Devoir maison n^o 5

(corrigé)

Table des matières

1 Commentaires

Ce devoir est une adaptation du sujet de Mathématiques A de la Banque X-ENS, année 2019, filière MP. J'ai supprimé la première question, qui est une redite du cours (ce n'est pas la seule, vous me direz ; si j'ai laissé les autres, c'est qu'elles donnent un indice sur les intentions des questions qui suivent), ainsi que la dernière partie, afin que le devoir ne soit pas d'une longueur excessive.

Il manipule les polynômes minimaux de nombres algébriques, en montrant tout un tas de résultats indispensables pour quiconque voulant briller dans l'étude des polynômes irréductibles de $\mathbb{Q}[X]$ (qui, elle-même, est liée à l'étude des nombres algébriques sur $\mathbb{Q}$: très vaste sujet), à savoir :

- les racines **complexes** d'un polynôme **irréductible** sur $\mathbb{Q}$ sont toutes **simples** (cela se généralise aussi aux polynômes irréductibles sur un corps fini, mais la démonstration est de nature totalement différente) ;
- les racines **rationnelles** d'un polynôme **unitaire à coefficients entiers** sont des **entiers** (et on a même mieux que cela : des relations de divisibilité entre les coefficients de ce polynôme, et ces racines, permettant de les déterminer par recensement exhaustif) ;
- le théorème de Kronecker : si un polynôme **unitaire** à coefficients **entiers**, **irréductible**, a toutes les racines sont de module 1, alors ces racines sont des **racines de l'unité** ;
- la démonstration de ce dernier théorème nécessite en particulier de montrer que si $\alpha_1, \dots, \alpha_n$ sont les **racines** d'un tel polynôme, alors $\sum_{i=1}^{n} \alpha_i^k$ est un **entier** pour tout $k \in \mathbb{N}$ (cela ne va pas du tout de soi, sauf pour $k = 0$ et $k = 1$!) ; il existe d'autres démonstrations que celle du sujet, passant par les matrices compagnons ou des algorithmes élémentaires exprimant ces sommes (appelées **sommes de Newton**) à l'aide des coefficients du polynôme ; c'est d'ailleurs implicitement ce que permet la démonstration du sujet, si l'on y regarde bien ;
- si p est **un nombre premier**, alors p divise le **coefficient binomial** $\binom{p}{k}$ pour tout $k \in [\![1, p-1]\!]$, ce qui est souvent un lemme préfigurant le *rêve du débutant* : l'application $x \mapsto x^p$ est additive sur tout anneau contenant $\mathbb{Z}/p\mathbb{Z}$ (c'est **l'automorphisme de Frobenius**) ;
- les **polynômes cyclotomiques** Φ_n, définis comme les polynômes unitaires dont les racines complexes sont exactement les racines primitives n^{es} de l'unité, sont à coefficients entiers et irréductibles dans $\mathbb{Q}[X]$ (rien de tout cela n'est évident).

On finit par quelques manipulations sur les polynômes réciproques, intéressantes sans être au cœur des mathématiques avancées. Le sujet se termine par quelques curiosités sur les **nombres de Salem**, dont le problème initial donnait quelques exemples de degré 4 en quatrième partie.

Bref, voici un long devoir riche en enseignements ! On se gardera bien de l'oublier aussitôt traité.

Toutes les propriétés des polynômes cyclotomiques découlent de la relation fondamentale :

$$X^n - 1 = \prod_{d|n} \Phi_d,$$

à savoir impérativement démontrer lorsqu'on a affaire à ces polynômes. Cette identité se démontre suivant une idée proche de la relation : $n = \sum_{d|n} \varphi(d)$.

On remarquera, tout au long de ce devoir, que l'on peut se passer systématiquement de l'expression explicite des racines primitives de l'unité avec la forme exponentielle. Il importe seulement de savoir que l'ensemble des racines n^{es} est un groupe cyclique (ce qui vaut dans n'importe quel corps), et qu'une racine primitive n^{e} z donne toutes les autres en calculant z^k pour tous entiers k premiers avec n. Ainsi les polynômes cyclotomiques sont des objets purement formels, qu'on pourrait manipuler en remplaçant $\mathbb{C}$ par n'importe quel corps.

La beauté de la relation ci-dessus, et du fait que les polynômes cyclotomiques soient à coefficients entiers, est qu'elle est universelle. Partant de celle-ci, on peut la réduire modulo n'importe quel entier n, et (à quelques précautions près) toutes les relations entre polynômes cyclotomiques restent valables modulo n. En particulier, on peut démontrer que, sauf si p divise n, les racines de $\overline{\Phi}_n$ dans $\mathbb{Z}/p\mathbb{Z}$ sont exactement les éléments d'ordre n dans $(\mathbb{Z}/p\mathbb{Z})^\times$. N'est-il pas surprenant qu'un objet construit à partir des éléments d'ordre n dans $\mathbb{C}^*$ puisse permettre de calculer les éléments d'ordre n dans des anneaux qui n'ont, *a priori*, aucun rapport avec $\mathbb{C}$? Un seul objet, à savoir Φ_n, qui permet d'avoir les éléments d'ordre n de tous les anneaux $\mathbb{Z}/p\mathbb{Z}$ (à un nombre fini d'exceptions près, dont je ne parlerai pas pour éviter d'alourdir le propos) ? C'est cette universalité des propriétés des polynômes à coefficients entiers qui les rend si essentiels aux mathématiques (cette idée est encore exploitée en mathématiques contemporaines, *via* les schémas en groupe et autres objets très sophistiqués).

C'est une idée utilisée pour l'une des démonstrations classiques du théorème de la progression arithmétique de Dirichlet dans un cas particulier : si $n \in \mathbb{N} \setminus \{0\}$, alors il existe une infinité de nombres premiers p tels que : $p \equiv 1 \bmod n$. Dans les grandes lignes, l'idée est de produire un élément d'ordre n dans $(\mathbb{Z}/p\mathbb{Z})^\times$ pour une infinité de nombres premiers p (puisque dans ce cas, par le théorème de Lagrange, n divise $p-1$). Pour ce faire, il suffit de noter que si $a \in \mathbb{Z}$ et si p est un nombre premier divisant $\Phi_n(a)$ (il faut pour cela choisir a de sorte que $\Phi_n(a) \neq \pm 1$, ce qui est possible puisque Φ_n tend vers l'infini en l'infini), alors $\overline{\Phi_n(a)} = \bar{0}$ dans $\mathbb{Z}/p\mathbb{Z}$, donc a est d'ordre n dans $(\mathbb{Z}/p\mathbb{Z})^\times$ comme toutes les racines de $\overline{\Phi_n}$ (à une subtilité près dont je ne parle pas), et donc $n \equiv 1 \bmod p$. Si l'on choisit convenablement a, on s'assure que procédé de construction permet de fabriquer une suite strictement croissante de nombres premiers p vérifiant cette congruence.

Les polynômes cyclotomiques apparaissent dans bien d'autres considérations encore. Il serait vain d'en faire l'inventaire. Un dernier exemple d'utilisation : comme Φ_n est de degré $\varphi(n)$ (facile à démontrer, si l'on a compris ce qu'est μ_n), et que c'est le polynôme minimal de $e^{\frac{2i\pi}{n}}$ (c'est en effet une racine primitive de l'unité), on sait donner une condition nécessaire et suffisante simple sur n pour que $e^{\frac{2i\pi}{n}}$ soit solution d'une équation polynomiale à coefficients rationnels et de degré au plus 4 (cela revient à résoudre $\varphi(n) = k$ pour tout $k \in [\![1,4]\!]$), et par extension on sait en déduire une condition nécessaire et suffisante simple sur n pour que $\cos\left(\frac{2\pi}{n}\right)$ soit solution d'une équation polynomiale de degré au plus 2 (pourquoi ?). Cela tombe bien, puisque vous savez résoudre une telle équation. On retrouve alors que, hormis les angles remarquables que vous connaissez depuis longtemps, on sait aussi calculer, uniquement à l'aide d'une racine carrée, et de sommes, produits et quotients de rationnels : $\cos\left(\frac{2k\pi}{5}\right)$, et il n'y en a pas d'autres (si l'on s'autorise plusieurs racines carrées, ou des racines cubiques, etc., il suffit de changer la condition recherchée sur $\varphi(n) = \deg(\Phi_n)$).

