Devoir Maison n° 8 : corrigé

MPSI Lycée Camille Jullian

5 mars 2024

Problème

I. Nombres algébriques.

1. Si z est algébrique, alors $\sum_{k=0}^{n} \frac{p_k}{q_k} z^k = 0$, avec p_k et q_k qui sont tous des nombres entiers. Il suffit de multiplier cette égalité par le produit de tous les nombres q_k pour obtenir une équation polynômiale dont z est solution, et dont tous les coefficients sont entiers.
2. Ce sont les nombres z vérifiant $az+b=0$, avec a et b entiers (d'après la question précédente), donc z est nécessairement rationnel. La réciproque étant évidente, les nombres algébriques de degré 1 sont les nombres rationnels.
3. Le nombre $\sqrt{3}$ est solution de l'équation de degr 2 $z^2-3=0$, qui est bien à coefficients rationnels. Bien sûr, $\sqrt{3}$ n'étant pas rationnel, il ne peut pas être de degré 1. Il est donc de degré exactement 2.
4. Calculons $(z-1-i)(z-1+i) = z^2-2z+2$. Le nombre $1+i$ est donc algébrique de degré au maximum 2. Comme il n'est pas rationnel (il n'est même pas réel), son degré vaut exactement 2. Son polynôme minimal est celui qu'on vient de calculer : $P = X^2-2X+2$.
5. Les racines sixièmes de l'unité sont $z_1 = 1$, $z_2 = e^{i\frac{\pi}{3}} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$, $z_3 = j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $z_4 = -1$, $z_5 = -z_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ et $z_6 = -j = \frac{1}{2} - i\frac{\sqrt{3}}{2}$. Ces six nombres sont évidemment algébriques puisqu'ils sont tous solutions de l'équation $z^6-1=0$. Les racines z_1 et z_4 étant rationnelles (et même entières), elles sont de degré 1, de polynôme minimal respectif $X-1$ et $X+1$. Similairement à ce qui s'est passé pour la question précédente, z_2 et z_6 sont de degré 2 et de polynôme minimal $(X-z_2)(X-z_6) = X^2-X+1$, et z_3 et z_5 sont aussi de degré 2 et de polynôme minimal $(X-z_3)(X-z_5) = X^2+X+1$.
6. Bon, vous commencez à avoir l'habitude, on va calculer $(X-5-i\sqrt{3})(X-5+i\sqrt{3}) = X^2-10X+34$, qui est évidemment le polynôme minimal de $5+i\sqrt{3}$.
7. (a) Bien sûr, le polynôme minimal étant par définition un polynôme dont les coefficients sont réels, on aura $\gamma = \overline{\alpha}$ et $\delta = \overline{\beta}$. De plus, le polynôme minimal $(X-\alpha)(X-\gamma)$ étant à coefficients rationnels, la somme $\alpha+\gamma$ et le produit $\alpha\gamma$ sont des nombres rationnels (de même bien sûr pour $\beta+\delta$ et $\beta\delta$). On développe alors brutalement le produit demandé pour obtenir (je vous passe les détails du developpement) $X^4-2(\alpha+\beta+\gamma+\delta)X^3+(3(\alpha+\gamma)(\beta+\delta)+(\alpha+\gamma)^2+(\beta+\delta)^2+2\alpha\gamma+2\beta\delta)X^2-(4\alpha\gamma(\beta+\delta)+4\beta\delta(\alpha+\gamma)+(\alpha+\gamma)(\beta^2+\delta^2)+(\beta+\delta)(\alpha^2+\gamma^2)+2\alpha\gamma(\alpha+\gamma)+2\beta\delta(\beta+\delta))X+\alpha^2\gamma^2+\beta^2\delta^2+2\alpha\gamma\beta\delta+\alpha\gamma(\beta^2+\delta^2)+\beta\delta(\alpha^2+\gamma^2)+(\alpha\gamma+\beta\delta)(\alpha+\gamma)(\beta+\delta)$. Sous cette écriture, le coefficient de X^3 est rationnel

