Université Paris Cité
Sorbonne Université
Master de Mathématiques

Théorie algébrique des nombres I
Année 2024-25
R. Brasca, L. Merel

CORRIGÉ de l'EXAMEN du 29 octobre 2024

I

Soit K un corps décomposition du polynôme X^3-2 sur $\mathbf{Q}$. Posons $G=\mathrm{Gal}(K/\mathbf{Q})$. Pour p premier non ramifié dans K, notons $C(p)$ la classe de conjugaison dans G d'une substitution de Frobenius en p. Notons d le degré de l'extension $K|\mathbf{Q}$.

1. Montrer que le polynôme X^3-2 est irréductible sur $\mathbf{Q}$.

C'est le critère d'Eisenstein pour le nombre premier 2.

2. Montrer que K contient une racine cubique primitive de 1, notée j, et que $K=\mathbf{Q}(\alpha,j)$ où $\alpha\in K$ vérifie $\alpha^3-2=0$.

Évidemment puisque les racines de K sont α, $j\alpha$, $j^2\alpha$.

3. En déduire que $d=6$. Quels sont les nombres de plongements réels et complexes non réels de K ?

Comme X^3-2 est irréductible sur $\mathbf{Q}$, le corps K est de degré ≥ 3 sur $\mathbf{Q}$. Il est de degré $\leq 6=3!$, puisque le degré de X^3-2 est 3. Il contient le corps $\mathbf{Q}(\alpha)$ engendré par α qui est de degré 3 sur $\mathbf{Q}$. Mais K n'est pas $\mathbf{Q}(\alpha)$, puisque $\mathbf{Q}(\alpha)$ est plongé dans $\mathbf{R}$ par $\alpha\mapsto\sqrt{2}$ et que j ne peut pas être plongé dans $\mathbf{R}$. Donc $d>3$, $3|d$ et $d\leq 6$. Donc $d=6$. Comme j ne peut être plongé dans $\mathbf{R}$, on a $r_1=0$ et $r_2=3$.

4. Notons μ_3 le groupe formé par les racines cubiques de l'unité dans $\mathbf{Q}(j)$. Montrer que l'application $\mathrm{Gal}(K/\mathbf{Q}(j))\to\mu_3$ qui à σ associe $\sigma(\alpha)/\alpha$ est un isomorphisme de groupes. En déduire que $\mathrm{Gal}(K/\mathbf{Q})$ est un groupe d'ordre 6. Il est engendré par deux éléments τ et ϵ, qui vérifient $\tau^3=1$, $\epsilon\tau\epsilon=\tau^{-1}$ et $\epsilon^2=1$. On pourra caractériser τ et ϵ par $\tau(\alpha)=j\alpha$, $\tau(j)=j$, $\epsilon(j)=j^{-1}$ et $\epsilon(\alpha)=\alpha$.

L'extension $K|\mathbf{Q}$ est galoisienne de degré 6. Donc $\mathrm{Gal}(K/\mathbf{Q})$ est un groupe d'ordre 6. Le sous-groupe $\mathrm{Gal}(K/\mathbf{Q}(j))$ est d'ordre $6/2=3$. On vérifie que $\sigma\mapsto\sigma(\alpha)/\alpha$ est bien un morphisme en remarquant que $\sigma(\alpha)/\alpha\in\mu_3$ et est donc invariant par $\mathrm{Gal}(K/\mathbf{Q}(j))$. Ce morphisme est injectif car si $\sigma(\alpha)=\alpha$, on a que σ est trivial sur α et j et donc trivial sur K. Soit τ un générateur de $\mathrm{Gal}(K/\mathbf{Q}(j))$. Il vérifie $\tau(\alpha)=j\alpha$ ou $\tau(\alpha)=j^2\alpha$. Quitte à changer τ en son inverse, on peut supposer que $\tau(\alpha)=j\alpha$. Soit ϵ un générateur du groupe $\mathrm{Gal}(K/\mathbf{Q}(\alpha))$ qui est d'ordre 2. Il vérifie bien les conditions demandées.

5. Montrer que les extensions $\mathbf{Q}(\alpha)|\mathbf{Q}$ et $\mathbf{Q}(j)|\mathbf{Q}$ sont non ramifiées en dehors de 2 et 3. En déduire que l'extension $K|\mathbf{Q}$ est non ramifiée en dehors de 2 et 3.

Le discriminant du polynôme X^2-3 est le résultant des polynômes X^3-2 et $3X^2$. C'est $-108=-2^2.3^3$. C'est pourquoi K est non ramifié en dehors de 2 et 3.