En résumé : dès qu'il est question de polynômes irréductibles dans $\mathbb{Q}[X]$, il y a une probabilité non négligeable de croiser des polynômes cyclotomiques.

Ce qu'on retiendra en bref. Propriétés de base des polynômes minimaux. Les racines d'un polynôme irréductible sont simples. Théorème de Kronecker. Sommes de Newton. Automorphisme de Frobenius $x \mapsto x^p$. Polynômes cyclotomiques : coefficients entiers, irréductibilité, relation $X^n - 1 = \prod_{d|n} \Phi_d$.

Questions faciles ou classiques à retravailler

— PREMIÈRE PARTIE : questions 1 à 4.(a) ;

— DEUXIÈME PARTIE : questions 6 et 7.(a), question 9, question 10, question 12.(a) ;

— TROISIÈME PARTIE : questions 14 et 15.

2 Corrigé

PREMIÈRE PARTIE

1. Si α est de degré 1, alors son polynôme minimal, qui est unitaire et annule α, est $X - \alpha$, donc : $\alpha \in \mathbb{Q}$. Réciproquement, si : $\alpha \in \mathbb{Q}$, alors $X - \alpha \in \mathbb{Q}[X]$ est annulateur de α, donc π_α divise $X - \alpha$. Pour des raisons de degré : $\pi_\alpha = X - \alpha$, et α est de degré 1.

2. (a) Soient $A, B \in \mathbb{Q}[X]$ unitaires tels que : $\pi_\alpha = AB$. On a : $A(\alpha)B(\alpha) = \pi_\alpha(\alpha) = 0$ donc, par exemple : $A(\alpha) = 0$, d'où : $A \in I(\alpha) = \pi_\alpha\mathbb{Q}[X]$, c'est-à-dire : $\pi_\alpha \mid A$. Or A divise aussi π_α, donc ils sont associés et unitaires, c'est-à-dire : $A = \pi_\alpha$. Ainsi, si π_α est produit de deux polynômes de $\mathbb{Q}[X]$, l'un des deux lui est associé, ce qui montre que π_α est irréductible.

> **Questions à se poser, réflexes à acquérir.**
> — Si l'on n'avait pas défini π_α comme le plus petit élément de $I(\alpha)$ au sens de la relation de divisibilité, mais au sens du degré, comment aurait-on conclu ?
> — Pourquoi deux polynômes associés et unitaires sont égaux ? Il est important de le comprendre car cet argument revient souvent.

(b) Puisque P annule z, ce nombre est algébrique et donc π_z divise P. Comme : π_z et P sont irréductibles, ce n'est possible que s'ils sont associés. Or ces deux polynômes sont unitaires, donc on a : $P = \pi_z$.

Remarque. Une conséquence de ceci est que si w est une racine de π_z, alors : $\pi_w = \pi_z$. Autrement : un polynôme minimal est « le polynôme minimal de toutes ses racines ».

> **Questions à se poser, réflexes à acquérir.**
> — Vérifier de ce que dit la remarque : quel rapport avec ce qui précède ?
> — Pourquoi l'irréductibilité de π_z et P, et la relation de divisibilité, impliquent qu'ils sont associés ? S'assurer d'avoir compris l'argument. Si on ne le comprend pas : essayer de le comprendre dans le cas de nombres premiers se divisant mutuellement.

3. (a) Soit α une racine commune de A et B. Alors α est algébrique sur $\mathbb{Q}$, et comme A et B appartiennent à $I(\alpha)$, on a les relations de divisibilité : $\pi_\alpha \mid A$, et : $\pi_\alpha \mid B$. Ainsi A et B admettent un diviseur irréductible en commun, ce qui démontre qu'ils ne sont pas premiers entre eux.

> **Questions à se poser, réflexes à acquérir.**
> — Pourquoi ne dit-on pas sobrement que $X - \alpha$ est un diviseur commun irréductible de A et B ?
> — Est-ce que la relation « être premier avec » est invariante par extension de corps ? C'est-à-dire : si $K \subseteq L$ et si $(A, B) \in K[X]^2$, est-ce que A et B sont premiers entre eux, vus comme polynômes de $K[X]$, si et seulement s'ils le sont dans $L[X]$? Il y a de nombreuses façons de répondre à cette question, et la résolution de la question ci-dessus donne une piste. On peut se demander plus généralement si le pgcd dans $K[X]$ est égal au pgcd dans $L[X]$.

(b) Rappelons que si $P \in \mathbb{Q}[X]$ admet une racine double $z \in \mathbb{C}$, alors $P'(z) = 0$, donc par la question précédente P et P' ne sont pas premiers entre eux. Par contraposée : si P et P' sont premiers entre eux, alors les racines de P sont simples : c'est ce que nous allons donc démontrer dans le cas où P est irréductible.

Notons : $D = \text{pgcd}(P, P')$. Par définition du pgcd, D divise P, et comme ce polynôme est irréductible on a : $D = 1$, ou : $D = P$. Or le degré de D est inférieur ou égal à celui de P' (puisqu'il divise ce polynôme), donc strictement inférieur à celui de P. On en déduit : $D = 1$, ce qui suffit à démontrer que les racines de P sont simples par ce qui précède.

Autre démonstration. Comme P est irréductible, il est premier avec P' (en effet, un diviseur commun de P et P' est en particulier un diviseur de P, donc égal à 1 ou P à un inversible près ; mais le second cas est exclu parce que P ne peut pas diviser P' pour des raisons de degré). D'après le théorème de Bézout, il existe $(U, V) \in \mathbb{Q}[X]^2$ tel que : $UP + VP' = 1$. En évaluant en une racine z de P, on a : $V(z)P'(z) = 1$, donc : $P'(z) \neq 0$, ce qui prouve que z est une racine simple de P.

Autre démonstration. Si $z \in \mathbb{C}$ vérifie : $P(z) = P'(z) = 0$, alors d'une part P est le polynôme minimal de z, et d'autre part $P = \pi_z$ divise P' (puisque P' appartient à $I(z)$), ce qui est impossible pour une raison de degré. Ainsi P n'admet pas de racine au moins double.

Questions à se poser, réflexes à acquérir.

— Bien comprendre chaque démonstration et retenir sa préférée : c'est TRÈS important car ce résultat classique revient dès qu'on étudie des polynômes irréductibles hors de $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

— J'affirme que mon argument de degré, que je n'ai pas détaillé une seule fois (alors qu'il apparaît à chaque fois), n'est pas si trivial que cela. Il utilise une propriété de P et une autre de $\mathbb{Q}$: lesquelles ? Méditer par exemple sur $P = X^p + \bar{1} \in \mathbb{Z}/p\mathbb{Z}[X]$ et sa dérivée.

