

EXAMEN du 21 octobre 2025

Durée : 3h

*Tout appareil électronique et tout document sont interdits, exceptée une feuille manuscrite.
Les parties sont indépendantes.*

I

Soit $P \in \mathbf{Z}[X]$ un polynôme irréductible de degré premier p . Notons L un corps de décomposition de P . Notons G le groupe de Galois de $L|\mathbf{Q}$.

1. Montrer que G agit transitivement sur les racines de P .
2. En déduire que G contient un p -cycle.
3. Montrer qu'il y a une infinité de nombres premiers q tels que le groupe de décomposition en tout idéal premier de L au dessus de q soit cyclique d'ordre p .
4. En déduire que, pour ces nombres premiers q , la réduction de P modulo q est irréductible sur le corps fini $\mathbf{F}_q$.

II

Soit $P(X) = X^5 - 2 \in \mathbf{Z}[X]$. Soit $K = \mathbf{Q}(\alpha)$ où α est une racine de P . On précise $\frac{5!}{5^5}(\frac{4}{\pi})^2\sqrt{50000} = 13,919\dots$

1. Montrer que P est irréductible sur $\mathbf{Q}$.
2. Quel est le degré de l'extension $K|\mathbf{Q}$?
3. Quels sont les nombres r_1 et $2r_2$ de plongements réels et complexes non réels de K ?
4. Quel est le nombre de racines de l'unité de K ?
5. Montrer que le discriminant de P est 50000.
6. Quels sont les nombres premiers ramifiés dans l'extension $K|\mathbf{Q}$?
7. Montrer que 2 et 5 sont totalement ramifiés dans l'extension $K|\mathbf{Q}$. (On pourra considérer le polynôme $(X + 2)^5 - 2$.)
8. Montrer que l'anneau des entiers de K est $\mathbf{Z}[\alpha]$.
9. Quel est le discriminant de K ?
10. Montrer que pour p nombre premier ≤ 13 , il existe un unique premier non nul $\mathcal{P}_p$ de $\mathcal{O}_K$ de norme absolue p si et seulement si $p \neq 11$.
11. Montrer que le groupe des classes de K est engendré par $\{\mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_5, \mathcal{P}_7, \mathcal{P}_{13}\}$.
12. Notons les relations $N_{K/\mathbf{Q}}(1 + 2\alpha) = 65$, $N_{K/\mathbf{Q}}(1 - 2\alpha) = -63$, $N_{K/\mathbf{Q}}(\alpha) = -2$, $N_{K/\mathbf{Q}}(2 - \alpha) = -30$, $N_{K/\mathbf{Q}}(1 + \alpha) = -3$. En déduire que le groupe des classes de K est trivial.

III

Soit $F \in \mathbf{Z}[X]$ unitaire, irréductible de degré d . Soit α un entier algébrique racine de F . Notons $\alpha_1, \alpha_2, \dots, \alpha_d$ les conjugués de α dans $\mathbf{C}$. On pose $M(\alpha) = M(F) = \prod_{i=1}^d \max(1, |\alpha_i|)$. C'est la *mesure de Mahler* de F (et de α). On pose $\overline{|\alpha|} = \max(|\alpha_1|, |\alpha_2|, \dots, |\alpha_d|)$. Supposons que α n'est pas une racine de l'unité et $\alpha \neq 0$. La *conjecture de Lehmer* affirme qu'il existe $c_L > 1$ (indépendant de F et d) tel que $M(\alpha) > c_L$. La *conjecture de Schinzel-Zassenhaus*, démontrée par Dimitrov, affirme qu'il existe $c_{SZ} > 0$ (indépendant de F et d) avec $\overline{|\alpha|} > 1 + c_{SZ}/d$.

Rappelons que le résultant $\mathcal{R}(P, Q)$ de deux polynômes unitaires P et Q est $\prod_y Q(y)$ où y parcourt les racines de P , comptées avec multiplicité. Le discriminant $\mathcal{D}(P)$ de P est le résultant de P et P' . Si $P = \prod_{i=1}^n (X - \beta_i)$ est sans racine multiple, $\mathcal{D}(P)$ est, au signe près, $\prod_{i,j,i \neq j} (\beta_i - \beta_j)$, ce qui est, au signe près, le carré du déterminant de Vandermonde $\det(\beta_i^j)_{1 \leq i \leq n, 0 \leq j \leq n-1}$.

1. Montrer que la conjecture de Lehmer entraîne la conjecture de Schinzel-Zassenhaus.
2. Quels sont les entiers algébriques α tels que $M(\alpha) = 1$?
3. Montrer que si α n'est pas une unité, on a $M(\alpha) \geq 2$. En déduire que ces conjectures sont vraies si on se restreint au cas où α n'est pas une unité.
4. Soit p un nombre premier. Posons $F_p(X) = (X - \alpha_1^p)(X - \alpha_2^p) \dots (X - \alpha_d^p)$. Montrer que $F_p \in \mathbf{Z}[X]$ et que $F_p \equiv F \pmod{p}$.
5. En déduire que p^d divise $\mathcal{R}(F, F_p)$, puis que p^{2d} divise le discriminant Δ_p de FF_p .
6. Montrer par ailleurs que $|\Delta_p| \leq (2d)^{2d} M(\alpha)^{4d(p+1)}$. On pourra utiliser l'inégalité d'Hadamard : le déterminant d'une matrice complexe est borné par le produit des normes hermitiennes de ses vecteurs lignes (ou colonnes).
7. Montrer que F et F_p n'ont pas de racine commune.
8. Montrer que $M(\alpha) \geq (\frac{p}{2d})^{1/(2p+2)}$ pour p assez grand.
9. En déduire qu'il existe $c_D > 1$ (indépendant de d et F) tel que $M(\alpha) > c_D^{1/d}$. (On pourra utiliser le postulat de Bertrand : il existe un nombre premier entre x et $2x$, pour tout entier $x \geq 2$ ou le théorème des nombres premiers dont le postulat de Bertrand découle.)