6. Montrer que les classes de conjugaison de G sont $C_1=\{1\}$, $C_2=\{\tau,\tau^{-1}\}$, $C_3=\{\epsilon,\epsilon\tau,\epsilon\tau^2\}$.

C_1 est la classe de conjugaison de l'identité. Les conditions données sur τ et ϵ montrer que les éléments de C_2 et C_3 respectivement sont conjugués. Les éléments de C_2 et C_3 sont d'ordres 3 et 2 respectivement, si bien qu'un élément de C_2 ne peut être conjugué à un élément de C_3. Ainsi on a bien des classes de conjugaison.

7. Soit p un nombre premier > 3.

7.a Montrer que $C(p) = C_1$ si et seulement si on a simultanément que 2 est un cube modulo p et que -3 est un carré modulo p. Ou encore si et seulement si on a $p \equiv 1 \pmod 3$ et $2^{(p-1)/3} \equiv 1 \pmod p$.

On a $C(p) = C_1$ si et seulement si p est totalement décomposé dans K. Cela revient à dire que $X^3 - 2$ est scindé sur $\mathbf{F}_p$. Cela revient à dire que $X^3 - 2$ a une racine sur $\mathbf{F}_p$ et que son discriminant est un carré modulo p. Cela revient encore à dire que 2 est un cube modulo p et que -3 est un carré modulo p (puisque $-108 = -3.6^2$). Cela revient encore à dire que $2^{(p-1)/3} \equiv 1 \pmod p$ et que $p \equiv 1 \pmod 3$.

7.b Montrer que $C(p) = C_2$ si et seulement si on a simultanément que -3 est un carré et 2 n'est pas un cube modulo p. Ou encore si et seulement si on a $p \equiv 1 \pmod 3$ et on n'a pas $2^{(p-1)/3} \equiv 1 \pmod p$.

On a $C(p) = C_2$ si et seulement si $X^3 - 2$ est sans racine sur $\mathbf{F}_p$. Cela revient à dire que 2 n'est pas un cube modulo p. Cela revient encore à dire que $p \equiv 1 \pmod 3$ et qu'on n'a pas $2^{(p-1)/3} \equiv 1 \pmod p$.

7.c Montrer que $C(p) = C_3$ si et seulement si on a simultanément que -3 n'est pas un carré modulo p et que 2 est un cube modulo p. Ou encore si et seulement si on a $p \equiv -1 \pmod 3$.

On a $C(p) = C_3$ si et seulement si une substitution de Frobenius en p agit comme une transposition sur les trois racines de $X^3 - 2$. Cela revient à dire que $X^3 - 2$ admet une seule racine dans $\mathbf{F}_p$. Cela revient à dire que 2 est un cube modulo p et que -3 n'est pas un carré modulo p. Si -3 n'est pas un carré modulo p, on a $p \equiv -1 \pmod 3$. Ainsi l'application $x \mapsto x^3$ est surjective sur $\mathbf{F}_p^*$, si bien que 2 est un cube modulo p. Cela revient encore à dire que $p \equiv -1 \pmod 3$.

8. Calculer les densités analytiques des ensembles de nombres premiers $\{p/C(p) = C_i\}$, pour $i = 1, 2, 3$. Dans chaque cas, indiquer le degré résiduel en p de l'extension $K|\mathbf{Q}$.

La densité analytique est $|C_i|/|G| = i/6$. Le degré résiduel est l'ordre d'une substitution de Frobenius dans G. L'ordre d'une substitution de Frobenius dans C_i est 1 si $i = 1$, c'est 2 si $i = 3$ et c'est 3 si $i = 2$.

II

Soit K un corps de nombres. Notons $\mathcal{O}_K$ son anneau d'entiers et $d = [K : \mathbf{Q}]$ son degré. Soit r un entier ≥ 1. On dit que $\mathcal{O}_K$ est *engendré par r éléments comme* $\mathbf{Z}$*-algèbre* s'il existe $(\alpha_1, \alpha_2, ..., \alpha_r) \in \mathcal{O}_K^r$ tel que l'application $\mathbf{Z}[X_1, ..., X_r] \to \mathcal{O}_K$ qui à P associe $P(\alpha_1, ..., \alpha_r)$ est surjective.

Soit p un nombre premier totalement décomposé dans K (*i.e.* p est non ramifié dans K et tous les idéaux premiers de $\mathcal{O}_K$ au-dessus de p sont de degré résiduel égal à 1). On note $\mathbf{F}_p$ le corps à p éléments.

Supposons que $\mathcal{O}_K$ est engendré par r éléments comme $\mathbf{Z}$-algèbre.

