

Corrigé de l'EXAMEN du 21 octobre 2025

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 .

C'est le cas, car P est irréductible.

2. En déduire que G contient un p -cycle.

L'orbite sous G de n'importe quelle racine est d'ordre p . Donc p divise l'ordre de G , qui contient donc un élément d'ordre p . Comme G s'identifie à un sous-groupe du groupe symétrique $\mathcal{S}_p$, il 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 .

D'après Chebotarev, il existe une infinité de nombre premiers q tel que la classe de conjugaison de Frobenius en q soit la classe de conjugaison du cycle d'ordre p . Pour presque tout nombre premier q , tout groupe de décomposition en q est cyclique engendré par le Frobenius correspondant. Il est donc 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 $\mathbf{F}_q$.

Le groupe de décomposition agit fidèlement sur les racines de la réduction de P modulo q . Comme il est cyclique d'ordre p , il agit transitivement, si bien que la réduction modulo q est irréductible.

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 $\mathbf{Q}$.

Critère d'Eisenstein en le nombre premier 2.

2. Quel est le degré de l'extension $K|\mathbf{Q}$?

Puisque P est irréductible, c'est le degré de P , c'est-à-dire 5.

3. Quels sont les nombres r_1 et $2r_2$ de plongements réels et complexes non réels de K ?

Le polynôme P admet une racine réelle et 4 racines non réelles. On a donc $r_1 = 1$ et $2r_2 = 4$.

4. Quel est le nombre de racines de l'unité de K ?

Comme K admet un plongement réel, il n'y a que 2 racines de l'unité.

5. Montrer que le discriminant de P est 50000.

Calcul direct.

6. Quels sont les nombres premiers ramifiés dans l'extension $K|\mathbf{Q}$?

Comme le discriminant de P a pour seuls diviseurs premiers 2 et 5, seuls 2 et 5 sont ramifiés.

7. Montrer que 2 et 5 sont totalement ramifiés dans l'extension $K|\mathbf{Q}$. (On pourra considérer le polynôme $(X + 2)^5 - 2$.)

Comme 2 est une puissance 5-ème dans K , l'indice de ramification de $K|\mathbf{Q}$ vaut au moins 5. Comme l'indice de ramification est $\leq [K : \mathbf{Q}]$, l'extension est totalement ramifiée en 2. Le polynôme $(X - 2)^5 - 2$ est d'Eisenstein en 5, si bien que pour les mêmes raisons l'extension est totalement ramifiée en 5.

8. Montrer que l'anneau des entiers de K est $\mathbf{Z}[\alpha]$.

Il contient $\mathbf{Z}[\alpha]$. L'indice de l'anneau des entiers $\mathcal{O}_K$ dans $\mathbf{Z}[\alpha]$ divise le discriminant de P . D'après le critère d'Eisenstein pour la p -maximalité, 2 et 5 ne divisent pas cet indice. Donc l'indice vaut 1 et $\mathcal{O}_K = \mathbf{Z}[\alpha]$.

9. Quel est le discriminant de K ?

C'est le discriminant de P puisque l'anneau des entiers de K est $\mathbf{Z}[\alpha]$ et α est une racine de P .

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 $p \neq 11$.

Examinons la réduction de P modulo p . Si $p = 2$ ou $p = 5$, comme l'extension $K|\mathbf{Q}$ est totalement ramifiée, on a la propriété voulue. Si $p = 5, 7$ ou 13 , 2 est une puissance 5-ème modulo p (en effet $x \mapsto x^5$ est surjective sur les entiers modulo p , pour p congru à 2 ou 3 modulo 5) $\mathbf{F}_p$ est un corps résiduel de K . L'idéal premier $\mathcal{P}_p$ correspondant est de norme absolue p . Comme $\mathbf{Z}[\alpha] \simeq \mathbf{Z}[X]/(P(X))$, les corps résiduels en les premiers au-dessus de p sont les $\mathbf{F}_p[X](Q(X))$ où Q est un facteur irréductible de la réduction modulo p de P . De façon équivalente, ces facteurs irréductibles correspondent à la décomposition de p comme produit d'idéaux premiers de $\mathbf{Z}[\alpha]$. Comme 2 admet une unique racine 5-ème dans $\mathbf{F}_p$, un seul de ces facteurs irréductible est de degré 1. Ainsi, il n'y a qu'un seul idéal au-dessus de p de norme absolue égale à p .

