Algèbre avancée
Corrigé de l'examen partiel

Exercice 1

Soit B une base de transcendance de L/K. Par définition du degré de transcendance, B est de cardinal n. Alors B est une famille algébriquement libre dans l'extension $K(T_1,\dots,T_n)/K$, qui est elle aussi de degré de transcendance n, ce qui entraîne que B est une base de transcendance de $K(T_1,\dots,T_n)/K$. En particulier l'extension $K(T_1,\dots,T_n)/K(B)$ est algébrique ; a fortiori $K(T_1,\dots,T_n)/L$ est algébrique. Cette dernière extension étant aussi de type fini (engendrée par $T_1,\dots,T_n$), elle est donc nécessairement finie.

Exercice 2

1. Posons $n = km$ avec $k \geqslant 1$. On a $M = K(\zeta^k)$ car ζ^k est une racine primitive m-ième de l'unité. Soit $\sigma \in \mathrm{Gal}(L/K)$; notons σ_M la restriction de σ à M (cette restriction est bien définie car M/K est cyclotomique, donc galoisienne). Il s'agit de montrer que

$$\chi_n(\sigma) \equiv \chi_m(\sigma_M) \pmod{m}.$$

   Par définition du caractère cyclotomique, on a $\sigma(\zeta) = \zeta^a$ où a est un représentant de $\chi_n(\sigma)$ dans $\mathbf{Z}$. En élevant cette identité à la puissance k, il vient

$$\sigma_M(\zeta^k) = \sigma(\zeta^k) = \sigma(\zeta)^k = \zeta^{ka} = (\zeta^k)^a$$

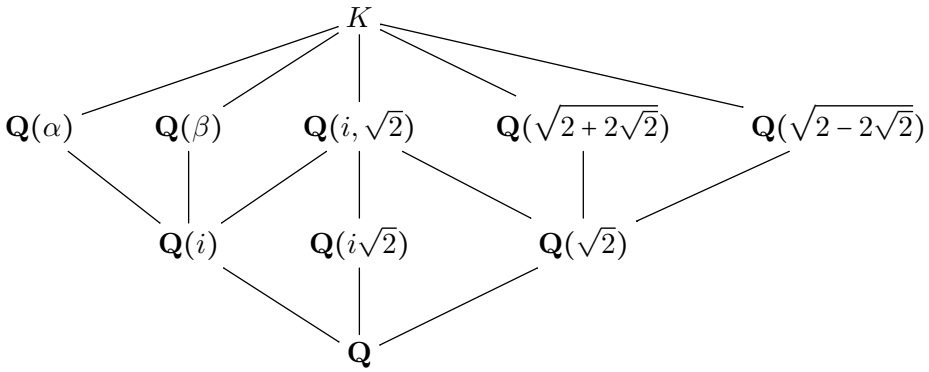
   et donc $\chi_m(\sigma_M)$ est égal à la classe de a modulo m, ce qu'il fallait démontrer.
2. On sait que $\mathbf{F}_{16}^\times$ est cyclique d'ordre 15, donc $\mathbf{F}_{16}$ contient bien une racine primitive quinzième de l'unité ζ. De même, le sous-corps $\mathbf{F}_4$, vu comme extension de $\mathbf{F}_2$, est engendré par une racine primitive cubique de l'unité, et donc $M = \mathbf{F}_4$. D'après le cours, le groupe $\mathrm{Gal}(\mathbf{F}_{16}/\mathbf{F}_2)$ est cyclique d'ordre 4, engendré par le Frobenius $F : x \mapsto x^2$. En particulier $F(\zeta) = \zeta^2$ ce qui prouve que $\chi_{15}(F) = 2 \in (\mathbf{Z}/15\mathbf{Z})^\times$. Le groupe $\mathrm{Gal}(\mathbf{F}_4/\mathbf{F}_2)$ est cyclique d'ordre 2, engendré par le Frobenius $F_M : x \mapsto x^2$, et l'on a $\chi_3(F_M) = 2 \in (\mathbf{Z}/3\mathbf{Z})^\times$.

