Correction du DS n°5

Sujet groupe A

2 Appliquons l'algorithme du pivot de Gauß.

$$\left(\begin{array}{ccc|ccc} 1 & 4 & 7 & 1 & 0 & 0 \\ 2 & 5 & 8 & 0 & 1 & 0 \\ 3 & 6 & 9 & 0 & 0 & 1 \end{array}\right)$$

$$\left(\begin{array}{ccc|ccc} 1 & 4 & 7 & 1 & 0 & 0 \\ 0 & -3 & -6 & -2 & 1 & 0 \\ 0 & -6 & -12 & -3 & 0 & 1 \end{array}\right) \begin{array}{l} \\ \mathrm{L}_2 \leftarrow \mathrm{L}_2 - 2\mathrm{L}_1 \\ \mathrm{L}_3 \leftarrow \mathrm{L}_3 - 3\mathrm{L}_1 \end{array}$$

On arrive à une matrice non inversible (car les deux dernières colonnes sont proportionnelles) donc la matrice de départ n'est pas inversible. Passons à la seconde :

$$\left(\begin{array}{ccc|ccc} 0 & 1 & -1 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 1 & 0 \\ 2 & 1 & 3 & 0 & 0 & 1 \end{array}\right)$$

$$\left(\begin{array}{ccc|ccc} 2 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 1 & 0 & 0 \\ 2 & 1 & 3 & 0 & 0 & 1 \end{array}\right) \mathrm{L}_2 \leftrightarrow \mathrm{L}_1$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 1/2 & 0 & 1/2 & 0 \\ 0 & 1 & -1 & 1 & 0 & 0 \\ 2 & 1 & 3 & 0 & 0 & 1 \end{array}\right) \mathrm{L}_1 \leftarrow \mathrm{L}_1/2$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 1/2 & 0 & 1/2 & 0 \\ 0 & 1 & -1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & -1 & 1 \end{array}\right) \mathrm{L}_3 \leftarrow \mathrm{L}_3 - 2\mathrm{L}_1$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 1/2 & 0 & 1/2 & 0 \\ 0 & 1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 3 & -1 & -1 & 1 \end{array}\right) \mathrm{L}_3 \leftarrow \mathrm{L}_3 - \mathrm{L}_2$$

On arrive à une matrice triangulaire dont les coefficients diagonaux sont tous non nuls donc cette matrice est inversible : la matrice de départ est donc inversible et on peut poursuivre.

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 1/2 & 0 & 1/2 & 0 \\ 0 & 1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1/3 & -1/3 & 1/3 \end{array}\right) \mathrm{L}_3 \leftarrow \mathrm{L}_3/3$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1/6 & 2/3 & -1/6 \\ 0 & 1 & 0 & 2/3 & -1/3 & 1/3 \\ 0 & 0 & 1 & -1/3 & -1/3 & 1/3 \end{array}\right) \begin{array}{l} \mathrm{L}_1 \leftarrow \mathrm{L}_1 - \mathrm{L}_3/2 \\ \mathrm{L}_2 \leftarrow \mathrm{L}_2 + \mathrm{L}_3 \\ \\ \end{array}$$

En conclusion

$$\boxed{\mathrm{A}^{-1} = \begin{pmatrix} 1/6 & 2/3 & -1/6 \\ 2/3 & -1/3 & 1/3 \\ -1/3 & -1/3 & 1/3 \end{pmatrix}}$$

3 Notons

$$f : \begin{cases}]\,1\,;+\infty\,[& \longrightarrow \mathbb{R} \\ x & \longmapsto \dfrac{x}{1+x^2} \end{cases}$$

Montrons que c'est une relation d'ordre.

- Soit $x \in \mathbb{R}$. Alors $f(x) \geqslant f(x)$ donc $x\mathrm{R}x$ si bien que R est réflexive.

- Soient $x, y \in \mathbb{R}$ tels que $x\mathrm{R}y$ et $y\mathrm{R}x$. Alors $f(x) \geqslant f(y)$ et $f(y) \geqslant f(x)$ si bien que $f(x) = f(y)$. f est dérivable et
$$f'(x) = \frac{(1+x^2) - 2x \times x}{(1+x^2)^2} = \frac{1-x^2}{(1+x^2)^2} < 0$$
sur $]\,1\,;+\infty\,[$: f est strictement décroissante donc injective, si bien que $x = y$: R est antisymétrique.
- Soient x, y, z tels que $x\mathrm{R}y$ et $y\mathrm{R}z$. Alors $f(x) \geqslant f(y)$ et $f(y) \geqslant f(z)$ donc $f(x) \geqslant f(z)$ c'est-à-dire que $x\mathrm{R}z$: la relation est transitive.

On a donc une relation d'ordre. Enfin, si x et $y \in\,]\,1\,;+\infty\,[$, $f(x) \geqslant f(y)$ ou $f(y) \geqslant f(x)$, c'est-à-dire que $x\mathrm{R}y$ ou $y\mathrm{R}x$: l'ordre est total.

R est une relation d'ordre total.