4. (a) Posons $\alpha = \dfrac{p}{q}$, où p et q sont deux entiers premiers entre eux, avec $q \geqslant 1$. Soit $P = X^n + a_{n-1}X^{n-1} + \ldots a_1X + a_0 \in \mathbb{Z}[X]$ un polynôme annulateur de α. On a :

$$q^n P\left(\alpha\right) = p^n + a_{n-1}p^{n-1}q + \ldots a_1pq^{n-1} + a_0q^n = 0,$$

donc, en réduisant modulo q cette égalité, on observe que q divise p^n. Puisque p et q sont premiers entre eux (et donc p^n et q également), cela entraîne : $q = 1$ et : $\alpha = p \in \mathbb{Z}$.

Questions à se poser, réflexes à acquérir.

— Vu que α est rationnel, on sait que π_α est de degré 1 ; pourquoi, pour autant, introduis-je un polynôme annulateur de degré quelconque ?

— Pourquoi est-il naturel de multiplier $P(\alpha)$ par q^n ? Qu'est-ce que cela permet de faire, qui aurait été inenvisageable avec l'égalité $P(\alpha) = 0$?

— Pourquoi est-il vrai que p^n et q sont aussi premiers entre eux ? Est-ce que, plus généralement, a et b sont premiers entre eux si et seulement si a^k et b^ℓ le sont, où k et ℓ sont des entiers naturels non nuls fixés ? (Penser à une caractérisation simple des entiers premiers entre eux, qui a l'avantage de faciliter la réflexion sur les puissances grâce au lemme d'Euclide ou au théorème de Gauß.)

(b) Soit $P \in \mathbb{Z}[X]$ unitaire tel que : $P(\alpha) = 0$. Comme π_α divise P, les racines de π_α sont des entiers algébriques. Or, π_α étant unitaire, les relations coefficients-racines et le théorème admis en introduction montrent que les coefficients de π_α sont des entiers algébriques. Comme ce sont des rationnels, la question 4.(a) montre que ce sont des entiers, d'où : $\pi_\alpha \in \mathbb{Z}[X]$.

5. (a) Soit $(a, b) \in \mathbb{Z}^2$ tel que : $\alpha^2 + a\alpha + b = 0$. On a, en conjuguant : $\bar{\alpha}^2 + a\bar{\alpha} + b = 0$. Comme α n'est pas réel (car les réels de module 1 sont 1 et -1 qui ne sont pas algébriques de degré 2), les nombres α et $\bar{\alpha}$ sont les deux racines distinctes de $X^2 + aX + b$. Donc : $b = \alpha\bar{\alpha} = 1$, et : $-a = \alpha + \bar{\alpha} = 2\text{Re}(\alpha)$. En particulier, on a : $|a| \leqslant 2|\alpha| = 2$. Le cas $a = \mp 2$ conduit à $\alpha = \pm 1$, qui est exclu. Donc : $a \in \{-1,0,1\}$, et selon les valeurs de a :

$$\alpha \in \left\{i, -i, j, -j, j^2, -j^2\right\},$$

qui sont tous des racines de l'unité : d'où le résultat.

Questions à se poser, réflexes à acquérir.
- Vérifier en détails le cas $a = \pm 2$, si vous n'êtes pas convaincus.
- Je n'ai pas détaillé comment on obtient les six valeurs possibles de α : le faire. Se souvenir que a donne la partie réelle de α, et que α est de module 1.

(b) On a : $\left|\frac{3+4i}{5}\right|^2 = \frac{9+16}{25} = 1$. Par ailleurs, le polynôme :

$$\left(X - \frac{3+4i}{5}\right)\left(X - \frac{3-4i}{5}\right) = X^2 - \frac{6}{5}X + 1 \in \mathbb{Q}[X]$$

annule $\frac{3+4i}{5}$, qui est donc algébrique. Le polynôme minimal π_α divise le polynôme ci-dessus, et comme $\frac{3+4i}{5}$ n'est pas rationnel on a nécessairement : $\pi_\alpha = X^2 - \frac{6}{5}X + 1$. Comme ce polynôme n'est pas à coefficients entiers, la question 4.(b) montre que α n'est pas un entier algébrique. En particulier, ce n'est pas une racine de l'unité.

Questions à se poser, réflexes à acquérir.
- Peut-on généraliser ceci et donner, pour tout $z \in \mathbb{C} \setminus \mathbb{R}$, son polynôme minimal sur $\mathbb{R}$?
- Pourquoi mentionner que $\frac{3+4i}{5}$ n'est pas rationnel ?

Deuxième partie

6. L'ensemble μ_n n'est autre que l'ensemble des générateurs de $\mathbb{U}_n$. Notons $s(\omega)$ l'ordre d'une racine de l'unité, c'est-à-dire l'ordre du sous-groupe de $\mathbb{U}$ qu'elle engendre. Par le théorème de Lagrange, on sait que si : $\omega \in \mathbb{U}_n$, alors $s(\omega)$ divise n, et que réciproquement : si $\omega \in \mathbb{U}$ est d'ordre d, avec d divisant n, alors $\omega^n = 1$ (caractérisation de l'ordre d'un élément) et donc : $\omega \in \mathbb{U}_n$. Ainsi : $\{\omega \in \mathbb{U}_n \mid s(\omega) = d\} = \mu_d$ si d divise n (tandis que c'est un ensemble vide sinon), et :

$$\mathbb{U}_n = \bigsqcup_{d|n} \{\omega \in \mathbb{U}_n \mid s(\omega) = d\} = \bigsqcup_{d|n} \mu_d,$$

On en déduit immédiatement :

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) = \prod_{d|n} \prod_{\omega \in \mu_d} (X - \omega) = \prod_{d|n} \Phi_d.$$

Questions à se poser, réflexes à acquérir.
- Le raisonnement, ainsi que le résultat, devrait faire penser à un exercice de travaux dirigés. Lequel ?
- Quel est le degré de Φ_d ? Que donne l'identité démontrée, quand on compare les degrés ?
- Ne peut-on pas écrire cette identité, au moins formellement, comme un produit de convolution de fonctions arithmétiques ? (Ce qui y fait penser est le produit indexé par les diviseurs.) Ne peut-on pas en déduire, grâce à la fonction μ de Möbius, une expression de Φ_n pour tout n ? Est-elle utile pour le calcul pratique ?

7. (a) Soit $k \in \mathbb{N} \setminus \{0\}$. Les diviseurs de p^k sont les entiers de la forme p^j avec $j \in [\![1, k]\!]$. Donc :

$$X^{p^{k-1}} - 1 = \prod_{j=1}^{k-1} \Phi_{p^j}, \quad \text{et :} \quad X^{p^k} - 1 = \prod_{j=1}^{k} \Phi_{p^j} = \Phi_{p^k} \prod_{j=1}^{k-1} \Phi_{p^j} = \Phi_{p^k} \cdot (X^{p^{k-1}} - 1),$$

d'où :

$$\Phi_{p^k} = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = \sum_{j=0}^{p-1} X^{jp^{k-1}} = X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + \cdots + X^{p^{k-1}} + 1.$$

Questions à se poser, réflexes à acquérir.

— Ne pouvait-on pas obtenir Φ_{p^k} comme proposé dans mes commentaires de la question précédente, avec la fonction μ de Möbius, étant donné qu'elle a une expression très simple en p^j ?

— Obtenir d'abord Φ_p et Φ_{p^2} pour comprendre pourquoi la démonstration proposée est plutôt naturelle.

— Ne pouvait-on pas obtenir Φ_p directement à partir de sa définition, et du fait que les éléments d'ordre p premier soient faciles à décrire ?

— On remarque que l'on a : $\Phi_{p^k} = \Phi_p(X^{p^{k-1}})$. Ne pouvait-on pas le prédire ? N'a-t-on pas une relation simple entre les éléments de μ_p et ceux de μ_{p^k} ? Proposer, alors, une autre démonstration que celle ci-dessus.