1. Montrer qu'il existe p totalement décomposé dans K.

C'est un fait général qui découle du théorème de densité de Chebotarev (il existe un nombre premier p tel que la classe de conjugaison d'une substitution de Frobenius en p soit l'identité dans le groupe de Galois d'une extension galoisienne contenant K).

2. Montrer qu'il existe un morphisme surjectif d'anneaux $\mathbf{F}_p[X_1, ..., X_r] \to \mathcal{O}_K/p\mathcal{O}_K$.

Comme le morphisme d'anneaux $\mathbf{Z}[X_1, ..., X_r] \to \mathcal{O}_K$ qui à P associe $P(\alpha_1, ..., \alpha_r)$ est surjectif. On peut passer au quotient pour obtenir un morphisme surjectif d'anneaux $\mathbf{F}_p[X_1, ..., X_r] \to \mathcal{O}_K/p\mathcal{O}_K$.

3. Montrer que l'anneau $\mathcal{O}_K/p\mathcal{O}_K$ est isomorphe à $\mathbf{F}_p^d$.

Comme p est totalement décomposé dans $\mathcal{O}_K$, il s'écrit comme produit de d idéaux premiers distincts de $\mathcal{O}_\mathcal{K}$. On a donc $\mathcal{O}_K/p\mathcal{O}_K \simeq \prod_{\mathcal{P}|p} \mathcal{O}_K/\mathcal{P}$. Comme le degré résiduel de tout facteur est 1, on a $\mathcal{O}_K/\mathcal{P}$ est isomorphe à $\mathbf{F}_p$. On a donc d copies de $\mathbf{F}_p$.

4. Montrer que l'anneau $\mathbf{F}_p[X_1, ..., X_r]$ possède p^r idéaux maximaux de corps résiduel $\mathbf{F}_p$.

Les idéaux maximaux de $A = \mathbf{F}_p[X_1, ..., X_r]$ de corps résiduel $\mathbf{F}_p$ sont de la forme $(X_1 - a_1)A + ... + (X_r - a_r)A$, avec $(a_1, ..., a_r) \in \mathbf{F}_p^r$. Il y en a donc p^r.

5. En déduire que $d \leq p^r$.

L'anneau $\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbf{F}_p^d$ possède au moins d idéaux maximaux qui sont les noyaux des projections sur les coordonnées de $\mathbf{F}_p^d$. Or tout idéal maximal de $\mathcal{O}_K/p\mathcal{O}_K$ donne lieu injectivement à un idéal maximal de $\mathbf{F}_p[X_1, ..., X_r]$. Ainsi on a $d \leq p^r$.

III

On reprend les notations de la partie **II**. On ne suppose plus que $\mathcal{O}_K$ est engendré par r éléments comme $\mathbf{Z}$-algèbre.

Soit l un nombre premier. Soit ζ est une racine primitive l-ème de l'unité. Notons $\mathbf{Q}(\zeta)$ le corps cyclotomique engendré par ζ. On rappelle que son anneau des entiers est $\mathbf{Z}[\zeta]$, que $\mathbf{Q}(\zeta)|\mathbf{Q}$ est une extension abélienne, dont le groupe de Galois s'identifie à $(\mathbf{Z}/l\mathbf{Z})^\times$ par $i + l\mathbf{Z} \mapsto (\zeta \mapsto \zeta^i)$. Notons $\mathbf{Q}(\zeta)^+$ le sous-corps de $\mathbf{Q}(\zeta)$ formé par les invariants sous le groupe $\{-1, 1\} \subset (\mathbf{Z}/l\mathbf{Z})^\times \simeq \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$.

1. Montrer que l'anneau des entiers de $\mathbf{Q}(\zeta)^+$ est engendré par 1 élément comme $\mathbf{Z}$-algèbre.

On a $\alpha = \zeta + \zeta^{-1} \in \mathbf{Q}(\zeta)^+$. Montrons que c'est le générateur cherché. C'est un entier algébrique, car $\zeta^{-1} = \zeta^{l-1}$. L'anneau $\mathbf{Z}[\zeta]$ est un $\mathbf{Z}$-module libre sur $(\zeta^i)_{1 \leq i \leq l-1}$. Soit $a = \sum_i \lambda_i \zeta^i$ une combinaison linéaire entière de $(\zeta^i)_{1 \leq i \leq l-1}$ telle que $a \in \mathbf{Q}(\zeta)^+$. On a alors, pour tout i, la relation $\lambda_i = \lambda_{-i}$. Cela montre que l'anneau des entiers de $\mathbf{Q}(\zeta)^+$ est engendré comme groupe par les $(\zeta^i + \zeta^{-i})_{1 \leq i \leq (l-1)/2}$. On montre par une récurrence sur i que $\zeta^i + \zeta^{-i}$ est dans $\mathbf{Z}[\alpha]$ (utiliser la formule du binôme pour $(\zeta + \zeta^{-1})^i$). Ainsi, l'anneau des entiers de $\mathbf{Q}(\zeta)^+$ est $\mathbf{Z}[\alpha]$.