4 Montrons que c'est une relation d'équivalence.

- Soit $(x, y) \in \mathbb{R}^2$. Alors, en prenant $a = b = 1 > 0$, $x = ax$ et $y = by$ donc $(x, y)\mathrm{R}(x, y)$ si bien que R est réflexive.
- Soient (x_1, y_1) et $(x_2, y_2) \in \mathbb{R}^2$ tels que $(x_1, y_1)\mathrm{R}(x_2, y_2)$. Alors il existe $a > 0$ et $b > 0$ tels que $x_2 = ax_1$ et $y_2 = by_1$ et donc $x_1 = (1/a) \times x_2$ et $y_1 = (1/b) \times y_2$ et on a $1/a, 1/b > 0$ donc $(x_2, y_2)\mathrm{R}(x_1, y_1)$: R est symétrique.
- Soient $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^2$ tels que $(x_1, y_1)\mathrm{R}(x_2, y_2)$ et $(x_2, y_2)\mathrm{R}(x_3, y_3)$. Alors il existe $a, b, c, d > 0$ tels que $x_2 = ax_1$, $y_2 = by_1$, $x_3 = cx_2$ et $y_3 = dy_2$ donc $x_3 = cax_1$ et $y_3 = dby_1$ et $ac, db > 0$ si bien que $(x_1, y_1)\mathrm{R}(x_3, y_3)$: la relation est transitive.

C'est une relation d'équivalence.

5 Montrons que c'est une relation d'équivalence.

- Soit $(x, y) \in \mathbb{R}^2$. Alors $x = x$ donc $(x, y)\mathrm{R}(x, y)$ si bien que R est réflexive.
- Soient (x_1, y_1) et $(x_2, y_2) \in \mathbb{R}^2$ tels que $(x_1, y_1)\mathrm{R}(x_2, y_2)$. Alors $x_1 = x_2$ donc $x_2 = x_1$ si bien que $(x_2, y_2) = (x_1, y_1)$: $(x_2, y_2)\mathrm{R}(x_1, y_1)$, la relation est symétrique.
- Soient $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^2$ tels que $(x_1, y_1)\mathrm{R}(x_2, y_2)$ et $(x_2, y_2)\mathrm{R}(x_3, y_3)$. Alors $x_1 = x_2$ et $x_2 = x_3$ donc $x_1 = x_3$ si bien que $(x_1, y_1)\mathrm{R}(x_3, y_3)$: la relation est transitive.

R est une relation d'équivalence sur $\mathbb{R}^2$.

Si $(a, b) \in \mathbb{R}^2$, les éléments équivalents à (a, b) sont les points du plan ayant la même abscisse que (a, b), c'est-à-dire la droite d'équation $x = a$ (le dessin est laissé à votre charge).

6 Voir question 5 des préliminaires du sujet B et C.

7 Puisque ce n'est pas une loi connue, on ne peut pas prouver que c'est un sous-groupe d'un groupe connu. Une seule solution : la définition d'un groupe.

- La loi est évidemment interne car un produit de deux réels strictement positifs est strictement positif, et donc la première coordonnée est toujours dans $\mathbb{R}_+^*$.
- Montrons que la loi est associative. Soient $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^2$. D'une part :
$$\begin{aligned}(x_1, y_1) \oplus ((x_2, y_2) \oplus (x_3, y_3)) &= (x_1, y_1) \oplus (x_2x_3, x_2y_3 + y_2)\\ &= (x_1x_2x_3, x_1(x_2y_3 + y_2) + y_1)\\ &= (x_1x_2x_3, x_1x_2y_3 + x_1y_2 + y_1)\end{aligned}$$
et d'autre part
$$\begin{aligned}((x_1, y_1) \oplus (x_2, y_2)) \oplus (x_3, y_3) &=\\ &= (x_1x_2, x_1y_2 + y_1) \oplus (x_3, y_3)\\ &= (x_1x_2x_3, x_1x_2(y_3) + (x_1y_2 + y_1)\end{aligned}$$
donc la loi est associative.
- $(1, 1) \oplus (2, 2) = (2, 3)$ et $(2, 2) \oplus (1, 1) = (2, 4)$ donc la loi n'est pas commutative.
- La loi n'étant pas commutative, il faut prouver que le neutre est neutre des deux côtés (et idem pour le symétrique). Il est immédiat que $(1, 0)$ est neutre (des deux côtés !).

- Soit $(x,y) \in \mathbb{R}_+^* \times \mathbb{R}$. On cherche (a,b) tel que $(x,y) \oplus (a,b) = (1,0)$ c'est-à-dire $(ax, xb+y) = (1,0)$. Alors $a = 1/x$ et $b = -y/x$ conviennent, et on a également $(1/x, -y/x) \oplus (x,y) = (1,0)$ donc $(1/x, -y/x)$ est le symétrique (à gauche et à droite) de (x,y).

C'est bien un groupe, et il est non abélien.

8 Voir question 3 des préliminaires du sujet B et C.

9 On rappelle que la loi de ce groupe est $\mathbb{C}^*$. Soient donc z_1 et z_2 dans $\mathbb{C}^*$.

$$\begin{aligned} f(z_1 \times z_2) &= \frac{z_1 \times z_2}{|z_1 \times z_2|} \\ &= \frac{z_1}{|z_1|} \times \frac{z_2}{|z_2|} \\ &= f(z_1) \times f(z_2) \end{aligned}$$

On en déduit que f est un morphisme de groupes. Le neutre de $\mathbb{C}^*$ étant 1, $\mathrm{Ker}\,(f) = \{z \in \mathbb{C}^* \mid f(z) = 1\}$ c'est-à-dire que $\mathrm{Ker}\,(f)$ est l'ensemble des complexes (non nuls) tels que $z = |z|$. Par conséquent :

f est un morphisme de groupes et son noyau est $\mathbb{R}_+^*$.

10 Notons A l'ensemble en question.

- La fonction nulle appartient à A donc A est non vide.
- A est stable par somme : soient en effet f_1 et f_2 appartenant à A, qui tendent respectivement vers L_1 et $\mathrm{L}_2 \in \mathbb{R}$ en $+\infty$. Alors $f_1 + f_2$ tend vers $\mathrm{L}_1 + \mathrm{L}_2 \in \mathbb{R}$ en $+\infty$ donc $f_1 + f_2 \in$ A.
- $-f_1$ tend vers $-\mathrm{L}_1$ en $+\infty$ donc $-f_1 \in$ A : A est stable par opposé, c'est un sous-groupe de $(\mathbb{R}^{\mathbb{R}}, +)$.
- La fonction constante égale à 1 appartient à A.
- $f_1 \times f_2 \in$ A car tend vers $\mathrm{L}_1 \times \mathrm{L}_2$: A est stable par produit.

