\chi, s) = (-i)^t \prod_{v\in S_f} \eta_v(\mathcal{O}_v)/(\chi_v(\pi_v^{n_v})q_v^{n_v(1-s)}) = (-i)^t \prod_{v\in S_f} \bar\chi_v(\pi_v^{n_v})/q_v^{(1/2-s)n_v} = (-i)^t \overline{\tilde\chi(\mathcal{D}_K)}/|\mathcal{D}_K|^{1/2-s}$.

II

1. Montrer que sa différente est l'idéal engendré par $2\sqrt{3}$.

On a $\mathbf{Z}[\sqrt{3}] = \mathbf{Z} + \mathbf{Z}\sqrt{3}$. Soit $a + b\sqrt{3} \in \mathbf{Q}(\sqrt{3})$, avec a, $b \in \mathbf{Q}$. On a $\mathrm{Tr}_{\mathbf{Q}(\sqrt{3})/\mathbf{Q}}(y(a + b\sqrt{3})) \in \mathbf{Z}$ pour tout $y \in \mathbf{Z}[\sqrt{3}]$ si et seulement si on a $\mathrm{Tr}_{\mathbf{Q}(\sqrt{3})/\mathbf{Q}}(a + b\sqrt{3}) \in \mathbf{Z}$ et $\mathrm{Tr}_{\mathbf{Q}(\sqrt{3})/\mathbf{Q}}(\sqrt{3}(a + b\sqrt{3})) \in \mathbf{Z}$. C'est-à-dire : $2a \in \mathbf{Z}$ et $6b \in \mathbf{Z}$. Ainsi, la condition devient : $a + b\sqrt{3} \in \frac{1}{2\sqrt{3}}\mathbf{Z}[\sqrt{3}]$. Donc la différente est engendrée par $2\sqrt{3}$.

2. Quel est le discriminant de $\mathbf{Q}(\sqrt{3})$?

C'est l'indice de cet idéal dans l'anneau des entiers, ou encore la norme de $2\sqrt{3}$. Ainsi, c'est $(2\sqrt{3})^2 = 12$.

3. Montrer que la différente de $\mathbf{Q}(\sqrt{3})$ n'est pas un carré dans $\mathcal{C}\ell^+_{\mathbf{Q}(\sqrt{3})}$.

Cette différente est un idéal principal. Il suffit de montrer qu'elle n'est pas engendrée par un élément totalement positif. Or $2\sqrt{3}$ n'est pas totalement positif. Tout autre générateur de la différente est le produit de $2\sqrt{3}$ par une unité. Or $\mathbf{Q}(\sqrt{3})$ a pour seules unités les $a + b\sqrt{3}$ avec a, $b \in \mathbf{Z}$ et $a^2 - 3b^2 = 1$ ou -1. Le cas $a^2 - 3b^2 = -1$ est rendu impossible par les congruences modulo 4. Ainsi, toute unité de $\mathbf{Q}(\sqrt{3})$ est de norme 1 et est donc totalement positive ou totalement négative. Donc aucun générateur de la différente n'est totalement positif.

4. Montrer que $\mathbf{Q}(\sqrt{-1}, \sqrt{3})|\mathbf{Q}(\sqrt{3})$ est quadratique et contient $\mathbf{Q}(\sqrt{-3})$.

Cette extension est engendrée par $\sqrt{-1}$, racine de $X^2 + 1$ qui n'est pas réelle et donc pas dans $\mathbf{Q}(\sqrt{3})$. On a bien une extension quadratique. Comme le produit d'une racine de -1 et d'une racine de 3 est une racine de -3, l'extension contient bien $\mathbf{Q}(\sqrt{-3})$.