Problème – Équations bicarrés

1. On a $K = \mathbf{Q}(\alpha,\beta)$ donc $[K : \mathbf{Q}] = [\mathbf{Q}(\alpha)(\beta) : \mathbf{Q}(\alpha)] \cdot [\mathbf{Q}(\alpha) : \mathbf{Q}]$. Comme P est irréductible, on a $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 4$. De plus $P = (X^2-\alpha^2)(X^2-\beta^2)$ donc β est annulé par le polynôme $X^2-\beta^2 = X^2+a+\alpha^2$ à coefficients dans $\mathbf{Q}(\alpha)$, et donc β est de degré 1 ou 2 sur $\mathbf{Q}(\alpha)$, d'où le résultat.
2. D'après le cours, G est isomorphe à un sous-groupe de $\mathfrak{S}_4$. Comme G est d'ordre 4 ou 8, il suit que G est contenu dans un 2-Sylow de $\mathfrak{S}_4$. Or, les 2-Sylow de $\mathfrak{S}_4$ sont isomorphes à D_4 (le groupe diédral D_4 est le groupe des symétries du carré ; il se plonge dans $\mathfrak{S}_4$ en considérant l'action sur les sommets du carré). Donc G est isomorphe à un sous-groupe de D_4.
3. Si G est d'ordre 8, alors $G \cong D_4$. Sinon G est d'ordre 4, et tout groupe d'ordre 4 est isomorphe à $\mathbf{Z}/4\mathbf{Z}$ ou $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (si G contient un élément d'ordre 4, alors $G \cong \mathbf{Z}/4\mathbf{Z}$; sinon tous les éléments de G sont d'ordre 1 ou 2, donc G est abélien et même un $\mathbf{Z}/2\mathbf{Z}$-espace vectoriel, nécessairement isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$).
4. On sait que $\alpha^2 + \beta^2 = -a \in \mathbf{Q}$. Par l'absurde, si $\alpha^2 - \beta^2 \in \mathbf{Q}$, alors $\alpha^2, \beta^2 \in \mathbf{Q}$, ce qui contredit l'irréductibilité de P.