2. Montrer qu'il existe un corps cubique dont l'anneau des entiers est engendré par 1 élément comme $\mathbf{Z}$-algèbre.

Pour $l = 7$, le corps $\mathbf{Q}(\zeta)^+$ est un corps cubique. On utilise la question précédente.

3. Quels sont les nombres premiers p et l tels que $\mathbf{Q}(\zeta)$ contienne un corps cubique K (*i.e.* de degré 3 sur $\mathbf{Q}$) et p totalement décomposé dans K ?

Les sous-corps de $\mathbf{Q}(\zeta)$ correspondent aux sous-groupes d'indice 3 de $(\mathbf{Z}/l\mathbf{Z})^\times$. Un tel sous-groupe C existe si et seulement si $l \equiv 1 \pmod 3$, c'est le sous groupe formé par les cubes modulo l. La substitution de Frobenius en p dans l'extension $\mathbf{Q}(\zeta)|\mathbf{Q}$ correspond à

la classe de p modulo l dans $(\mathbf{Z}/l\mathbf{Z})^\times$. Ainsi le nombre premier p est totalement décomposé dans K si et seulement $p \in C$, *i.e.* p est un cube modulo l.

4. Pour $p = 2$, y a-t-il une infinité de tels nombres premiers l ? (On pourra utiliser la partie **I**.)

Oui, c'est l'ensemble des nombres premiers p tels que la substitution de Frobenius en p est dans C_1. Il y en a une infinité par le théorème de Chebotarev.

5. Donner un exemple de corps cubique K tel que $\mathcal{O}_K$ n'est pas engendré par 1 élément comme $\mathbf{Z}$-algèbre. (On pourra utiliser la partie **II**.)

D'après la partie **II**, il suffit de trouver un tel corps cubique dans lequel 2 est totalement décomposé. Cela contredit l'inégalité $3 = d < 2^r = 2$. Considérons le cas $l = 31$. Comme $32 = 2^5 \equiv 1 \pmod{31}$, 2 est un cube modulo 31, si bien que 2 est totalement décomposé dans le sous-corps cubique K de $\mathbf{Q}(\zeta)$.

6. Montrer que $\mathbf{Q}(\zeta)$ admet un sous-corps K de degré d sur $\mathbf{Q}$ avec p totalement décomposé dans K si et seulement si $l \equiv 1 \pmod{d}$ et $p^{(l-1)/d} \equiv 1 \pmod{l}$.

Comme ci-dessus, l'existence de ce sous-corps revient à l'existence d'un sous-groupe C d'indice d de $(\mathbf{Z}/l\mathbf{Z})^\times$ tel que la classe de p modulo l soit dans C, qui est nécessairement le sous-groupe des puissances d-èmes. Ces conditions reviennent à $l \equiv 1 \pmod{d}$ et $p^{(l-1)/d} \equiv 1 \pmod{l}$.

7. Montrer que cette dernière condition est satisfaite si et seulement si l est totalement décomposé dans un corps de décomposition du polynôme $X^d - p$.

Cela revient à ce que p soit une puissance d-ème modulo l et que l soit congru à 1 modulo d. Cela revient encore à ce que le polynôme $X^d - p$ soit scindé sur $\mathbf{F}_l$.

8. Montrer qu'il existe une extension abélienne K de $\mathbf{Q}$ telle que $\mathcal{O}_K$ n'est pas engendré par r éléments comme $\mathbf{Z}$-algèbre. (On pourra utiliser la partie **II**.)

D'après la partie **II**, il suffit de trouver une extension K de degré $d > 2^r$ avec 2 totalement décomposé dans K. Si on choisit K comme un sous-corps d'un corps cyclotomique, on est assuré que K est une extension abélienne. Soit d tel que $d > 2^r$. D'après le théorème de Chebotarev, il existe un nombre premier l qui est totalement décomposé dans un corps de décomposition du polynôme $X^d - 2$. Alors le corps $\mathbf{Q}(\zeta)$ admet un sous-corps K de degré d sur $\mathbf{Q}$ avec 2 totalement décomposé dans K, si bien qu'on a trouvé l'exemple cherché.