On en déduit que A est un sous-anneau de $\mathbb{R} \times \mathbb{R}$. Ce n'est pas un anneau intègre : par exemple, si on note f l'indicatrice de 0 et g l'indicatrice de $[\,1\,;2\,]$, alors $f \times g$ est la fonction nulle (et f et g appartiennent à A car tendent vers 0) alors que ni f ni g n'est la fonction nulle.

A est un sous-anneau non intègre de $\mathbb{R}^{\mathbb{R}}$.

> Attention de ne pas dire que A n'est pas intègre car $\mathbb{R}^{\mathbb{R}}$ ne l'est pas : un anneau non intègre peut avoir un sous-anneau intègre, par exemple le sous-anneau des fonctions constantes (exo).

11 cf. exercice 45 du chapitre 18 (avec $k = 1$).

C'est un corps.

12 D'après le binôme de Newton,

$$\begin{aligned} \mathrm{P} &= \sum_{k=0}^{2024} \tbinom{2024}{k} \mathrm{X}^k 2^{2024-k} - \sum_{k=0}^{2024} \tbinom{2024}{k} \mathrm{X}^k (-2)^{2024} \\ &= \sum_{k=0}^{2024} \tbinom{2024}{k} \left(2^{2024-k} - (-2)^{2024-k}\right) \mathrm{X}^k \end{aligned}$$

Le coefficient de X^{2024} est nul (il vaut $\binom{2024}{0}(2^0 - (-2)^0) = 0$) et celui de X^{2023} vaut

$$\tbinom{2024}{1}(2^{2024-2023} - (-2)^{2024-2023}) = 2024 \times (2 - (-2)) = 4 \times 2024 \neq 0$$

En conclusion P est de degré 2023 et de coefficient dominant 4×2024.

13 Faite dans le cours.

14 Appliquons l'algorithme d'Euclide.

$$\begin{array}{rl|l} X^4 - 3X^3 + X^2 + 4 & & X^3 - 3X^2 + 3X - 2 \\ -(X^4 - 3X^3 + 3X^2 - 2X) & & \hline X \\ \hline -2X^2 + 2X + 4 & & \end{array}$$

Ensuite :

$$\begin{array}{rl|l} X^3 - 3X^2 + 3X - 2 & & -2X^2 + 2X + 4 \\ -(X^3 - X^2 - 2X) & & \hline -X/2 + 1 \\ \hline -2X^2 + 5X - 2 & & \\ -(-2X^2 + 2X + 4) & & \\ \hline 3X - 6 & & \end{array}$$

Enfin :

$$\begin{array}{rl|l} -2X^2 + 2X + 4 & & 3X - 6 \\ -(-2X^2 + 4X) & & \hline -2X/3 - 2/3 \\ \hline -2X + 4 & & \\ -(-2X + 4) & & \\ \hline 0 & & \end{array}$$

On en déduit que $3X - 6$ (le dernier reste non nul) est UN PGCD et comme on demande $A \wedge B$ (avec A et B les deux polynômes de l'énoncé), on demande leur unique PGCD unitaire, c'est-à-dire $X - 2$.

$$\boxed{A \wedge B = X - 2}$$

15 D'après le théorème de division euclidienne, il existe Q et R uniques tels que

$$(X+1)^n - X^n - 1 = (X-2)^2 Q + R$$

avec $\deg(R) < \deg((X-2)^2) = 2$ donc $\deg(R) \leqslant 1$: il existe donc a et b tels que

$$(X+1)^n - X^n - 1 = (X-2)^2 Q + aX + b$$

En évaluant en 2, il vient : $3^n - 2^n - 1 = 2a + b$. Dérivons l'égalité ci-dessus, ce qui donne :

$$n(X+1)^{n-1} - nX^{n-1} = (X-2)^2 Q' + 2(X-2)Q + a$$

Si on évalue encore en 2, on obtient $a = n3^{n-1} - n2^{n-1}$ si bien que $b = 3^n - 2^n - 1 - 2n3^{n-1} + n2^n$.

$$\boxed{\text{Le reste recherché est } (n3^{n-1} - n2^{n-1}) \times X + 3^n - 2^n - 1 - 2n3^{n-1} + n2^n.}$$

16 Rappelons que la multiplicité est l'ordre de la première dérivée non nulle. En clair : on dérive jusqu'à obtenir une dérivée non nulle en 1 et ce sera la multiplicité cherchée.

- Tout d'abord, $P(1) = 0$: 1 est bien racine de P.
- Ensuite, $P' = 6X^5 - 25X^4 + 32X^3 - 6X^2 - 14X + 7$ donc on a encore $P'(1) = 0$: 1 est racine au moins double (ou est racine multiple).
- $P'' = 30X^4 - 100X^3 + 96X^2 - 12X - 14$ donc $P''(1) = 0$: 1 est racine au moins triple.
- $P^{(3)} = 120X^3 - 300X^2 + 192X - 12$ donc $P^{(3)}(1) = 0$: 1 est racine de multiplicité au moins 4.
- $P^{(4)}(1) = 360X^2 - 600X + 192$ donc $P^{(4)}(1) = -48 \neq 0$.

$$\boxed{\text{1 est racine de P de multiplicité 4.}}$$

17 cf. exercice 6 du chapitre 19.