Si $p = 11$, 2 n'est pas une puissance 5-ème modulo 11, si bien qu'il n'y a pas de morphisme d'anneaux $\mathbf{Z}[\alpha] \rightarrow \mathbf{F}_p$, et donc pas d'idéal au dessus de 11 de norme absolue égale à 11.

11. Montrer que le groupe des classes de K est engendré par $\{\mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_5, \mathcal{P}_7, \mathcal{P}_{13}\}$.

D'après Minkowski, toute classe d'idéaux de K admet un représentant dans $\mathbf{Z}[\alpha]$ de norme inférieure à $\frac{5!}{5^5}(\frac{4}{\pi})^2\sqrt{50000} < 14$. Le groupe des classes est donc engendré par les idéaux premiers de norme ≤ 13 , c'est-à-dire 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.

Comme $N_{K/\mathbf{Q}}(\alpha) = -2$, l'idéal $\mathcal{P}_2$ est principal. De même, comme $N_{K/\mathbf{Q}}(1 + \alpha) = -3$, l'idéal $\mathcal{P}_3$ est principal. Comme $N_{K/\mathbf{Q}}(2 - \alpha) = -30 = -2.3.5$, l'idéal $\mathcal{P}_5$ est principal. Comme $N_{K/\mathbf{Q}}(1 + 2\alpha) = 65 = 13.5$, l'idéal $\mathcal{P}_5\mathcal{P}_{13}$ est principal, donc $\mathcal{P}_{13}$ est principal. Comme $N_{K/\mathbf{Q}}(1 - 2\alpha) = -63 = -3^2.7$, l'idéal $\mathcal{P}_7$ est principal. Donc le groupe des classes 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* 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.

On a $|\overline{\alpha}| \geq M(\alpha)^{1/d} \geq c_L^{1/d} \geq 1 + \log(c_L)/d$.

2. Quels sont les entiers algébriques α tels que $M(\alpha) = 1$?

Ce sont les entiers α tel que $|\alpha_i| = 1$ pour tout i . Alors α est un entier algébrique de norme absolue 1 ou -1 , c'est donc une unité. Par le théorème des unités, c'est une racine de l'unité.

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.

On a alors $M(\alpha) \geq N_{K/\mathbf{Q}}(\alpha) \geq 2$, puisque 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 $F_p \equiv F \pmod{p}$.

Les racines de F_p sont des entiers algébriques permutés par le groupe de Galois, si bien que F_p est à coefficients rationnels et entiers algébriques, et donc à coefficients entiers.

Soit K un corps de décomposition de F . Soit $\mathcal{P}$ un idéal premier de $\mathcal{O}_K$ au dessus de p . La substitution de Frobenius en $\mathcal{P}$, donnée par $x \mapsto x^p$ permute les racines de la réduction $\tilde{F}$ modulo p de F . Elle transforme les racines de $\tilde{F}$ en les racines de la réduction $\tilde{F}_p$ modulo p de F_p , qui a donc les mêmes racines que $\tilde{F}$. On a donc $\tilde{F} = \tilde{F}_p$.

5. En déduire que p^d divise $\mathcal{R}(F, F_p)$, puis que p^{2d} divise le discriminant Δ_p de FF_p .

Posons $F = F_p - pG$ dans $\mathbf{Z}[X]$. On a $\mathcal{R}(F, F_p) = \prod_{i=1}^d F_p(\alpha_i) = \prod_{i=1}^d (F(\alpha_i) + pG(\alpha_i)) = p^d \prod_{i=1}^d G(\alpha_i)$. D'où la divisibilité cherchée. On a $\Delta_p = \mathcal{R}(FF_p, (FF_p)') = \mathcal{R}(FF_p, FF_p' + F'F_p) = \mathcal{D}_F \mathcal{R}(F, F_p)^2 \mathcal{D}_{F_p}$, d'où p^{2d} divise Δ_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).