(b) On a évidemment : $\Phi_1 = X - 1$. En appliquant la question précédente, on a ensuite :

$$\Phi_2 = X + 1, \quad \Phi_3 = X^2 + X + 1, \quad \Phi_4 = \Phi_{2^2} = X^2 + 1, \quad \Phi_5 = X^4 + X^3 + X^2 + X + 1,$$

et il reste à obtenir Φ_6. Nous proposons deux façons de l'obtenir. La seconde permet de comprendre en quoi Φ_6 peut s'étudier de manière purement formelle en raisonnant sur les ordres des éléments, en oubliant totalement l'origine complexe de ses racines.

Premier calcul de Φ_6. On a :

$$\mathbb{U}_6 = \left\{ \left(e^{\frac{2i\pi}{6}}\right)^k \mid k \in [\![0,5]\!] \right\} = \left\{ \left(e^{\frac{i\pi}{3}}\right)^k \mid k \in [\![0,5]\!] \right\} = \{1, -j, -\bar{j}, -1, j, \bar{j}\}.$$

Comme : $(\pm 1)^2 = 1$, et : $j^3 = \bar{j}^3 = 1$, les racines primitives sixièmes de l'unité sont $-j$ et $-\bar{j}$. Donc :

$$\Phi_6 = (X + j)(X + \bar{j}) = X^2 + 2\mathrm{Re}(j)X + j\bar{j} = X^2 - X + 1.$$

Deuxième calcul de Φ_6. On va montrer : $\Phi_6 = \Phi_3(-X)$, en comparant les éléments de μ_3 et de μ_6. Soit $z \in \mathbb{U}$. Notons que l'on a :

$$z \in \mu_6 \iff z^3 = -1 \text{ et } z^2 \neq 1.$$

En effet, z est d'ordre *divisant* 6 si et seulement si : $z^6 = 1$, si et seulement si : $z^3 = 1$, ou : $z^3 = -1$. Le premier cas se produit si et seulement si z est d'ordre divisant 3. Donc, par élimination, z est d'ordre 2 ou 6 si et seulement si : $z^3 = -1$. La condition $z^2 \neq 1$ permet d'exclure l'ordre 2. Comme $(-1)^3 = -1$, on en déduit :

$$z \in \mu_6 \iff (-z)^3 = 1 \text{ et } z \neq \pm 1 \iff -z \in \mathbb{U}_3 \text{ et } z \notin \{-1,1\} \iff -z \in \mu_3.$$

Pour la dernière équivalence, on utilise le fait que les éléments de $\mathbb{U}_3$ soient d'ordre 1 ou 3, l'ordre 1 étant exclu puisque $z \neq 1$. Ainsi l'application $z \mapsto -z$ est une bijection de μ_6 dans μ_3, de réciproque elle-même, ce dont on déduit :

$$\Phi_6 = \prod_{\omega \in \mu_6} (X - \omega) = \prod_{\omega \in \mu_3} (X + \omega) = (-1)^2 \prod_{\omega \in \mu_3} (-X - \omega) = \Phi_3(-X) = X^2 - X + 1.$$

On récapitule ce qu'on a trouvé ci-dessous :

n	1	2	3	4	5	6
Φ_n	$X-1$	$X+1$	X^2+X+1	X^2+1	$X^4+X^3+X^2+X+1$	X^2-X+1

Questions à se poser, réflexes à acquérir.

— Vérifier la description de $\left(e^{\frac{i\pi}{3}}\right)^k$ selon les valeurs de k. L'appui d'un DESSIN est le bienvenu.

— Trouver autrement les racines primitives sixièmes de l'unité, grâce au résultat figurant dans votre cours sur les générateurs du groupe cyclique $\mathbb{Z}/6\mathbb{Z}$.

— Peut-on généraliser l'équivalence entre $z \in \mu_6$ et $-z \in \mu_3$? En remplaçant 6 par un entier n quelconque ? Ou faut-il faire un ajustement ? Partant de là, déduire une relation entre Φ_{2n} et Φ_n.

— Pourquoi le deuxième calcul de Φ_6 se prête mieux aux généralisations à un corps quelconque ? (C'est-à-dire : au cas où l'on remplace les racines primitives n^{es} de l'unité par les éléments d'ordre n dans le groupe multiplicatif d'un corps quelconque, et où l'on définit les Φ_n semblablement.)

— Déterminer Φ_n pour tout $n \leqslant 104$ grâce à ce qui précède. Pourquoi m'arrêté-je à $n = 105$?

8. (a) On a : $\Phi_1 = X - 1$, donc : $\Phi_1(0) = -1$. Par ailleurs on déduit de la question 6 que pour tout $n \in \mathbb{N} \setminus \{0\}$, on a : $\prod_{d|n} \Phi_d(0) = -1$. On en déduit immédiatement, par récurrence forte sur n :

$$\Phi_n(0) = \begin{cases} 1 & \text{si} \quad n \geqslant 2, \\ -1 & \text{si} \quad n = 1. \end{cases}$$

Questions à se poser, réflexes à acquérir.

— Détailler la récurrence forte si vous n'êtes pas convaincus.

— Qu'est-ce que cette question enseigne sur le produit $\prod_{\omega \in \mu_n} \omega$ ou sur $\sum_{\substack{k=1 \\ \text{pgcd}(k,n)=1}}^{n} k$? Aurait-on su le démontrer directement, quitte à ce que ce soit uniquement sur quelques cas particuliers ?

(b) On a d'abord : $\Phi_1(1) = 0$. Ensuite, si n est de la forme p^k avec p premier et $k \in \mathbb{N} \setminus \{0\}$, alors la question 7.(a) montre que : $\Phi_{p^k} = p$. Déduisons-en le cas où n est de la forme $p_1^{k_1} \dots p_s^{k_s}$, où $s \geqslant 2$, les p_i sont des nombres premiers distincts et k_i des entiers naturels non nuls. D'après la question 6, après simplification par $X - 1 = \Phi_1$ on a :

$$\sum_{k=0}^{n-1} X^k = \prod_{\substack{d|n \\ d \neq 1}} \Phi_d.$$

On évalue en 1. On obtient : $n = \prod_{\substack{d|n \\ d \neq 1}} \Phi_d(1)$. Notons A l'ensemble des diviseurs de n de la forme p_i^k avec $i \in [\![1, s]\!]$ et $k \in [\![1, k_i]\!]$. En utilisant le fait que $\Phi_{p_i^k}(1) = p_i$ pour tout $i \in [\![1, s]\!]$ et tout $k \in \mathbb{N} \setminus \{0\}$, on obtient :

$$n = \prod_{\substack{d \in A \\ d \neq 1}} \Phi_d(1) \times \prod_{\substack{d|n \\ d \notin A \\ d \neq 1}} \Phi_d(1) = \prod_{i=1}^{s} \prod_{k=1}^{k_i} \Phi_{p_i^k} \times \prod_{\substack{d|n \\ d \notin A \\ d \neq 1}} \Phi_d(1) = \prod_{i=1}^{s} \prod_{k=1}^{k_i} p_i \times \prod_{\substack{d|n \\ d \notin A \\ d \neq 1}} \Phi_d(1) = n \times \prod_{\substack{d|n \\ d \notin A \\ d \neq 1}} \Phi_d(1),$$

et donc :

$$1 = \prod_{\substack{d|n \\ \rho(d) \geqslant 2}} \Phi_d(1),$$

où l'on note $\rho(d)$ le nombre de diviseurs premiers de d. On en déduit facilement, par récurrence forte sur le nombre de diviseurs premiers de n (ou sur n), que :

$$\Phi_n(1) = \begin{cases} p & \text{si } n \text{ est de la forme } p^k,\ p \text{ premier},\ k \in \mathbb{N} \setminus \{0\}, \\ 1 & \text{sinon.} \end{cases}$$

Questions à se poser, réflexes à acquérir. Faire la récurrence forte que j'ai omise.