18 Voir question 4 des préliminaires du sujet B et C.

19 On fait comme en cours pour donner un polynôme d'interpolation de Lagrange.

$$\boxed{P = 5 \times \frac{(X-2)(X-10)}{(1-2)(1-10)} + 7 \times \frac{(X-1)(X-10)}{(2-1)(2-10)} - 4 \times \frac{(X-1)(X-2)}{(10-1)(10-2)} \text{ convient.}}$$

20 cf. exercice 6 du chapitre 20.

Sujet groupes B et C

Préliminaires

3 Il est évident qu'on parle d'un groupe pour le produit, et donc le neutre est 1. Notons G cet ensemble.

- Précisons que G est bien inclus dans $\mathbb{R}^*$ (ne pas oublier de le vérifier) car un quotient de deux entiers impairs est forcément non nul.
- $1 = 1/1 \in \mathrm{G}$ donc G est non vide.
- Soit $x \in \mathrm{G}$ (donc non nul). Il existe p et q impairs tels que $x = p/q$ donc $1/x = q/p \in \mathrm{G}$: G est stable par inverse.
- Soient $x_1, x_2 \in \mathrm{G}$. Il existe p_1, p_2, q_1, q_2 impairs tels que $x_1 = p_1/q_1$ et $x_2 = p_2/q_2$ donc $x_1x_2 = (p_1p_2)/(q_1q_2)$. Or, un produit de nombres impairs est impair donc p_1p_2 et q_1q_2 sont impairs donc $x_1x_2 \in \mathrm{G}$: G est stable par produit.

$$\boxed{\text{G est un sous-groupe de } \mathbb{R}^*.}$$

4 On commence par chercher des racines évidentes : 0 et -1 sont racines évidentes, donc P est divisible par $\mathrm{X}(\mathrm{X}+1) = \mathrm{X}^2+\mathrm{X}$. Puisque P est de degré 4, il existe $a, b, c \in \mathbb{R}$ tels que $\mathrm{P} = (\mathrm{X}^2+\mathrm{X})(a\mathrm{X}^2+b\mathrm{X}+c)$. À l'aide du coefficient dominant, on trouve $a = 1$. À l'aide du terme constant, on trouve $c = 3$. À l'aide du terme en X^3, on trouve que $3 = a + b$ donc $b = 2$.

> On pouvait également trouver b à l'aide du coefficient en X^2 ou en X. N'hésitez pas à le faire au brouillon, pour vérifier que vous n'avez pas fait d'erreur.

Par conséquent, $\mathrm{P} = \mathrm{X}(\mathrm{X}+1)(\mathrm{X}^2+2\mathrm{X}+3)$ (on pouvait également faire la division euclidienne de P par $\mathrm{X}^2+\mathrm{X}$ et on trouvait évidemment le même résultat). Or, le discriminant de $\mathrm{X}^2 + 2\mathrm{X} + 3$ est strictement négatif, donc on ne peut pas aller plus loin sur $\mathbb{R}$.

$$\boxed{\text{La factorisation de P sur } \mathbb{R} \text{ est : } \mathrm{P} = \mathrm{X}(\mathrm{X}+1)(\mathrm{X}^2+2\mathrm{X}+3).}$$

Sur $\mathbb{C}$, il suffit de voir (à l'aide d'un calcul de discriminant) que $\mathrm{X}^2 + 2\mathrm{X} + 3 = (\mathrm{X} - 1 + i\sqrt{3})(\mathrm{X} - 1 - i\sqrt{3})$.

$$\boxed{\text{La factorisation de P sur } \mathbb{R} \text{ est : } \mathrm{P} = \mathrm{X}(\mathrm{X}+1)(\mathrm{X}-1+i\sqrt{3})(\mathrm{X}-1-i\sqrt{3}).}$$

5 On fait comme en TD : on a 2 I, 1 M, 2 A, 2 G, 2 N, 1 E, 1 D, 1 R, 1 O, 1 S, ce qui fait 14 lettres.

$$\boxed{\text{Il y a } \frac{14!}{2!^4} = \frac{14!}{2^4} \text{ anagrammes possibles.}}$$

> Cela donne 5 448 643 200 possibilités : bon courage ! On pouvait également utiliser la deuxième méthode vue en classe, i.e. jouer au pendu : il y a
> $$\binom{14}{2} \times \binom{12}{1} \times \binom{11}{2} \times \binom{9}{2} \times \binom{7}{2} \times \binom{5}{1} \times \binom{4}{1} \times \binom{3}{1} \times \binom{2}{1} \times \binom{1}{1}$$
> ce qui donnait évidemment le même résultat en simplifiant les factorielles.

Problème - Polynômes cyclotomiques

Partie I. Caractérisation des racines primitives n-ièmes de l'unité

1 En clair, on prend les racines de l'unité en supprimant celles qu'on a déjà rencontrées pour de plus petites valeurs de n. $\mathbb{U}_1 = \mathrm{P}_1 = \{1\}$. On a $\mathbb{U}_2 = \{\pm 1\}$ mais 1 n'est pas une racine primitive deuxième donc $\mathrm{P}_2 = \{-1\}$. On a $\mathbb{U}_3 = \{1; j; j^2\}$ mais 1 n'est pas une racine primitive troisième donc $\mathrm{P}_3 = \{j; j^2\}$. Enfin, $\mathbb{U}_4 = \{\pm 1; \pm i\}$ mais ± 1 ne sont pas des racines primitives quatrièmes (puisqu'on les rencontre avant) donc $\mathrm{P}_4 = \{\pm i\}$.

$$\boxed{\mathrm{P}_1 = \{1\}, \mathrm{P}_2 = \{-1\}, \mathrm{P}_3 = \{j; j^2\}, \mathrm{P}_4 = \{\pm i\}}$$

2 Si $n \geqslant 2$, P_n ne contient pas 1 donc n'est pas un groupe car ne contient pas de neutre. Si $n = 1$, $\mathrm{P}_n = \{1\}$ qui est un groupe (peu intéressant).