puisque somme de deux rationnels (au facteur 2 près), celui de X^2 est rationnel (c'est une sommé de carrés ou de produits par des entiers de nombres rationnels). Les deux derniers coefficients sont moins trivialement rationnels car ils font intervenir des quantités dont on n'a pas encore discuté le statut : $\alpha^2+\gamma^2=(\alpha+\gamma)^2-2\alpha\gamma$ est rationnel, de même pour $\beta^2+\delta^2$. Bien sûr, $\alpha^2\gamma^2=(\alpha\gamma)^2$ est rationnel et $\beta^2\delta^2$ aussi. Les deux derniers coefficients sont alors sommes de rationnels, donc rationnels. Ouf, on a prouvé que les quatre racines du polynôme développé, dont $\alpha+\beta$, sont des nombres algébriques puisque racines d'un polynôme dont tous les coefficients sont rationnels.

(b) Même principe que la question précédente, mais le calcul sera heureusement plus léger : avec les mêmes notations, on développe $(X-\alpha\gamma)(X-\alpha\delta)(X-\beta\gamma)(X-\beta\delta)=X^4-(\alpha+\gamma)(\beta+\delta)X^3+(2\alpha\beta\gamma\delta+\alpha\gamma(\beta^2+\delta^2)+\beta\delta(\alpha^2+\gamma^2))X^2-\alpha\beta\gamma\delta(\alpha+\gamma)(\beta+\delta)X+(\alpha\beta\gamma\delta)^2$. Les calculs déjà effectués suffisent à prouver que ce polynôme a des coefficients rationnels et donc que $\alpha\beta$ est un nombre algébrique.

(c) L'ensemble des nombres algébriques est stable par somme et par produit d'après la généralisation admise des deux questions précédentes. Il contient évidemment les éléments neutres 0 et 1 qui sont tous les deux rationnels. Reste à prouver la stabilité par passage à l'opposé et à l'inverse. Pour l'opposé, c'est assez facile : si $\sum_{k=0}^{n} a_k z^k = 0$, alors $\sum_{k=0}^{n} b_n(-z)^k = 0$ en posant simplement $b_k = a_k$ si k est un indice pair, et $b_k = -a_k$ si k est un indice impair (bien sûr, les coefficients b_k seront rationnels si les a_k le sont). Pour l'inverse, c'est à peine plus compliqué : si $z \neq 0$ et $\sum_{k=0}^{n} a_k z^k = 0$, en divisant tout par z^n, on a $\sum_{k=0}^{n} a^k z^{k-n} = 0$, soit $\sum_{k=0}^{n} a_k \frac{1}{z^{n-k}} = 0$, ce qui est une équation polynômiale à coefficients rationnels vérifiée par $\frac{1}{z}$. On a bien tous les éléments pour affirmer que l'ensemble des nombres rationnels est un sous-corps de $\mathbb{C}$.

II. Polynômes cyclotomiques.

1. Parmi les racines huitièmes de l'unité, il y en a quatre qui ne sont **pas** primitives : 1 bien entendu (pour laquelle $z^1 = 1$), mais aussi -1 (dont le carré est égal à 1), et i et $-i$ (qui vérifient $z^4 = 1$). Les autres : $e^{i\frac{\pi}{4}}$, $e^{i\frac{3\pi}{4}}$, $e^{i\frac{5\pi}{4}}$ et $e^{i\frac{7\pi}{4}}$, sont toutes primitives. En effet, un multiple de $\frac{\pi}{4}$ ne peut être multiple de 2π que si le facteur est multiple de 8, mais c'est aussi le cas pour les multiples de $\frac{3\pi}{4}$, $\frac{5\pi}{4}$ et $\frac{7\pi}{4}$ car 3, 5 et 7 sont des entiers premiers avec 8 (c'est donc une conséquence directe du théorème de Gauss).
2. C'est exactement le même principe que pour $n = 8$. Si $k \wedge n = 1$, aucun multiple de k plus petit que nk ne peut être un multiple de n, donc $(e^{2i\frac{k\pi}{n}})^p = e^{i\frac{2kp\pi}{n}}$ n'aura jamais un argument multiple de 2π si $k \in \{1, \ldots, n-1\}$, ce qui prouve que les puissances correspondantes de $e^{2i\frac{k\pi}{n}}$ ne peuvent pas être égales à 1, et donc que la racine est primitive. Inversement, si $n \wedge k \neq 1$, en posant $a = n \wedge k$, $\frac{n}{a} < n$ et $(e^{i2\frac{k\pi}{n}})^{\frac{n}{a}} = e^{2i\frac{k\pi}{a}} = 1$ puisque $\frac{k}{a}$ est entier, ce qui prouve cette fois-ci que la racine n'est pas primitive.
3. L'ordre des questions de cette deuxième partie n'étant en fait pas extrêmement pratique,