On écrit Δ_p comme le carré du Vandermonde $2d \times 2d$ associé aux racines de FF_p . Les colonnes de cette matrice sont de la forme $(\alpha_i^j)_{0 \leq j \leq 2d-1}$ (cas 1) ou $(\alpha_i^{pj})_{0 \leq j \leq 2d-1}$ (cas p). Dans le cas 1, la norme hermitienne d'une telle colonne est $\leq (2d)^{1/2}$ si $|\alpha_i| \leq 1$ et $\leq (2d|\alpha_i|^{4d})^{1/2}$ sinon. Dans le cas p , elle $\leq (2d)^{1/2}$ si $|\alpha_i| \leq 1$ et $\leq (2d|\alpha_i|^{4dp})^{1/2}$ sinon. Ainsi, par l'inégalité d'Hadamard, on en déduit le résultat.

7. Montrer que F et F_p n'ont pas de racine commune.

Si F et F_p ont une racine commune α_i , il existe j tel que $\alpha_i = \alpha_j^p$. Il existe σ dans le groupe de Galois G d'un corps de décomposition de F tel que $\sigma(\alpha_j) = \alpha_i$. On a alors

$\sigma(\alpha_j) = \alpha_j^p$. Soit k l'ordre de σ dans G . On a $\alpha_j = \sigma^k(\alpha_j) = \alpha_j^{p^k}$. Donc α_j est une racine de l'unité. Donc α est une racine de l'unité, ce qui est absurde.

8. Montrer que $M(\alpha) \geq (\frac{p}{2d})^{1/(2p+2)}$ pour p assez grand.

Supposons F_p sans racines multiples. Comme F et F_p n'ont pas de racine commune, le discriminant Δ_p est non nul. Comme p^{2d} divise Δ_p , on a $|\Delta_p| \geq p^{2d}$. On a donc $p^{2d} \leq (2d)^{2d} M(\alpha)^{4d(p+1)}$ (voir ci-dessus). Il suffit d'élever à la puissance $\frac{1}{2d}$.

Si F_p a des racines multiples, il existe i, j tels que $\alpha_i^p = \alpha_j^p$. Donc le corps $K(\alpha_i, \alpha_j)$ contient une racine p -ème de l'unité. Comme il est de degré $\leq d(d-1)$ sur $\mathbf{Q}$, et qu'une racine p -ème de l'unité est de degré $p-1$, on a $p-1 \leq d(d-1)$.

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.)

Par le postulat de Bertrand, il existe des nombres premiers distincts p et p' dans l'intervalle $]3d, 12d[$. Si F_p et $F_{p'}$ ont des racines multiples, il existe i, j et k , avec $i \neq j$ et $i \neq k$ tels que $\alpha_i^p = \alpha_j^p$ et $\alpha_i^{p'} = \alpha_k^{p'}$. Alors α_j/α_k est une racine primitive pp' -ème de l'unité contenue dans le corps $K(\alpha_k, \alpha_j)$. Une telle racine est de degré $(p-1)(p'-1)$ sur $\mathbf{Q}$. On a donc $d(d-1) \geq (p-1)(p'-1)$, ce qui est absurde, puisque p et p' sont $> 3d$. On peut donc appliquer la minoration de $M(\alpha)$ pour p ou p' , disons p .

On a alors $M(\alpha) > (\frac{3d}{2d})^{1/(26d)} > ((3/2)^{1/26})^{1/d}$, c'est l'inégalité cherchée avec $c_D = (3/2)^{1/26}$.

Remarques : L'argument donné ici est dû à Dobrowolski. On peut le raffiner en utilisant plusieurs nombres premiers p et obtenir $M(\alpha) \geq 1 + \frac{1}{1200} (\frac{\log \log(d)}{\log(d)})^3$.

La mesure de Mahler de P peut encore s'écrire

$$M(P) = \exp\left(\int_0^1 \log(P(e^{2i\pi\theta})) d\theta\right).$$

En dehors des polynômes cyclotomiques, la plus petite mesure de Mahler connue est celle du polynôme de Lehmer $X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$. La conjecture de Lehmer est encore ouverte. La conjecture de Schinzel-Zassenhaus a été démontrée par V. Dimitrov en 2019, avec $c_{SZ} = \log 2/4$.