$\boxed{\mathrm{P}_n \text{ est un groupe si et seulement si } n = 1.}$

3.(a) Notons ce complexe ω. Soit $d = k \wedge n$. Il existe k' et n' (premiers entre eux mais c'est inutile dans la suite) tels que $k = k'd$ et $n = n'd$ donc $\omega = e^{2ik\pi/n} = e^{2ik'\pi/n'}$. Dès lors, $\omega^{n'} = 1$ et $n' < n$ car $d > 1$ et donc

$\boxed{\omega = e^{2ik\pi/n} \text{ n'est pas une racine primitive } n\text{-ième de l'unité.}}$

3.(b) Notons encore $\omega = e^{2ik\pi/n}$. Supposons que ω ne soit pas une racine primitive n-ième de l'unité. Il existe donc $q \in [\![1\,;\, n-1]\!]$ tel que $\omega^q = 1$ donc $e^{2ikq\pi/n} = 1$. Ainsi,

$$\frac{2kq\pi}{n} \equiv 0[2\pi]$$

donc $kq \equiv 0[n]$, c'est-à-dire que n divise kq. Or, $n \wedge k = 1$ donc, d'après le théorème de Gauß, n divise q ce qui est impossible car $q \in [\![1\,;\, n-1]\!]$.

$\boxed{\omega \text{ est bien une racine primitive } n\text{-ième de l'unité.}}$

3.(c) D'après ce qui précède, il existe k_1 et k_2 premiers avec n tels que $z_1 = e^{2ik_1\pi/n}$ et $z_2 = e^{2ik_2\pi/n}$. On cherche u tel que $e^{2ik_1u\pi/n} = e^{2ik_2\pi/n}$ donc tel que

$$\frac{2k_1u\pi}{n} \equiv \frac{2k_2\pi}{n}$$

c'est-à-dire $k_1u \equiv k_2[n]$ donc tel qu'il existe v tel que $k_1u = k_2 + nv$. Or, k_2 est un multiple de $k_1 \wedge n = 1$ donc, d'après le théorème de Bézout, il existe u et v tels que $uk_1 + vn = k_2$. Par conséquent :

$$\begin{aligned} {z_1}^u &= e^{\frac{2ik_1u\pi}{n}} \\ &= e^{\frac{2i(k_2-vn)\pi}{n}} \\ &= e^{\frac{2ik_2\pi}{n}-2iv\pi} \\ &= z_2 \end{aligned}$$

Il suffit enfin de prouver que u est premier avec n. Si d est un diviseur commun à u et n alors d divise $uk_1 + vn = k_2$ donc d est un diviseur commun à n et k_2 qui sont premiers entre eux donc $d = 1$.

$\boxed{\text{Il existe } u \text{ tel que } {z_1}^u = z_2.}$

> On pouvait également raisonner en deux temps : d'après le théorème de Bézout, il existe m et p tels que $mk_1 + np = 1$ donc $mk_2k_1 + npk_2 = k_2$. Si on pose $u = mk_2$ alors on montre comme ci-dessus que ${z_1}^u = z_2$ et, d'après le théorème de Bézout, m est premier avec n, tout comme k_2, donc $u = mk_2$ est premier avec n (cf. chapitre 6 : le produit de deux entiers premiers avec n est premier avec n).

Partie II. Définition et premières propriétés des polynômes cyclotomiques

2 D'après la question 1 de la partie I, on a respectivement :

$$\boxed{\Phi_1 = \mathrm{X} - 1, \Phi_2 = \mathrm{X} + 1, \Phi_3 = (\mathrm{X} - j)(\mathrm{X} - j^2) = \mathrm{X}^2 + \mathrm{X} + 1 \text{ et } \Phi_4 = (\mathrm{X} - i)(\mathrm{X} + i) = \mathrm{X}^2 + 1 \in \mathbb{Z}[\mathrm{X}]}$$

> Il semblerait même que les Φ_n soient aussi à coefficients égaux à 0 ou ± 1... Ce n'est qu'une impression ! Par exemple, Φ_{105} a un coefficient égal à -2 (Wikipedia est votre ami) et c'est même le premier qui n'a pas un coefficient égal à 0 ou ± 1 : RIP les « par récurrence immédiate »...

3.(a) Par définition :

$$\Phi_5 = \prod_{k=0, k\wedge 5=1}^{5} (\mathrm{X} - e^{2ik\pi/5})$$

Or, 5 est premier donc tous les entiers de $[\![\, 0\,;\, 5\,]\!]$ (distincts de 0) sont premiers avec 5. On en déduit que :

$$\Phi_5 = \prod_{k=1}^{5} (\mathrm{X} - e^{2ik\pi/5})$$

Or, d'après la question 1 (la question de cours), $\mathrm{X}^5 - 1 = \prod_{k=0}^{5}(\mathrm{X} - e^{2ik\pi/5})$. En clair, « Φ_5 est le polynôme $\mathrm{X}^5 - 1$ auquel il manque $\mathrm{X} - 1$ » :

$$\boxed{\Phi_5 = \frac{\mathrm{X}^5 - 1}{\mathrm{X} - 1}}$$

On reconnaît « une somme géométrique » (attention, on a des objets formels, ne me parlez pas de valeur interdite) donc

$$\boxed{\Phi_5 = 1 + \mathrm{X} + \mathrm{X}^2 + \mathrm{X}^3 + \mathrm{X}^4}$$

3.(b) De même, p étant premier, le seul entier $k \in [\![\, 0\,;\, p-1\,]\!]$ qui n'est pas premier avec p est $p = 0$ donc il faut « retirer $\mathrm{X} - 1$ du polynôme $\mathrm{X}^p - 1$ », c'est-à-dire :

$$\boxed{\Phi_p = \frac{\mathrm{X}^p - 1}{\mathrm{X} - 1} = 1 + \mathrm{X} + \mathrm{X}^2 + \cdots + \mathrm{X}^{p-1}}$$