5. Montrer que l'extension $\mathbf{Q}(\sqrt{-1}, \sqrt{3})|\mathbf{Q}(\sqrt{3})$ est partout non ramifiée.

L'extension $\mathbf{Q}(\sqrt{3})|\mathbf{Q}$ est ramifiée en 2 et 3 seulement (les nombres premiers qui divisent le discriminant). L'extension $\mathbf{Q}(\sqrt{-3})|\mathbf{Q}$ est ramifiée en 3 seulement. L'extension $\mathbf{Q}(\sqrt{-1})|\mathbf{Q}$ est ramifiée en 2 seulement. Donc l'extension $\mathbf{Q}(\sqrt{-1}, \sqrt{3})|\mathbf{Q}(\sqrt{3})$ est ramifiée tout au plus en les premiers au-dessus de 2. L'indice de ramification en ces nombres premiers est le rapport des indices de ramifications des extensions $\mathbf{Q}(\sqrt{-1}, \sqrt{3})|\mathbf{Q}$ et $\mathbf{Q}(\sqrt{3})|\mathbf{Q}$. L'extension $\mathbf{Q}(\sqrt{3})|\mathbf{Q}$ est totalement ramifiée (indice 2). L'extension $\mathbf{Q}(\sqrt{-1}, \sqrt{3})|\mathbf{Q}$ est ramifiée en 2, mais pas totalement car l'extension intermédiaire $\mathbf{Q}(\sqrt{-3})|\mathbf{Q}$ n'est pas ramifiée en 2 (l'indice divise 4 mais n'est ni 1, ni 4 ; c'est 2). Ainsi $\mathbf{Q}(\sqrt{-1}, \sqrt{3})|\mathbf{Q}(\sqrt{3})$ est non-ramifiée en les premiers au-dessus de 2.

6. Le corps de classe de Hilbert de $\mathbf{Q}(\sqrt{3})$ contient-il $\mathbf{Q}(\sqrt{-1}, \sqrt{3})$?

Non puisque le corps $\mathbf{Q}(\sqrt{-1}, \sqrt{3})$ n'est pas totalement réel alors que $\mathbf{Q}(\sqrt{3})$ l'est.

7. Soit $\tilde\chi$ un caractère non trivial de $\mathcal{C}\ell^+_{\mathbf{Q}(\sqrt{3})}$. Supposons que χ est le caractère de $C_{\mathbf{Q}(\sqrt{3})}$ associé. Calculer $\epsilon(\chi, s)$.

On reprend la formule de **I**.7. Observons d'abord que le corps $\mathbf{Q}(\sqrt{3})$ possède deux places archimédiennes qui sont toutes deux réelles. Comme on a $\chi(-1) = 1$, on a $\prod_{v\in S_\infty} \chi_v(-1) = 1$. Comme χ est non-trivial, on a $\chi_v(-1) = -1$ pour tout $v \in S_\infty$. On a donc $t = 2$. Montrons que $\mathcal{C}\ell^+_{\mathbf{Q}(\sqrt{3})}$ est d'ordre 2. Un élément a de $K^\times$ engendre un élément de $\mathcal{C}\ell^+_{\mathbf{Q}(\sqrt{3})}$ qui ne dépend des deux signes de a (pour les deux plongements de K dans $\mathbf{R}$). Comme a et $-a$ engendrent le même idéal fractionnaire, un éléments de $K^\times$ ne peut définir que deux classes dans $\mathcal{C}\ell^+_{\mathbf{Q}(\sqrt{3})}$, qui est donc d'ordre au plus 2. Il est d'ordre 2 puisque $\mathcal{D}_{\mathbf{Q}(\sqrt{3})}$ n'est pas trivial dans $\mathcal{C}\ell^+_{\mathbf{Q}(\sqrt{3})}$. On a donc $\tilde{\chi}(\mathcal{D}_K) = -1$. On trouve finalement $\epsilon(\chi, s) = 12^{s-1/2}$.

III

1. Montrer qu'il existe une extension quadratique $E|K$ partout non ramifiée, réelle au dessus de toutes les places réelles de K et telle que, pour toute place finie v, la substitution de Frobenius en v soit triviale dans $\mathrm{Gal}(E/K)$ si et seulement si $\tilde{\chi}(\mathcal{P}_v) = 1$.

Le noyau de $\tilde{\chi}$ est un sous-groupe d'indice 2 de $\mathcal{C}\ell_K$. Soit T le sous-groupe correspondant de $\mathrm{Gal}(H/K) \simeq \mathcal{C}\ell_K$. Posons $E = H^T$. L'extension $E|K$ est de degré l'indice de T dans $\mathrm{Gal}(H/K)$, c'est-à-dire 2. Les autres propriétés découlent immédiatement des propriétés de H.