on va tricher un peu dans ce corrigé en admettant (provisoirement) une partie du résultat demandé en question 6 (qui est en fait la partie la plus délicate de cette question elle-même difficile) : « toutes les racines n-èmes primitives de l'unité ont le même polynôme minimal ». Une fois ce résultats admis, il suffit pour répondre à la question qui nous intéresse pour l'instant de prouver que toute racine de l'unité est primitive pour un certain entier $k \leqslant n$. C'est en fait complètement évident, il suffit de poser $k = \min\{p \geqslant 1 \mid z^p = 1\}$. Par définition, $k \leqslant n$ puisqu'une racine n-ème de l'unité vérifie $z^n = 1$, et par construction, $z^p \neq 1$ pour $p \in \{1, \dots, k-1\}$, ce qui prouve que notre racine est une racine k-ème primitive de l'unité. Son polynôme minimal est donc le polynôme Φ_k, ce qui prouve en particulier qu'elle est racine de ce polynôme cyclotomique Φ_k.

Tant qu'on y est, allons un peu plus loin et démontrons que cet entier k est non seulement inférieur ou égal à n, mais même quil s'agit d'un diviseur de n. Notons pour cela α notre racine n-ème de l'unité, et $A = \{p \in \mathbb{Z} \mid \alpha^p = 1\}$. Par définition, k est le plus petit entier positif appartenant à A. Par ailleurs, A est un ensemble non vide (il contient entre autres 0 et n), et il est stable par somme (si $\alpha^p = \alpha^q = 1$, alors $\alpha^{p+q} = \alpha^p \times \alpha^q = 1$) et par passage à l'opposé : si $\alpha^p = 1$, $\alpha^{-p} = \dfrac{1}{\alpha^p} = 1$. Autrement dit, A est un sous-groupe additif de $\mathbb{Z}$, donc de la forme $a\mathbb{Z}$, avec a le plus petit élément strictement positif de A. Ah, donc en fait $a = k$. Comme $n \in A$, n est donc un multiple de k.

4. Il suffit de prouver que deux polynômes cyclotomiques ne peuvent pas avoir de racine commune. Signalons déjà que l'entier k pour lequel une racine n-ème de l'unité est une racine k-ème primitive de l'unité est toujours unique (c'est évident au vu de sa définition comme plus petite puissance positive de la racine égale à 1). Aucune racine n-ème de l'unité ne peut donc être primitive pour deux valeurs différentes n et p. Reste à prouver que seules les racines n-èmes primitives de l'unité sont racines de Φ_n (ce qui éviterait d'avoir d'autres racines qui pourraient être racine de deux polynômes cyclotomiques simultanément). C'est en fait une conséquence du résultat de la question 6 dont nous allons achever la démonstration maintenant. On sait déjà que toutes les racines primitives sont racines de Φ_n, qui est donc un multiple de $\displaystyle\prod_{z \in \mathbb{P}_n} (X - z)$. Si on prouve que ce produit est à coefficients rationnels, il sera nécessairement **égal** à Φ_n à cause de la minimalité de ce dernier. Prouvons ce résultat par récurrence forte sur l'entier n. Le polynôme $\Phi_1 = X - 1$ est à coefficients rationnels. Supposons que ce soit le cas de tous les Φ_k pour $k < n$, et parcourons la liste des racines n-èmes de l'unité, en les regroupant selon la valeur de l'entier k pour lequel elles sont racines primitives k-èmes de l'unité. Les valeurs de k correspondantes sont les diviseurs de n, et comme toute racine k-ème de l'unité sera a fortiori racine n-ème, toutes les racines k-èmes primitives font partie de notre liste de racines n-èmes. Autrement dit, le polynôme Φ_k est un sous-produit du produit $\displaystyle\prod_{\alpha \in \mathbb{U}_n} (X - \alpha)$, lui-même égal à $X^n - 1$. Par hypothèse de récurrence, Φ_k est un polynôme à coefficients rationnels, donc $\dfrac{X^n - 1}{\Phi_k}$ sera aussi à coefficients rationnels. Il suffit donc de partir du polynôme $X^n - 1$ et de le diviser successivement par tous les polynômes Φ_k pour k divisant n pour ne conserver que le produit $\displaystyle\prod_{z \in \mathbb{P}_n} (X - z)$, en ayant à chaque étape un polynôme à coefficients rationnels, et on obtiendra donc à la fin le polynôme Φ_n, lui-même à coefficients rationnels. C'est d'ailleurs la procédure qu'on utilisera en question 8 pour calculer les polynômes Φ_n.