9. On a : $X^n - 1 = \Phi_n \prod_{\substack{d|n \\ d<n}} \Phi_d$. Donc Φ_n est le quotient (dans $\mathbb{Q}[X]$) dans la division euclidienne de $X^n - 1$ par $\prod_{\substack{d|n \\ d<n}} \Phi_d$. Or l'algorithme usuel de la division euclidienne permet d'observer que le quotient d'un polynôme de $\mathbb{Z}[X]$ par un polynôme UNITAIRE de $\mathbb{Z}[X]$ est encore un polynôme de $\mathbb{Z}[X]$. Une récurrence forte sur n montre alors que : $\Phi_n \in \mathbb{Z}[X]$.

> **Questions à se poser, réflexes à acquérir.** Pourquoi la division euclidienne d'un polynôme de $\mathbb{Z}[X]$ par un autre polynôme de $\mathbb{Z}[X]$ donne un quotient dans $\mathbb{Z}[X]$, à condition que le diviseur soit unitaire ? Est-ce aussi le cas du reste ? (La poser comme vous le feriez à la main, et raisonner par récurrence sur le degré du dividende.)

10. (a) Soit $z \in \mathbb{C}$ tel que : $|z| < 1$. Pour tout $i \in [\![1, n]\!]$, on a : $|z_i z| = |z| < 1$, donc la série géométrique $\sum_{k\geqslant 0}(z_i z)^k$ converge. En tant que somme de séries convergentes, la série $\sum_{k\geqslant 0} a_k z^k$ converge : d'où le résultat.

(b) On montre sans difficulté que la dérivée logarithmique d'un polynôme non nul Q, définie par : $D(Q) = \dfrac{Q'}{Q}$, est additive :

$$\forall (Q_1, Q_2) \in \mathbb{C}[X]^2, \quad D(Q_1 Q_2) = D(Q_1) + D(Q_2).$$

Donc : $\dfrac{P'}{P} = D(P) = \sum_{i=1}^{n} \dfrac{1}{X - z_i}$. On a maintenant, par linéarité, et parce qu'on reconnaît des sommes géométriques de raisons strictement inférieures à 1 :

$$f(z) = \sum_{k=0}^{+\infty} \sum_{i=1}^{n} z_i^k z^k = \sum_{i=1}^{n} \sum_{k=0}^{\infty} z_i^k z^k = \sum_{i=1}^{n} \frac{1}{1 - z_i z} = \sum_{i=1}^{n} \frac{1}{z} \frac{1}{\frac{1}{z} - z_i} = \frac{1}{z} \frac{P'\left(\frac{1}{z}\right)}{P\left(\frac{1}{z}\right)}$$

d'où la relation cherchée.

> **Questions à se poser, réflexes à acquérir.**
> — Vérifier la formule d'additivité de la dérivée logarithmique. Notamment, s'assurer qu'elle est purement formelle et ne nécessite pas de réellement recourir au logarithme (il vaut mieux, puisque les polynômes sont à coefficients complexes !). Est-ce que la dérivée logarithmique est linéaire ?
> — Quel est le noyau du morphisme de groupes induit par la dérivée logarithmique ? Et son image ? Pourriez-vous donner des antécédents de fractions rationnelles simples ? Cela peut être utile pour déterminer *en un instant* des fonctions vérifiant $\frac{f'}{f} = \alpha$, $\frac{f'(x)}{f(x)} = \frac{\beta}{x-\gamma}$, etc. Certains collègues procèdent ainsi pour résoudre les équations différentielles linéaires d'ordre raisonnable.
> — Réfléchir aux cas où il est plus intéressant de passer par cette dérivée logarithmique plutôt que par la dérivée.

(c) Pour tout $z \in \mathbb{C}^*$ tel que : $|z| < 1$, on a d'après la question précédente :

$$z^n P\left(\frac{1}{z}\right) f(z) = z^{n-1} P'\left(\frac{1}{z}\right).$$

Voyons comment en déduire le résultat. Nous rédigeons d'abord une solution utilisant l'élégante théorie des séries entières, puis une autre qui la contourne (en attendant de l'aborder plus tard cette année). Posons d'abord : $P = b_0 X^n + b_1 X^{n-1} + \cdots + b_{n-1} X + b_n$, avec : $(b_0, \ldots, b_n) \in \mathbb{Z}^{n+1}$ tel que $b_0 = 1$, et notons que l'on a : $X^n P\left(\frac{1}{X}\right) = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0$, ce qui montre que $X^n P\left(\frac{1}{X}\right)$ est un polynôme (à coefficients entiers).

Avec la théorie des séries entières. La fonction $z \mapsto z^n P\left(\frac{1}{z}\right) f(z)$, définie sur le disque unité ouvert, est le produit de la fonction polynomiale $z \mapsto z^n P\left(\frac{1}{z}\right)$ par la fonction développable en

série entière f, donc c'est aussi une fonction développable en série entière, son développement étant donné par un produit de Cauchy :

$$z^n P\left(\frac{1}{z}\right) f(z) = \sum_{k=0}^{+\infty} c_k z^k,$$

avec : $\forall k \in \mathbb{N}$, $c_k = \sum_{i=0}^{\min(k,n)} b_i a_{k-i}$, et $z \in \mathbb{C}^*$ tel que : $|z| < 1$. Mais on a aussi, par ce qui précède, avec la même condition sur z :

$$z^n P\left(\frac{1}{z}\right) f(z) = z^{n-1} P'\left(\frac{1}{z}\right) = \sum_{k=0}^{n-1} b_k (n-k) z^k.$$

On en déduit, pour tout $z \in \mathbb{C}^*$ tel que $|z| < 1$:

$$\sum_{k=0}^{+\infty} c_k z^k = \sum_{k=0}^{n-1} b_k (n-k) z^k.$$

Par continuité d'une fonction développable en série entière, cette égalité est valable aussi en $z = 0$. Par unicité des coefficients :

$$\forall k \in \mathbb{N}, \quad c_k = \begin{cases} b_k(n-k) & \text{si} \quad k \leqslant n, \\ 0 & \text{si} \quad k > n. \end{cases}$$

Tout ce qui importe, pour la suite, est qu'on ait : $\forall k \in \mathbb{N}$, $c_k \in \mathbb{Z}$. L'expression explicite de c_k, où l'on isole $a_k b_0 = a_k$, permet alors d'écrire :

$$\forall k \in \mathbb{N}, \quad a_k = c_k - \sum_{i=1}^{\min(k,n)} b_i a_{k-i}.$$

On rappelle que les b_i sont tous entiers, ainsi que c_k. Cette relation de récurrence permet alors d'en déduire aisément, par récurrence sur k, que a_k est entier pour tout $k \in \mathbb{N}$.