Le caractère $\tilde{\chi}$ s'identifie à un caractère de $\mathrm{Gal}(H/K)$ qui se factorise par le quotient $\mathrm{Gal}(H/K)/T \simeq \mathrm{Gal}(E/K)$. La substitution de Frobenius en v de $\mathrm{Gal}(E/K)$ est triviale si et seulement si la substitution de Frobenius en v de $\mathrm{Gal}(H/K)$ est dans T, c'est-à-dire si et seulement si $\tilde{\chi}(\mathcal{P}_v) = 1$.

2. Quelle est la densité de Dirichlet de l'ensemble d'idéaux premiers $\mathcal{P}_v$ de $\mathcal{O}_K$ tels que $\chi_v(\pi_v) = 1$?

C'est la densité de Dirichlet des idéaux premiers $\mathcal{P}_v$ de $\mathcal{O}_K$ tels que la substitution de Frobenius en v est triviale dans $\mathrm{Gal}(E/K)$. Puisque l'extension $E|K$ est quadratique, c'est $1/2$, par le théorème de Chebotarev.

3. Pour v place finie de K, montrer la formule $\prod_{w|v}(1-q_v^{-f_w s}) = (1-q_v^{-s})(1-\chi_v(\pi_v)q_v^{-s})$, où w parcourt les places de E au-dessus de v et f_w est le degré résiduel de $E_w|K_v$.

On sait que v n'est pas ramifiée dans K. Si v est décomposée dans E, on a $f_w = 1$ et $\chi_v(\pi_v) = 1$. La formule est vérifiée. Si v est inerte dans E, on a $f_w = 2$ et $\chi_v(\pi_v) = -1$. La formule est vérifiée.

4. En déduire qu'on a $\Lambda_E(s) = \Lambda_K(s)\Lambda(\chi, s)$.

On vérifie cela facteur par facteur. Plus précisément, on vérifie pour chaque place v de K que $\prod_{w|v} L_w(1_{E,s}) = L_v(1_K, s)L_v(\chi_v, s)$. C'est ce qu'on vient de montrer pour les places finies. Si v est une place archimédienne réelle (resp. non-réelle), il y a deux places réelles (resp. non-réelles) au dessus de v, si bien que la formule est évidente si on tient compte du fait que les composantes aux places infinies de χ sont triviales.

5. Montrer que $\epsilon(1_E, s) = \epsilon(1_K, s)\epsilon(\chi, s)$.

On a $\epsilon(1_K, s)\epsilon(\chi, s)\Lambda(K, 1-s)\Lambda(\bar{\chi}, 1-s) = \Lambda_K(s)\Lambda(\chi, s) = \Lambda(E, s) = \epsilon(1_E, s)\Lambda_E(1-s) = \epsilon(1_E, s)\Lambda_K(1-s)\Lambda(\chi, 1-s)$. Comme χ est quadratique, on a $\bar{\chi} = \chi$. On obtient la formule cherchée.

6. En déduire que $|\mathcal{D}_E| = |\mathcal{D}_K|^2$.

On a $\epsilon(\chi, s) = (-i)^t\tilde{\chi}(\mathcal{D}_K)|\mathcal{D}_K|^{1/2-s}$ d'après **I**.7 avec $t = 0$ et $\tilde{\chi} = \overline{\tilde{\chi}}$. On a de plus $\epsilon(1_K, s) = |\mathcal{D}_K|^{1/2-s}$ et $\epsilon(1_E, s) = |\mathcal{D}_E|^{1/2-s}$. La formule en résulte en considérant les modules de ces nombres.

7. *Coronidis loco* : en déduire que $\mathcal{D}_K$ est un carré dans $\mathcal{C}\ell_K$.

On reprend la formule de **III**.5 et les précisions de **III**.6. On trouve $\tilde{\chi}(\mathcal{D}_K) = 1$, ce qui démontre que $\mathcal{D}_K$ est un carré dans $\mathcal{C}\ell_K$ d'après le critère de **I**.1.

Cette dernière assertion est un théorème de Hecke (dont la preuve donnée ici est due à Serre). On peut voir cet énoncé de parité comme analogue en arithmétique de certains théorèmes de géométrie, tels que la parité de la caractéristique d'Euler–Poincaré d'une surface de Riemann compacte. Il occupe la dernière section du livre de Weil *Basic Number Theory*, où il est annoncé par la locution *Coronidis loco*.