5. Soit $\sigma \in G$ tel que $\sigma(\alpha) = \beta$ et $\sigma(\beta) = -\alpha$. Montrons que σ est d'ordre 4. L'ordre de σ ne pouvant être que 1, 2 ou 4, il suffit de montrer que $\sigma^2 \neq \mathrm{id}_K$. Or $\sigma^2(\alpha) = \sigma(\beta) = -\alpha$.
   Réciproquement, supposons que G contient un élément σ d'ordre 4. Montrons que σ ou σ^{-1} remplit les conditions demandées. On voit σ comme une permutation de l'ensemble $R = \{\pm\alpha, \pm\beta\}$, et on distingue les cas suivants la valeur de $\sigma(\alpha) \in R$. Si $\sigma(\alpha) = \pm\alpha$, alors σ laisse stable l'ensemble $\{\alpha, -\alpha\}$, donc (la permutation associée à) σ est d'ordre 1 ou 2, ce qui est exclu. Supposons $\sigma(\alpha) = \beta$. On a $\sigma(\beta) = \pm\alpha$ par le même argument que précédemment. Si $\sigma(\beta) = \alpha$ alors σ échange α et β, ainsi que $-\alpha$ et $-\beta$, donc est d'ordre 2, impossible. Ainsi $\sigma(\beta) = -\alpha$ comme demandé. Supposons enfin $\sigma(\alpha) = -\beta$. Le raisonnement ci-dessus étant insensible au choix de la racine de $X^2 - \beta^2$, on a aussi $\sigma(-\beta) = -\alpha$, donc σ est le 4-cycle $(\alpha; -\beta; -\alpha; \beta)$, et σ^{-1} convient.
6. Supposons $G \cong \mathbf{Z}/4\mathbf{Z}$. D'après la question 5, le groupe G est engendré par un élément σ vérifiant $\sigma(\alpha) = \beta$ et $\sigma(\beta) = -\alpha$. Alors
$$\sigma\Big(\frac{\alpha}{\beta} - \frac{\beta}{\alpha}\Big) = \frac{\beta}{-\alpha} - \frac{-\alpha}{\beta} = \frac{\alpha}{\beta} - \frac{\beta}{\alpha},$$
   Ainsi $\frac{\alpha}{\beta} - \frac{\beta}{\alpha}$ est fixé par G, et donc $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} \in \mathbf{Q}$. De plus $\sigma(\alpha\beta) = -\beta\alpha \neq \alpha\beta$ donc $\alpha\beta \notin \mathbf{Q}$ (on peut aussi remarquer que $(\alpha\beta) \cdot (\frac{\alpha}{\beta} - \frac{\beta}{\alpha}) = \alpha^2 - \beta^2$ est irrationnel d'après la question 4, donc nécessairement l'un des facteurs l'est aussi).
7. Supposons $G \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Comme P est irréductible, le groupe G agit transitivement sur R. Soit $\sigma \in G$ un élément tel que $\sigma(\alpha) = \beta$. On a nécessairement $\sigma(\beta) = \alpha$ (sinon G contiendrait un élément d'ordre 4, grâce à la question 5). Ainsi σ est la double transposition $(\alpha; \beta)(-\alpha; -\beta)$. Mais il existe aussi un élément $\sigma' \in G$ tel que $\sigma'(\alpha) = -\beta$, et par symétrie des rôles joués par β et $-\beta$, la permutation σ' est aussi une double transposition, à savoir $(\alpha; -\beta)(-\alpha; \beta)$. Les éléments σ et σ' étant distincts, ils engendrent G. On vérifie que $\alpha\beta$ est fixé par σ et σ', ce qui entraîne $\alpha\beta \in \mathbf{Q}$. D'autre part $\frac{\alpha}{\beta} - \frac{\beta}{\alpha}$ n'est pas fixé par σ ; on aurait sinon $\frac{\alpha}{\beta} = \frac{\beta}{\alpha}$, donc $\alpha^2 = \beta^2$, ce qui est impossible d'après la question 4.
   Remarque. Dans ce cas G s'identifie au groupe de Klein (groupe des doubles transpositions dans $\mathfrak{S}_4$).
8. Supposons $G \cong D_4$. D'après la question 5, G contient le 4-cycle $\sigma = (\alpha; \beta; -\alpha; -\beta)$. On a $\sigma(\alpha\beta) = -\alpha\beta$ et donc $\alpha\beta \notin \mathbf{Q}$. Comme G est d'ordre 8, G contient *exactement* deux éléments envoyant α sur β. Notons τ l'autre élément de G tel que $\tau(\alpha) = \beta$. On a alors $\tau(\beta) = \alpha$ (le cas $\tau(\beta) = \pm\beta$ conduit à une absurdité, car τ est injective). Donc τ échange α et β, et on montre comme dans la question 7 que $\frac{\alpha}{\beta} - \frac{\beta}{\alpha}$ n'est pas fixé par τ.
9. Le polynôme P est irréductible d'après le critère d'Eisenstein (avec $p = 2$). On calcule explicitement $\alpha = \sqrt[4]{2} \cdot e^{i\pi/8}$ et $\beta = \sqrt[4]{2} \cdot e^{-i\pi/8}$. Alors $\alpha\beta = \sqrt{2}$ est irrationnel, ce qui exclut le cas $G \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, et $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} = e^{i\pi/4} - e^{-i\pi/4} = i\sqrt{2} \notin \mathbf{Q}$, ce qui exclut le cas $G \cong \mathbf{Z}/4\mathbf{Z}$. Par suite $G \cong D_4$.
10. On reprend les notations de la question 8 : le groupe G est engendré par $\sigma = (\alpha; \beta; -\alpha; -\beta)$ et $\tau = (\alpha; \beta)(-\alpha; -\beta)$. En posant $H = \langle\sigma\rangle$, on a $G = H \sqcup \tau H$. On peut visualiser les éléments de G en dessinant un carré et en notant $\alpha, \beta, -\alpha, -\beta$ ses sommets, dans le sens trigonométrique. Alors les éléments de H correspondent aux rotations d'angle multiple de $\pi/2$, et les éléments de τH correspondent aux symétries par rapport à l'axe des abscisses, l'axe des ordonnées ou une diagonale du carré.
    Les sous-corps de K sont en bijection avec les sous-groupes de D_4. Considérons uniquement les sous-corps non triviaux, c'est-à-dire de degré 2 ou 4 sur $\mathbf{Q}$. Les sous-corps de degré 2 sont en bijection avec les sous-groupes d'ordre 4 de D_4. Ils sont au nombre de trois : H (rotations), $H_0 = \{1, \tau, \sigma^2, \tau\sigma^2\}$ (symétries par rapport aux axes de coordonnées) et $H_1 = \{1, \tau\sigma, \sigma^2, \tau\sigma^3\}$ (symétries par rapport aux diagonales). On a déjà vu que H fixe $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} = i\sqrt{2}$, donc $K^H = \mathbf{Q}(i\sqrt{2})$. Par ailleurs $\alpha^2 = 1 + i$ donc K contient i et $\sqrt{2}$. On dispose donc de deux sous-corps supplémentaires, à savoir $\mathbf{Q}(i)$ et $\mathbf{Q}(\sqrt{2})$, et d'après la correspondance de Galois il n'y en a pas d'autre (exercice : déterminer quel sous-corps correspond à quel sous-groupe).
    Les sous-corps de degré 4 sont en bijection avec les sous-groupes d'ordre 2 de G, eux-mêmes en bijection avec les éléments d'ordre 2, c'est-à-dire σ^2 et $\tau\sigma^i$ avec $i \in \{0, 1, 2, 3\}$. Les sous-corps « évidents » $\mathbf{Q}(\alpha)$