Avec un développement limité. C'est le même raisonnement, à ceci près que, à défaut d'avoir vu la théorie des séries entières, vous ne savez pas qu'on peut identifier les coefficients dans un « polynôme infini ». L'idée est de tronquer le développement pour ne plus avoir de somme à support infini. C'est un développement limité (comme son nom l'indique) qui le permet. Soient $N \in \mathbb{N}$ un entier plus grand que $n-1$ et z un nombre complexe au voisinage de 0. On a :

$$f(z) = \sum_{k=0}^{N} a_k z^k + \sum_{i=1}^{n} \sum_{k=N+1}^{+\infty} (z_i z)^k = \sum_{k=0}^{N} a_k z_k + \sum_{i=1}^{n} \frac{(z_i z)^{N+1}}{1 - z_i z} = \sum_{k=0}^{N} a_k z_k + \underset{z \to 0}{o}\left(z^N\right).$$

Par le même raisonnement que ci-dessus (mais en faisant des produits de sommes finies ! là est la différence), et en reprenant les mêmes notations, on a donc :

$$z^n P\left(\frac{1}{z}\right) f(z) = \sum_{k=0}^{N} c_k z^k + \underset{z \to 0}{o}\left(z^N\right),$$

et aussi : $z^n P\left(\frac{1}{z}\right) f(z) = \sum_{k=0}^{n-1} b_k (n-k) z^k$. Par unicité de la partie régulière d'un développement limité, on a : $\forall k \in [\![0, N]\!]$, $c_k = \begin{cases} b_k(n-k) & \text{si} \quad k \leqslant n \\ 0 & \text{si} \quad k > n \end{cases}$. Ceci vaut pour tout $N \in \mathbb{N}$. On peut alors reprendre le raisonnement comme dans le premier cas, pour en déduire que a_k est un entier relatif pour tout $k \in \mathbb{N}$.

Questions à se poser, réflexes à acquérir. Faire si besoin la récurrence omise.

11. (a) Comme z_i est de module 1 pour tout $i \in [\![1,n]\!]$, on a : $\forall k \in \mathbb{N}$, $|a_k| \leqslant n$. Or a_k est un entier pour tout $k \in \mathbb{N}$, donc : $\forall k \in \mathbb{N}$, $a_k \in [\![-n,n]\!]$. Par conséquent :

$$(a_k, a_k+1, \dots, a_{k+n}) \in [\![-n,n]\!]^{n+1}.$$

L'application $k \mapsto (a_k, a_k+1, \dots, a_{k+n})$ de $\mathbb{N}$ dans $[\![-n,n]\!]^{n+1}$ ne peut donc pas être injective. On en déduit l'existence de k et ℓ entiers naturels distincts, tels que $k < \ell$ (quitte à échanger k et ℓ) et :

$$(a_k, a_k+1, \dots, a_{k+n}) = (a_\ell, a_\ell+1, \dots, a_{\ell+n}),$$

d'où le résultat : $\forall i \in [\![0,n]\!]$, $a_{k+i} = a_{\ell+i}$.

Questions à se poser, réflexes à acquérir. Noter là l'efficacité d'interpréter en termes d'applications des prédicats de la forme $\exists \bigstar$, $\spadesuit = \clubsuit$, etc. Selon les cas, cela découle de l'injectivité ou non, ou de la surjectivité, d'une certaine application. Procéder ainsi permet d'utiliser des théorèmes sur les structures (ensembles, ou groupes, anneaux, corps le cas échéant). On a déjà illustré la stratégie pour montrer qu'un anneau commutatif de cardinal fini est intègre si et seulement s'il est un corps, ou pour caractériser l'ordre d'un élément en termes de divisibilité, par exemple.

(b) Par linéarité, il suffit de vérifier l'égalité lorsque F est un polynôme de la forme X^s. Or :

$$\sum_{i=1}^{n} z_i^s \left(z_i^\ell - z_i^k\right) = \sum_{i=1}^{n} z_i^{s+\ell} - \sum_{i=1}^{n} z_i^{s+k} = a_{s+\ell} - a_{s+k} = 0,$$

d'où le résultat.

Questions à se poser, réflexes à acquérir. Lorsqu'on doit montrer un résultat pour tout polynôme, songer au fait que raisonner sur la base canonique, puis par linéarité, allège considérablement les calculs !

(c) Comme P est irréductible, le pgcd de P et P', qui est un diviseur strict de P (pour une raison de degré déjà évoquée dans la question 3), vaut 1. Donc les racines complexes de P sont distinctes par la question 3. Les relations obtenues dans la question précédente pour $F = X^s$ donnent, en prenant $s \in [\![0,n-1]\!]$:

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ z_1 & z_2 & \dots & z_n \\ \vdots & \vdots & & \vdots \\ z_1^{n-1} & z_2^n & \dots & z_n^{n-1} \end{pmatrix} \begin{pmatrix} z_1^\ell - z_1^k \\ z_2^\ell - z_2^k \\ \vdots \\ z_n^\ell - z_n^k \end{pmatrix} = 0.$$

Comme les z_i sont deux à deux distincts, la matrice de Vandermonde est inversible d'où : $\forall i \in [\![1,n]\!]$, $z_i^\ell = z_i^k$. D'où le résultat, après multiplication par z_i^{-k} : on a montré que pour tout polynôme unitaire de $\mathbb{Z}[X]$, irréductible dans $\mathbb{Q}[X]$ si toutes les racines sont de module 1, alors ce sont des racines de l'unité. Notons qu'on aurait pu, depuis la question 11.(a), prendre $i \in [\![0,n-1]\!]$ plutôt que $i \in [\![0,n]\!]$.

Remarque. On a démontré le théorème de Kronecker.

Questions à se poser, réflexes à acquérir.

— Peut-on alléger les hypothèses ? Si P n'est pas irréductible, le résultat reste-t-il vrai ?

— Est-ce que le résultat reste vrai pour un polynôme unitaire de $\mathbb{Q}[X]$ dont les racines sont de module 1 ? (Le sujet permet de répondre à cette question.) Pourquoi le caractère entier est-il crucial dans cette démonstration ?

12. (a) On a, par la formule du binôme de Newton :

$$(F+G)^p = \sum_{k=0}^{p} \binom{p}{k} F^k G^{p-k} = F^p + G^p + \sum_{k=1}^{p-1} \binom{p}{k} F^k G^{p-k}.$$

Montrons alors que pour tout $k \in [\![1, p-1]\!]$, le nombre premier p divise $\binom{p}{k}$. Nous proposons une autre démonstration, plus classique, que celle vue en travaux dirigés. Soit $k \in [\![1, p-1]\!]$. On a :

$$k!(p-k)!\binom{p}{k} = p! = p \cdot (p-1)!.$$

On en déduit que p divise $k!(p-k)!\binom{p}{k}$. Cependant il ne divise pas les entiers entre 1 et k (puisqu'ils lui sont tous strictement inférieurs par hypothèse sur k), donc par le lemme d'Euclide p ne divise pas $k!$. Par le même raisonnement, p ne divise pas $(p-k)!$. Toujours par le lemme d'Euclide, on en déduit que p divise $\binom{p}{k}$, ce qu'on voulait démontrer. On peut alors écrire, pour tout $k \in [\![1, p-1]\!]$, le coefficient binomial sous la forme : $\binom{p}{k} = p \cdot n_k$, avec $n_k \in \mathbb{N}$. Ensuite, en reprenant le calcul ci-dessus :

$$(F+G)^p = F^p + G^p + p\sum_{k=1}^{p-1} n_k F^k G^{p-k},$$

d'où le résultat en posant : $H = \sum_{k=1}^{p-1} n_k F^k G^{p-k}$, qui appartient à $\mathbb{Z}[X]$ en tant que somme de produit d'éléments de $\mathbb{Z}[X]$.

Remarque. On a implicitement montré que l'application $Q \mapsto Q^p$ est un morphisme de $(\mathbb{Z}/p\mathbb{Z}[X], +)$ dans lui-même. Remarquable ! C'est l'automorphisme de Frobenius.

Questions à se poser, réflexes à acquérir.

— Comprendre en quoi c'est le lemme d'Euclide qui permet d'affirmer que p ne divise pas $k!$ ni $(p-k)!$. Vérifier qu'il est en général faux de penser que n ne divise pas $k!$ pour tout $k < n$.