5. C'est une conséquence directe de la question 4 : si la racine n'est pas primitive, elle est racine

k-ème primitive de l'unité pour un certain diviseur k de l'entier n, et donc racine de Φ_k. Comme Φ_k et Φ_n sont premiers entre eux, elle n'est donc pas racine de Φ_n.

6. On connait les racines de Φ_n, on sait que le produit proposé est à coefficients dans $\mathbb{Q}$, c'est donc bien le polynôme minimal de chaque racine n-ème primitive de l'unité, et en particulier de $e^{\frac{2i\pi}{n}}$ (on ne peut pas avoir de racine multiple, sinon le polynôme ne serait pas minimal). Il ne reste plus qu'à démontrer le fameux lemme indiquant que toutes ces racines primitives ont le même polynôme minimal, et ça c'est très difficile.

   Commençons par démontrer le résultat suivant, connu sous le nom de lemme de Gauss (oui, encore lui) : si un polynôme unitaire à coefficients entiers est produit de deux polynômes unitaires à coefficients rationnels, alors ceux-ci sont en fait à coefficients entiers. Pour cela, introduisons le concept suivant : le **contenu** d'un polynôme à coefficients entiers est le pgcd de ses coefficients. Un polynôme à coefficients entiers est **primitif** si son contenu est égal à 1 (autrement dit, on ne peut pas le « simplifier » par un facteur entier en conservant des coefficients qui sont tous entiers). C'est évidemment le cas d'un polynôme unitaire qui a un coefficient égal à 1. Montrons que le produit de deux polynômes primitifs A et B est lui aussi primitif : soit p un entier premier, comme A et B sont supposés primitifs, il existe au moins un coefficient de A et un coefficient de B qui ne sont pas divisibles par p. Notons i l'indice du premier coefficient de A non divisible par p (dans l'ordre des degrés croissants), et j l'indice du premier coefficient de B non divisible par p. Alors le coefficient d'indice $i+j$ du polynôme AB est égal à $\sum_{k=0}^{i+j} a_k b_{i+j-k}$ ne peut pas être divisible par p (la somme contient le produit $a_i b_j$ qui n'est pas divisible par p, et tous les autres termes de la somme font intervenir un coefficient a_k d'indice strictement inférieur à i ou un coefficient b_{i+j-k} d'indice strictement inférieur à j). Aucun nombre premier n'est donc facteur de tous les coefficients du polynôme AB, le pgcd de ces coefficients est alors égal à 1. Si A et B sont des polynômes qui ne sont pas supposés primitifs, on peut constater qu'en les divisant par leur contenu, on retombe sur des polynômes primitifs, dont le produit va donc être primitif. Ceci prouve que le contenu du produit AB est égal au produit des contenus de A et de B. Supposons maintenant que P soit un polynôme à coefficients entiers unitaire qui peut se factoriser sous la forme $P = AB$, avec A et B à coefficients rationnels et unitaires. On note a le pgcd des dénominateurs des coefficients du polynôme A, de façon à avoir aA qui est à coefficients entiers et primitif. De même, on note b le pgcd des dénominateurs des coefficients de B, et bB est un polynôme à coefficients entiers primitif. Alors $abAB = abP$ est un polynôme primitif. Comme P lui-même est un polynôme à coefficients entiers, cela voudrait dire que tous les coefficients de P sont divisibles par ab, en particulier le coefficient dominant égal à 1, donc $ab = 1$ (ici tous les entiers sont naturels, sinon -1 conviendrait aussi). Comme a et b sont des entiers, on a donc $a = b = 1$, ce qui prouve que A et B étaient en fait des polynômes à coefficients entiers. On remarque en passant que ce théorème explique pourquoi les polynômes cyclotomiques qu'on va calculer plus loin sont systématiquement des polynômes unitaires à coefficients entiers et pas seulement rationnels.