et $\mathbf{Q}(\beta)$ sont fixés respectivement par $\tau\sigma$ et $\tau\sigma^3$. On connaît également le sous-corps $\mathbf{Q}(i,\sqrt{2})$, qui est fixé par $H_0 \cap H_1$, c'est-à-dire par σ^2. Il reste à trouver les sous-corps fixés par τ et $\tau\sigma^2$. En fait τ est la conjugaison complexe (on a $\beta = \overline{\alpha}$), donc $K^\tau = K \cap \mathbf{R}$. Montrons que ce corps est engendré par $\alpha+\beta$. Il est clair que $\alpha+\beta \in \mathbf{R}$. Par ailleurs les itérés de $\alpha+\beta$ par σ sont successivement $\beta-\alpha$, $-\alpha-\beta$ et $-\beta+\alpha$, qui sont deux à deux distincts, donc $\alpha+\beta$ est de degré au moins 4 sur $\mathbf{Q}$, et donc $K^\tau = \mathbf{Q}(\alpha+\beta)$ avec $\alpha+\beta = 2\sqrt[4]{2}\cos(\frac{\pi}{8}) = \sqrt{2+2\sqrt{2}}$. Enfin, l'élément $\tau\sigma^2$ est conjugué à τ : on a $\tau\sigma^2 = \sigma\tau\sigma^{-1}$, et d'après le cours, il vient $K^{\tau\sigma^2} = \sigma(K^\tau) = \mathbf{Q}(\sigma(\alpha+\beta)) = \mathbf{Q}(\alpha-\beta) = \mathbf{Q}(i\sqrt{2\sqrt{2}-2})$.
Voici donc le treillis des sous-corps de K :



Les sous-corps galoisiens sur $\mathbf{Q}$ sont ceux qui correspondent aux sous-groupes distingués de G ; dans la liste précédente, il y a $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(i\sqrt{2})$ et $\mathbf{Q}(i,\sqrt{2})$; en effet, un sous-groupe d'indice 2 de G est distingué, et σ^2 est le seul élément d'ordre 2 invariant par conjugaison (*i. e.* dans le centre de G).

11. En calculant explicitement les racines $\pm\alpha, \pm\beta$ du polynôme $P = X^4 + aX^2 + b$, on trouve les formules suivantes :
$$(\alpha\beta)^2 = b \qquad \frac{\alpha}{\beta} - \frac{\beta}{\alpha} = \frac{\alpha^2-\beta^2}{\alpha\beta} = \sqrt{\frac{a^2-4b}{b}}$$
Ainsi $\alpha\beta \in \mathbf{Q}$ si et seulement si b est un carré dans $\mathbf{Q}$ (*i. e.* dans $\mathbf{Z}$), et $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} \in \mathbf{Q}$ si et seulement si $\frac{a^2-4b}{b}$ est un carré dans $\mathbf{Q}$. De plus, pour assurer que $P = X^4 + aX^2 + b$ soit irréductible, on fait en sorte que les produits (ou sommes) deux à deux des racines de P sont tous irrationnels, ce qui rajoute la condition $\alpha^2, \beta^2 \notin \mathbf{Q}$, c'est-à-dire que $a^2 - 4b$ n'est pas un carré dans $\mathbf{Q}$ (*i. e.* dans $\mathbf{Z}$).
Pour le premier cas ($G \cong \mathbf{Z}/4\mathbf{Z}$), on peut prendre $a = 3$ et $b = 1$, d'où $P = X^4 + 3X^2 + 1$.
Pour le deuxième cas ($G \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$), on peut prendre $a = 4$ et $b = 2$, d'où $P = X^4 + 4X^2 + 2$.
Pour le troisième cas ($G \cong D_4$), on a déjà $P = X^4 - 2X^2 + 2$.

Question subsidiaire. Un nombre entier ou un nombre rationnel pris « au hasard » n'est, le plus souvent, pas un carré : par exemple, la densité des carrés parfaits dans l'ensemble des entiers naturels tend vers zéro lorsque l'on considère des entiers de plus en plus grands. Par suite, le groupe de Galois d'un polynôme bicarré sera le plus souvent D_4. On peut rendre cette affirmation précise de la manière suivante : la proportion de couples $(a,b) \in [\![-N, N]\!]^2$ tels que le polynôme $X^4 + aX^2 + b$ est irréductible sur $\mathbf{Q}$ et de groupe Galois D_4 tend vers 1 lorsque N tend vers l'infini. En utilisant les conditions trouvées à la question 11, il n'est pas trop difficile d'établir cette assertion rigoureusement.