— On avait démontré : $(X+\bar{1})^p = X^p + \bar{1}$, en travaux dirigés, par une autre méthode. Cela donne le résultat voulu pour $F = X$ et $G = \bar{1}$. Pouvait-on adapter cette autre méthode pour avoir directement le résultat avec F et G quelconques ?

— La démonstration de la divisibilité de p par $\binom{p}{k}$ étant très classique : retenir sa démonstration préférée, parmi celles abordées.

(b) Puisque $z \in \mathbb{U}_n$ est racine de $X^n - 1 \in \mathbb{Z}[X]$, le nombre complexe z est un entier algébrique. Donc, par la question 4.(b), on a : $\pi_z \in \mathbb{Z}[X]$. Posons : $\pi_z = X^s + b_{s-1}X^{s-1} + \cdots + b_1 X + b_0$, avec $(b_0, \ldots, b_{s-1}) \in \mathbb{Z}^s$. On a, en utilisant la question 12.(a), étendue à la somme d'un nombre quelconque de polynômes (récurrence immédiate), l'existence d'un polynôme $G \in \mathbb{Z}[X]$ tel que :

$$\pi_z(X)^p = X^{sp} + b_{s-1}^p X^{p(s-1)} + \cdots + b_1^p X^p + b_0^p + pG(X).$$

Or, par le petit théorème de Fermat : $\forall k \in [\![0, s-1]\!]$, $b_k^p \equiv b_k \bmod p$. Donc il existe $G \in \mathbb{Z}[X]$ tel que :

$$\pi_z(X)^p = \pi_z\left(X^p\right) + pG(X).$$

Remarque. Pour tout polynôme de $\mathbb{Z}/p\mathbb{Z}[X]$, on a donc, en imitant ce raisonnement : $(P(X))^p = P(X^p)$.

(c) La dernière relation entraîne : $\pi_z\left(z^p\right) = pF(z)$. Puisque l'ensemble des entiers algébriques est un anneau d'après le théorème admis dans l'énoncé, $\frac{\pi_z(z^p)}{p} = F(z)$ est un entier algébrique.

13. (a) On a d'une part :

$$\prod_{i=1}^{n} P'(z_i) = \prod_{i=1}^{n} \prod_{\substack{j=1 \\ j\neq i}}^{n} (z_i - z_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{1\leqslant i<j\leqslant n} (z_i - z_j)^2,$$

et d'autre part, les relations coefficients-racines avec le coefficient constant de $X^n - 1$ impliquent :

$$\prod_{i=1}^{n} P'(z_i) = \prod_{i=1}^{n} n z_i^{n-1} = n^n \left(\prod_{i=1}^{n} z_i\right)^{n-1} = \left((-1)^{(n+1)}\right)^{n-1} n^n = (-1)^{n^2-1} n^n = (-1)^{n-1} n^n.$$

On en déduit :

$$\prod_{1\leqslant i<j\leqslant n} (z_i - z_j)^2 = (-1)^{\frac{n(n+1)}{2}+1} n^n.$$

Culture scientifique. La quantité $\prod_{i=1}^{n} P'(z_i)$ est le *discriminant* de P. Vous vérifierez en effet que pour un polynôme de degré 2 ou 3, cela vous donne la formule connue. Cette expression-là a l'avantage de rendre évident le fait que le discriminant s'annule en cas de racine multiple.

Questions à se poser, réflexes à acquérir.

— Vérifier en détails le calcul de $\prod_{i=1}^{n} P'(z_i)$, avec notamment le changement d'indexation sur i et j.

— Pourquoi $(-1)^{n^2-1} = (-1)^{n-1}$? A-t-on quelque chose d'analogue en remplaçant n^2 par n^k ?

(b) Les racines de π_z sont bien sûr des éléments de $\mathbb{U}_n$ et elles sont distinctes par la question 3. Posons : $I = \{i \in [\![1, n]\!] \mid \pi_z(z_i) = 0\}$. Avec cette notation, on a : $\pi_z = \prod_{i\in I}(X - z_i)$.

Pour montrer : $\pi_z(z^p) = 0$, nous allons raisonner par l'absurde. Supposons : $\pi_z(z^p) \neq 0$. Alors, puisque $z^p \in \mathbb{U}_n$ (un groupe est en effet stable par produit), il existe $k \in [\![1, n]\!] \setminus I$ tel que : $z^p = z_k$. Il vient : $\pi_z(z^p) = \prod_{i\in I}(z_k - z_i)$. Or ce produit peut être isolé dans le produit étudié dans la question précédente :

$$\prod_{1\leqslant i<j\leqslant n} (z_i - z_j)^2 = v\pi_z(z^p)$$

où v, qui est un produit de termes de la forme $z_i - z_j$, est un entier algébrique en tant que produit de différences d'entiers algébriques (*via* le théorème admis). Par la question précédente : $n^n = u\pi_z(z^p)$, où $u = (-1)^{\frac{n(n+1)}{2}+1} v$ est un entier algébrique. Comme l'ensemble des entiers algébriques est un anneau (théorème admis), le nombre $\frac{n^n}{p} = u \times \frac{\pi_z(z^p)}{p}$ est un entier algébrique. Comme $\frac{n^n}{p}$ est un rationnel, la question 4.(a) implique que c'est un entier, ce qui est absurde puisque p est un nombre premier qui ne divise pas n. On a prouvé, par l'absurde : $\pi_z(z^p) = 0$.

Questions à se poser, réflexes à acquérir.

— Comment écrirait-on formellement le nombre v ?

— Où intervient l'hypothèse $\pi_z(z^p) \neq 0$, qui justifiait de passer par un raisonnement par l'absurde, et échouerait sinon ?

(c) La question précédente montre que l'ensemble R des racines de π_z est stable par l'application $x \mapsto x^p$, pour tout nombre premier p ne divisant pas n. Il semble qu'on ait seulement démontré cette stabilité pour z et non pour tout $\omega \in R$. Justifions-la brièvement : Soit $\omega \in R$. On a $\pi_z = \pi_\omega$ d'après la remarque de la question 2.(b). donc, par la question précédente appliquée à ω, on a : $\pi_z(\omega^p) = \pi_\omega(\omega^p) = 0$. D'où le résultat de stabilité.

Par conséquent, si k est un entier premier avec n alors, en écrivant : $k = p_1 \cdots p_r$, où les p_i sont des nombres premiers non nécessairement distincts qui ne divisent pas n (en effet, des entiers sont premiers entre eux si et seulement s'ils n'ont pas de diviseur premier en commun), on note que $x \mapsto x^k$ s'obtient par composition des applications $x \mapsto x^{p_1}, \ldots, x \mapsto x^{p_r}$. La stabilité de R par ces applications implique donc la stabilité de R par $x \mapsto x^k$, pour tout k premier avec n. Or : $z \in R$, donc : $\mu_n = \left\{z^k \mid k \in \mathbb{N},\ \text{pgcd}(k,n) = 1\right\} \subseteq R$. On en déduit que $\Phi_n = \prod_{\omega \in \mu_n} (X - \omega)$ divise $\pi_z = \prod_{\omega \in R} (X - \omega)$.

D'où, puisque π_z est irréductible et que ces deux polynômes sont unitaires, $\Phi_n = \pi_z$. D'où le résultat. On a démontré l'irréductibilité de Φ_n, qui n'allait pas du tout de soi.

Questions à se poser, réflexes à acquérir.

— La relation de divisibilité entre Φ_n et π_z semble être dans $\mathbb{C}[X]$ (puisque j'utilise leur décomposition en facteurs irréductibles dans $\mathbb{C}[X]$), et pourtant je conclus en utilisant l'irréductibilité de π_z dans $\mathbb{Q}[X]$! Pourquoi n'ai-je pas fait une erreur de raisonnement ? La relation de divisibilité est-elle aussi valable dans $\mathbb{Q}[X]$?