   Passons à la démonstration proprement dite. On note $a = e^{i\frac{2\pi}{n}}$ (le raisonnement fonctionnerait avec n'importe quelle racine n-ème primitive), et b une autre racine primitive n-ème de l'unité, forcément de la forme a^k, avec k premier avec n. On peut supposer sans perte de généralité que k est un nombre premier ne divisant pas n (en général k sera un produit de tels nombres premiers : si par exemple $k = p_1 p_2$ avec p_1 et p_2 premiers avec n, a^{p_1} aura le même polynôme minimal que a, puis $(a^{p_1})^{p_2}$ aura le même que a^{p_1}, donc que a). On note par ailleurs A et

B les polynômes minimaux de a et b. Ce sont forcément des polynômes irréductibles **dans** $\mathbb{Q}[X]$ (sinon en isolant le facteur dont a ou b est racine, on aurait un polynôme annulateur de degré plus petit que le polynôme minimal, ce qui est aberrant). Supposons par l'absurde qu'ils ne sont pas égaux, alors $X^n-1 = A(X)B(X)C(X)$, où A, B et C sont trois polynômes à coefficients entiers d'après le lemme de Gauss démontré plus haut. Par ailleurs, $B(b) = 0$, donc $B(a^k) = 0$, ce qui signifie que a est racine du polynôme composé $B(X^k)$, donc que $B(X^k) = A(X)D(X)$, avec D nouveau polynôme à coefficients entiers (le facteur dont a est racine est nécessairement un multiple de $A(X)$ d'après la minimalité de ce dernier). Si on effectue les calculs modulo k, le petit théorème de Fermat assure que $B(X^k) = (B(X))^k$, donc le polynôme $\overline{A}$ divise le polynôme $\overline{B}^K$ (les barres au-dessus des polynômes ici indiquent qu'on ne les considère plus comme des polynômes de $\mathbb{Q}[X]$ mais comme des polynômes à coefficients dans le corps $\dfrac{\mathbb{Z}}{k\mathbb{Z}}$ des entiers modulo k). On en déduit que $\overline{A}$ divise $\overline{B}$. En reprenant l'égalité $X^n-1 = A(X)B(X)C(X)$, on aurait alors des facteurs carrés dans X^n-1 (bon ok, dans son équivalent modulo k, mais ça marche quand même) puisque $\overline{A}$ divise $\overline{B}$. C'est absurde pour un polynôme à racines simples, même si je suis en train de vous arnaquer ici puisqu'il faudrait étudier les racines non pas dans $\mathbb{C}$ mais dans un corps minimal contenant $\dfrac{\mathbb{Z}}{k\mathbb{Z}}$. Mais comme cette démonstration est de toute façon complètement infaisable avec vos connaissances, je vais m'arrêter là et vous admettrez que les derniers détails peuvent être rendus rigoureux.