4.(a) Les différents entiers de $[\![\, 1\,;\, n\,]\!]$ ont un PGCD avec n qui divise n (c'est par définition un diviseur commun). Il suffit ensuite de regrouper les entiers selon leur PGCD avec n (et on trouve même que l'union est disjointe).

$$\boxed{[\![\, 0\,;\, n-1\,]\!] = \bigcup_{d|n} \mathrm{E}_d}$$

4.(b) Soit

$$g : \begin{cases} \mathrm{E}_d \longrightarrow \mathrm{F}_d \\ k \longmapsto \dfrac{k}{d} \end{cases}$$

Montrons que g est une bijection de E_d dans F_d.

- Justifions déjà que g est bien définie : si $k \in \mathrm{E}_d$ alors $k \wedge n = d$ donc k est divisible par d donc k/d est bien un entier. De plus, d'après le cours d'arithmétique, k/d et n/d sont premiers entre eux donc g est bien à valeurs dans F_d.
- g est évidemment injective : si $k_1 \neq k_2$ alors $k_1/d \neq k_2/d$ donc $g(k_1) \neq g(k_2)$.
- Soit $k \in \mathrm{F}_d$. Puisque $k \wedge (n/d) = 1$ alors (cf. chapitre 6) $dk \wedge n = d$. On en déduit que $nk \in \mathrm{E}_d$ et puisque $g(nk) = k$, alors nk est un antécédent de k si bien que g est surjective.

$$\boxed{\mathrm{E}_d \text{ et } \mathrm{F}_d \text{ sont en bijection.}}$$

4.(c) En faisant le changement de variable bijectif $k' = g(k)$ (avec g la bijection de la question précédente), c'est-à-dire, plus simplement, $k' = k/d$, $k = dk'$, il vient :

$$\prod_{k\in \mathrm{E}_d} (\mathrm{X} - e^{2ik\pi/n}) = \prod_{k'\in \mathrm{F}_d} (\mathrm{X} - e^{2idk'\pi/n}) = \prod_{k'\in \mathrm{F}_d} (\mathrm{X} - e^{2ik'\pi/(n/d)})$$

On conclut en utilisant la définition de F_d : le produit de droite est en fait le produit pour les indices k' tels que $k' \wedge (n/d) = 1$, c'est par définition $\Phi_{n/d}$:

$$\boxed{\prod_{k\in \mathrm{E}_d} (\mathrm{X} - e^{2ik\pi/n}) = \Phi_{n/d}}$$

4.(d) On a successivement :

$$\mathrm{X}^n - 1 = \prod_{k=0}^{n-1} (\mathrm{X} - e^{2ik\pi/n}) \qquad \text{Question 1 et cours}$$

$$= \prod_{d|n} \prod_{k \in \mathrm{E}_d} (\mathrm{X} - e^{2ik\pi/n}) \qquad \text{Question 4.(a) et regroupement par paquets}$$

$$= \prod_{d|n} \Phi_{n/d} \qquad \text{Question 4.(c)}$$

Or, si on note D l'ensemble des diviseurs de n, $d \mapsto n/d$ est une bijection de D dans lui-même (exo, mais c'est tellement immédiat qu'on peut le dire directement). On peut donc effectuer le changement de variable bijectif $d' = n/d$ si bien que, l'indice étant muet :

$$\boxed{\mathrm{X}^n - 1 = \prod_{d'|n} \Phi_{d'} = \prod_{d|n} \Phi_d}$$

5.(a) On a $\Phi_1 = \mathrm{X} - 1 \in \mathbb{Z}[\mathrm{X}]$.

L'initialisation est donc prouvée.

5.(c) Un polynôme cyclotomique étant un produit de polynômes de la forme $\mathrm{X} - \alpha$, un polynôme cyclotomique est unitaire, et donc B est unitaire, et à coefficients entiers par hypothèse de récurrence : on peut donc bien appliquer le théorème de division euclidienne sur $\mathbb{Z}[\mathrm{X}]$. Il existe donc Q et R appartenant à $\mathbb{Z}[\mathrm{X}]$ uniques tels que $\mathrm{X}^n - 1 = \mathrm{BQ} + \mathrm{R}$ avec $\deg(\mathrm{R}) < \deg(\mathrm{B})$. Or, d'après la question 4.(d), $\mathrm{X}^n - 1 = \mathrm{B} \times \Phi_n$ (il ne manque que n parmi les diviseurs de n), c'est-à-dire que $\mathrm{X}^n - 1 = \mathrm{B} \times \Phi_n + 0$. Puisque $\deg(0) < \deg(\mathrm{B})$, par unicité, on a $\mathrm{Q} = \Phi_n$ et, en particulier, cela implique que $\Phi_n \in \mathbb{Z}[\mathrm{X}]$, ce qui clôt la récurrence.

Les polynômes cyclotomiques sont à coefficients entiers (relatifs).