— Vérifier que l'on a effectivement : $\mu_n = \left\{z^k \mid k \in \mathbb{N},\ \text{pgcd}(k,n) = 1\right\}$. Revoir le cours pour s'en convaincre, si besoin.

— Déduire de toute cette partie une stratégie potentielle (globale et résumée en peu de mots : la plupart des arguments ici nécessitent de manière décisive de manipuler des racines de l'unité et ne s'adaptent donc pas à toute circonstance) permettant de démontrer qu'un polynôme donné est irréductible.

Troisième partie

14. (a) C'est un calcul immédiat.

Questions à se poser, réflexes à acquérir. Peut-on avoir d'autres relations non triviales du même type entre $X^d P\left(\frac{1}{X}\right)$ et P ? Par exemple $X^d P\left(\frac{1}{X}\right) = -P$? Ou la même chose avec un facteur 2 devant P ? Un argument d'algèbre linéaire rend triviale la question.

(b) Puisque $P = X^d + \sum_{i=0}^{d-1} a_i X^i$ est unitaire et réciproque, son coefficient constant vaut 1 et 0 n'est pas racine de P. Donc : $x \neq 0$. Soit s l'ordre de multiplicité de x en tant que racine de P. Posons : $P = (X - x)^s Q$, où $Q \in \mathbb{C}_{d-s}[X]$ vérifie : $Q(x) \neq 0$. On a :

$$P = X^d P\left(\frac{1}{X}\right) = X^s \left(\frac{1}{X} - x\right)^s X^{d-s} Q\left(\frac{1}{X}\right) = (1 - xX)^s X^{d-s} Q\left(\frac{1}{X}\right)$$
$$= \left(\frac{1}{x} - X\right)^s x^s X^{d-s} Q\left(\frac{1}{X}\right).$$

Comme $\frac{1}{x}$ n'est pas racine de $X^{d-s} Q\left(\frac{1}{X}\right)$, ceci montre bien que $\frac{1}{x}$ est racine d'ordre s de P.

Questions à se poser, réflexes à acquérir. Y a-t-il d'autres propriétés de P qui se transfèrent aisément à son polynôme réciproque ? Irréductibilité par exemple, expression des dérivées, etc.

15. On a : $x\bar{x} = |x|^2 = 1$. Or $\pi_x \in \mathbb{Q}[X]$, donc on sait que le conjugué de x, c'est-à-dire $\bar{x} = \frac{1}{x}$, est aussi racine de π_x. Puisque $x \notin \{-1,1\}$, on a : $\frac{1}{x} \neq x$. C'est donc un conjugué de x. Par la remarque de la question 2.(b), on a donc : $\pi_{\frac{1}{x}} = \pi_x$. Or, en notant d le degré de π_x, le polynôme $X^d \pi_x\left(\frac{1}{X}\right)$ annule $\frac{1}{x}$, donc $\pi_x = \pi_{\frac{1}{x}}$ le divise. Comme ils sont de même degré d, on en déduit qu'il existe $\lambda \in \mathbb{Q}^*$ tel que : $X^d \pi_x\left(\frac{1}{X}\right) = \lambda \pi_x$. Pour déterminer λ, nous allons comparer les coefficients dominants. Pour connaître celui du membre de gauche, cela nécessite de connaître le coefficient constant de π_x, qui vaut, par les relations coefficients-racines : $(-1)^d \prod_{z \in R} z$.

Or l'égalité ci-dessus démontre que l'ensemble R des racines de π_x est stable par $z \mapsto z^{-1}$, ce qui permet de regrouper, dans ce produit, chaque racine avec son inverse ; à condition que $z \neq z^{-1}$ pour tout $z \in R$, c'est-à-dire à condition que $z \neq \pm 1$. Or 1 et -1 ne sont pas racines de π_x (car leur polynôme minimal vaut $X-1$ et $X+1$ respectivement, tandis que toute racine de π_x a π_x pour polynôme minimal), donc le raisonnement ci-dessus donne : $(-1)^d \prod_{z\in R} z = 1$. Les racines de π_x étant simples et pouvant être regroupées par paires (chaque racine peut être regroupée avec son inverse), il vient que d est pair et donc : $\pi_x(0) = \prod_{z\in R} z = 1$. Ceci montre que $X^d \pi_x\left(\frac{1}{X}\right)$ est unitaire, donc : $\lambda = 1$. Par conséquent, $\pi_x = X^d \pi_x\left(\frac{1}{X}\right)$, donc π_x est réciproque.

Questions à se poser, réflexes à acquérir.
- Quand on passe par les relations coefficients-racines, il faut toujours se demander pourquoi c'était l'idée pertinente à avoir. Pourquoi, ici, pouvait-on y être amené, au vu des hypothèses sur x ?
- Observer encore la commodité avec laquelle on peut démontrer des relations de divisibilité entre polynômes par simple évaluation (pourvu que le diviseur soit un polynôme irréductible).

16. (a) On a : $\gamma \notin \{-1,1\}$, car -1 et 1 sont algébriques de degré 1, tandis que γ est algébrique de degré 2 (car $\pi_\gamma = \pi_\alpha$). Par la question 15, le polynôme $\pi_\alpha = \pi_\gamma$ est réciproque et $\frac{1}{\alpha}$ est un conjugué de α (puisque les racines d'un polynôme réciproque sont stables par inverse, et le fait que $\alpha \in]1,+\infty[$ assure que l'on a : $\alpha \neq \frac{1}{\alpha}$).

Questions à se poser, réflexes à acquérir. Pourquoi raisonne-t-on avec π_γ au lieu de π_α directement ?

(b) Si γ était une racine de l'unité, donc une racine de $X^m - 1$ pour un certain $m \in \mathbb{N} \setminus \{0\}$, on aurait : $\pi_\gamma \mid X^m - 1$. Donc α serait une racine de l'unité, ce qui est absurde puisque : $|\alpha| = \alpha > 1$. Donc γ n'est pas une racine de l'unité.

Questions à se poser, réflexes à acquérir. Observer encore la commodité avec laquelle on peut démontrer des relations de divisibilité entre polynômes par simple évaluation (pourvu que le diviseur soit un polynôme irréductible).

(c) Si β est une racine de π_α de module différent de 1, alors β ou $\frac{1}{\beta}$ est de module strictement supérieur à 1. Comme π_α est réciproque, ce sont deux racines de π_α. Or, par définition de $\mathcal{S}$, le nombre α est l'unique racine de π_α de module strictement supérieur à 1. Donc $\beta = \alpha$ ou $\beta = \frac{1}{\alpha}$. On en déduit que tous les conjugués de α autres que $\frac{1}{\alpha}$ sont de module 1.

17. Si $\alpha \in \mathcal{S}$ est de degré impair, alors π_α, dont toutes les racines sont distinctes par la question 3, admet un nombre impair de racines. Or l'ensemble de ses racines est stable par inverse, donc en regroupant par paires chaque racine et son inverse, on observe que pour une raison de parité, le polynôme π_α admet une racine égale à son inverse. Autrement dit : le polynôme π_α admet 1 ou -1 pour racine, ce qui est absurde puisque le degré de π_α est au moins 2. Donc α est de degré pair. Si ce degré valait 2, on aurait : $C(\alpha) = \left\{\frac{1}{\alpha}\right\}$, ce qui contredit la définition de $\mathcal{S}$. Donc le degré de α est pair, au moins égal à 4 : d'où le résultat.

Questions à se poser, réflexes à acquérir. Pourquoi ai-je besoin d'écarter la possibilité de racines d'ordre multiple ?