7. Ce résultat découle directement du raisonnement fait en question 4. Il faudrait quand même préciser qu'il faut évidemment exclure n lui-même de la liste des diviseurs pour que ça marche.
8. Allons-y, en utilisant deux méthodes différentes tant qu'à faire :
   - $\Phi_1 = X-1$ comme on l'a déjà signalé (la seule racine 1-ème de l'unité est 1, elle est primitive).
   - Il y a deux racines carrées de l'unité, dont seule -1 est primitive, donc $\Phi_2 = X+1$. Autre façon de faire : $\Phi_2 = \dfrac{X^2-1}{X-1} = X+1$ (on divise par le polynôme Φ_1 puisque 1 est le seul diviseur de n).
   - Il y a deux racines cubiques primitives de l'unité : j et $\overline{j}$, donc $\Phi_3 = (X-j)(X-\overline{j}) = X^2+X+1$. Alternativement, $\Phi_3 = \dfrac{X^3-1}{X-1} = X^2+X+1$.
   - Parmi les quatre racines quatrièmes de l'unité, seules i et $-i$ sont primitives, donc $\Phi_4 = (X-i)(X+i) = X^2+1$. Alternativement, $\Phi_4 = \dfrac{X^4-1}{(X-1)(X+1)} = X^2+1$ puisque 1 et 2 sont diviseurs de 4.
   - Puisque 5 est premier, toutes les racines cinquièmes de l'unité sont primitives, sauf 1 bien entendu, donc $\Phi_5 = \dfrac{X^5-1}{X-1} = X^4+X^3+X^2+X+1$ (pas besoin de détailler le calcul si on connaît ses identités remarquables).
   - On a déjà vu dans la première partie du problème que $\Phi_6 = X^2-X+1$. On aurait pu l'obtenir en calculant $\dfrac{X^6-1}{(X-1)(X+1)(X^2+X+1)}$.
9. Puisque $\Phi_n(0) = \displaystyle\prod_{z\in\mathbb{P}_n}(X-z)$, on a $\Phi_n(0)\displaystyle\prod_{z\in\mathbb{P}_n}(-z)$. Bien sûr, aucune racine n-ème primitive de l'unité n'est réelle quand $n \geqslant 2$ (puisque 1 et -1 ne sont pas primitives), chaque racine primitive a donc son conjugué dans la liste. Le produit à calculer est donc décomposable en produits de la forme $(-z)\times(-\overline{z}) = |z|^2 = 1$ puisqu'il s'agit de racines de l'unité qui sont toutes de module 1. Finalement, $\Phi_n(0) = 1$.

10. Regardons ce qui se passe pour les entiers pour lesquels on a calculé Φ_n : $\Phi_2(1) = 2$, $\Phi_3(1) = 3$, $\Phi_4(1) = 2$, $\Phi_5(1) = 5$ et $\Phi_6(1) = 1$. On peut conjecturer que $\Phi_n(1) = n$ quand n est un nombre premier, mais $\Phi_n(1) = p$ si $n = p^k$, avec p premier (c'est le cas pour $n = 4 = 2^2$), et $\Phi_n(1) = 1$ si n admet au moins deux facteurs premiers distincts (c'est le cas pour $n = 6$). On va le démontrer par récurrence forte sur n. On sait déjà que c'est vrai pour tous les entiers entre 2 et 6, ça suffit largement comme initialisation. Supposons-le vrai pour tout entier $k < n$, pour un certain $n \geqslant 3$. Alors :

- si n est un nombre premier, alors $\Phi_n = \dfrac{X^n - 1}{X - 1} = \displaystyle\sum_{k=0}^{n-1} X^k$, donc $\Phi_n(1) = n$, ce qui est bien la valeur souhaitée.
- si $n = p^k$, avec p premier, alors $\Phi_n = \dfrac{X^n - 1}{(X-1) \times \Phi_p \times \Phi_{p^2} \times \cdots \times \Phi_{p^{k-1}}}$ $= \dfrac{X^{n-1} + X^{n-2} + \cdots + X + 1}{\Phi_p \times \Phi_{p^2} \times \cdots \times \Phi_{p^{k-1}}}$. Par hypothèse de récurrence, tous les facteurs du dénominateurs prennent la valeur p en 1, donc $\Phi_n(1) = \dfrac{n}{p^{k-1}} = \dfrac{p^k}{p^{k-1}} = p$, ce qu'on voulait démontrer.
- enfin, si $n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$, avec les p_i premiers et $k \geqslant 2$, on aura de même $X^{n-1} + X^{n-2} + \cdots + X + 1 = \Phi_n \times \displaystyle\prod_{k|n} \Phi_k$. On évalue cette égalité en 1, en éliminant du produit tous les polynômes qui prennent par hypothèse de récurrence la valeur 1 en 1 (donc tous ceux faisant intervenir au moins deux facteurs premiers dans la décomposition de k), et on obtient $n = \Phi_n(1) \times (\Phi_{p_1}(1)\Phi_{p_1^2}(1) \ldots \Phi_{p_1^{\alpha_1}}(1)) \times \cdots \times (\Phi_{p_k}(1)\Phi_{p_k^2}(1) \ldots \Phi_{p_k^{\alpha_k}}(1))$, soit $n = \Phi_n(1) \times p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} = \Phi_n(1) \times n$. On a donc bien $\Phi_n(1) = 1$.