Partie III. Théorème de Wedderburn

2

- Pour tout $y \in \mathrm{K}$, $0 \times y = y \times 0 = 0$ (dans un anneau et donc dans un corps, 0, c'est-à-dire le neutre de l'addition, est absorbant). En d'autres termes, $0 \in \mathrm{Z(K)}$: Z(K) est non vide.
- Soient x_1 et $x_2 \in \mathrm{K}$. Soit $y \in \mathrm{K}$. Alors $(x_1 + x_2)y = x_1 y + x_2 y$ (dans un anneau, et donc dans un corps, le produit est distributif par rapport à la somme, mais il n'est pas indispensable de l'écrire dans votre copie) et x_1 et x_2 appartiennent à Z(K) donc $(x_1 + x_2)y = yx_1 + yx_2 = y(x_1 + x_2)$: $x_1 + x_2 \in \mathrm{Z(K)}$ donc Z(K) est stable par somme.
- Soit $y \in \mathrm{K}$. $(-x_1)y = x_1(-y) = (-y)x_1 = y(-x_1)$ donc $-x_1 \in \mathrm{Z(K)}$: Z(K) est stable par opposé, c'est un sous-groupe de $(\mathrm{K}, +)$.
- Pour tout $y \in \mathrm{K}, y \times 1 = 1 \times y = y$ donc $1 \in \mathrm{Z(K)}$.
- Soit $y \in \mathrm{K}$. $x_1 x_2 y = x_1 y x_2 = y x_1 x_2$ car, successivement, x_2 et x_1 appartiennent à Z(K). On en déduit que $x_1 x_2 \in \mathrm{Z(K)}$: Z(K) est donc stable par produit.
- Supposons enfin que x_1 soit non nul. Soit $y \in \mathrm{K}$. Si $y = 0$ alors on a évidemment ${x_1}^{-1} y = y {x_1}^{-1}$. Si y est non nul, alors y est inversible (on est dans un corps) donc $x_1 y^{-1} = y^{-1} x_1$ et, en inversant (en changeant l'ordre), $y {x_1}^{-1} = {x_1}^{-1} y$ donc on a bien ${x_1}^{-1} \in \mathrm{Z(K)}$: Z(K) **privé de** 0 est stable par inverse.

Z(K) est un sous-corps de K.

3 Par définition, Z(K) est l'ensemble des éléments qui commutent avec tous les éléments de K. Si $n = 1$ alors $\mathrm{K} = \mathrm{Z(K)}$ donc tous les éléments de $\mathrm{K} = \mathrm{Z(K)}$ commutent avec tous les éléments de K, c'est-à-dire que K est commutatif, ce qui est absurde.

$n > 1$

4 Z_a est l'ensemble des éléments de K qui commutent avec a. Or, si un élément commute avec tous les éléments de K, il commute en particulier avec a. En d'autres termes, tout élément de Z(K) appartient à Z_a, d'où l'inclusion $\mathrm{Z(K)} \subset \mathrm{Z}_a$. Or, a commute évidemment avec lui-même donc $a \in \mathrm{Z}_a$ mais, par définition de a, $a \notin \mathrm{Z(K)}$ donc l'inclusion est bien stricte.

$\boxed{\mathrm{Z(K)} \text{ est inclus strictement dans } \mathrm{Z}_a.}$

5.(a) Cette quantité est égale à $q^{pd+r} - q^r + q^r - 1$ et puisque $n = pd + r$, on a :

$$\boxed{q^r(q^{pd} - 1) + (q^r - 1) = q^n - 1}$$

5.(b) q étant un nombre premier, il est distinct de 1. On reconnaît une somme géométrique de raison $q^d \neq 1$, si bien que :

$$\boxed{1 + q^d + q^{2d} + \cdots + q^{(p-1)d} = \frac{1 - q^{pd}}{1 - q^d} = \frac{q^{pd} - 1}{q^d - 1}}$$

5.(c) D'après la question précédente, $q^{pd} - 1 = (1 + q^d + \cdots + q^{(p-1)d})(q^d - 1)$. D'après la question 5.(a) :

$$q^n - 1 = q^r \times (1 + q^d + \cdots + q^{(p-1)d}) \times (q^d - 1) + (q^r - 1)$$

Or, d'après le théorème de division euclidienne (sur $\mathbb{Z}$), $r < d$ et $q \geqslant 2$ donc $q^r < q^d$ et donc $q^r - 1 < q^d - 1$. Par unicité de la division euclidienne (une fois la condition sur le reste vérifiée), on a le résultat voulu.

$\boxed{\text{Le reste de la division euclidienne de } q^n - 1 \text{ par } q^d - 1 \text{ est } q^r - 1 \text{ (et le quotient est } q^r \times (1 + q^d + \cdots + q^{(p-1)d})).}$

5.(d) K_a étant un corps, ${\mathrm{K}_a}^*$ est un groupe, inclus dans K^* (qui est un groupe pour la même raison), c'est donc un sous-groupe de K^*, et le théorème de Lagrange permet de conclure.

$$\boxed{q^d - 1 \text{ divise } q^n - 1.}$$

Il en découle que le reste dans la division euclidienne est nul, c'est-à-dire (question précédente) que $q^r - 1 = 0$, c'est-à-dire que $q^r = 1$. Or, $q \geqslant 2$ donc $r = 0$, c'est-à-dire que

$$\boxed{d \text{ divise } n.}$$

6.(a) À l'aide d'un simple regroupement par paquets (mais il est inutile d'employer des mots savants, l'égalité qui suit peut être donnée directement sans justification, tant elle est évidente) :

$$\prod_{m|n} \Phi_m = \prod_{m|n, m|d} \Phi_m \times \prod_{m|n, m\nmid d} \Phi_m$$

Or, d étant un diviseur de n, un diviseur de d divise forcément n donc :

$$\prod_{m|n} \Phi_m = \prod_{m|d} \Phi_m \times \prod_{m|n, m\nmid d} \Phi_m$$

Le premier polynôme, d'après la partie précédente, est égal à $\mathrm{X}^n - 1$, et le second à $\mathrm{X}^d - 1$, ce qui donne le résultat voulu.

$$\boxed{\frac{\mathrm{X}^n - 1}{\mathrm{X}^d - 1} = \prod_{m|n, m\nmid d} \Phi_m}$$

6.(b) En évaluant l'égalité précédente en q (qui n'est pas une valeur interdite de la fonction rationnelle associée car $q^d - 1 \neq 1$) :

$$\frac{q^n - 1}{q^d - 1} = \prod_{m|n, m\nmid d} \Phi_m(q)$$

Or, $d \neq n$ par hypothèse donc $m = n$ est un diviseur de n et pas un diviseur de d. En d'autres termes, le produit ci-dessus contient $\Phi_n(q)$, si bien que :

$$\frac{q^n - 1}{q^d - 1} = \prod_{m|n, m\nmid d, m\neq n} \Phi_m(q) \times \Phi_n(q)$$

Un polynôme cyclotomique étant à coefficients entiers (partie II), $\Phi_m(q) \in \mathbb{Z}$ pour tout m, donc le produit ci-dessus est bien un entier.

$$\boxed{\text{Si } d \neq n, \text{ alors } \Phi_n(q) \text{ divise (dans } \mathbb{Z}) \ \frac{q^n - 1}{q^d - 1}.}$$

7.(a) Montrons que c'est une relation d'équivalence.

- Soit $x \in \mathrm{K}^*$. Alors $1 \times x \times 1^{-1} = x$ et $1 \in \mathrm{K}^*$ donc $x \sim x$: $\sim$ est réflexive.
- Soient x et $y \in \mathrm{K}^*$ tels que $x \sim y$. Il existe donc $g \in \mathrm{K}^*$ tel que $gxg^{-1} = \mathrm{K}$. En multipliant par g à droite et g^{-1} à gauche (attention, K n'est pas supposé commutatif), on obtient $g^{-1}yg = x$ c'est-à-dire :

$$g^{-1}y\left(g^{-1}\right)^{-1} = x$$

  En d'autres termes, $y \sim x$: $\sim$ est une relation d'équivalence.
- Soient enfin $x, y, z \in \mathrm{K}^*$ tels que $x \sim y$ et $y \sim z$. Il existe alors g_1 et g_2 tels que $g_1 x {g_1}^{-1} = y$ et $g_2 y {g_2}^{-1} = z$. Dès lors :

$$\begin{aligned} z &= g_2(g_1 y {g_1}^{-1}){g_2}^{-1} \\ &= (g_2 g_1) y (g_2 g_1)^{-1} \end{aligned}$$

  et $g_2 g_1 \in \mathrm{K}^*$ (soit parce que K est un corps donc un anneau intègre, donc un produit d'éléments non nuls est non nul, soit parce qu'un produit d'éléments inversibles est inversible) donc $x \sim z$: $\sim$ est transitive.

$\boxed{\sim \text{ est une relation d'équivalence.}}$

7.(b) On pourrait le prouver par double inclusion, mais on peut aussi (pour aller plus vite) travailler par équivalence. Soit $g \in \mathrm{K}^*$. Alors :

$$g \in \mathrm{Stab}(x) \iff gxg^{-1} = x \iff gx = xg \iff g \in {\mathrm{Z}_x}^*$$

On a écrit ${\mathrm{Z}_x}^*$ et non pas Z_x car g est non nul par hypothèse. D'où le résultat.

$\boxed{\mathrm{Stab}(x) = {\mathrm{Z}_x}^*}$

8 Puisque les x de la somme n'appartiennent pas à $\mathrm{Z(K)}$, on peut appliquer les questions 4, 5 et 6. En remplaçant les cardinaux par leur valeur, on obtient donc :

$$q^n - 1 = q - 1 + \sum_{\mathrm{cl}(x) \mid \mathrm{Card}\,(\mathrm{cl}(x)) \geqslant 2} \frac{q^n - 1}{q^d - 1}$$

avec d un entier divisant n (question 5.(d)). Précisons que d n'est pas le même pour tout x, d dépend du x choisi (on pourrait le noter d_x mais on ne le fait pas pour ne pas surcharger l'écriture). Cependant, une chose ne change pas : si le cardinal de l'orbite est supérieur ou égal à 2, c'est que $d \neq n$ (et on rappelle que $d|n$). Par conséquent, dans la somme ci-dessus, tous les d de la somme ci-dessus divisent n et sont distincts de n donc, d'après la question 6.(b), tous les termes de la somme sont divisibles par $\Phi_n(q)$. Or, $\Phi_n(q)$ divise $q^n - 1$ (question 4.(d) de la partie II, évaluée en q). Le résultat en découle.

$\boxed{\Phi_n(q) \text{ divise } q - 1.}$

9 $n \neq 1$ donc $\omega \neq 1$ (1 n'est pas une racine primitive n-ième de l'unité puisque $n > 1$). Dès lors, $\mathrm{Re}\,(\omega) < 1$ (seul 1 a une partie réelle égale à 1 sur le cercle unité : si $z = x + iy \in \mathbb{U}$ alors $x^2 + y^2 = 1$ donc, si $x = 1$, alors $y = 0$ donc $z = 1$, mais on peut aussi l'affirmer directement) donc $q - \mathrm{Re}\,(\omega) > q - 1 > 0$. Par conséquent :

$$\begin{aligned} |q - \omega| &= \sqrt{(q - \mathrm{Re}\,(\omega))^2 + \mathrm{Im}\,(\omega)^2} \\ &\geqslant \sqrt{(q - \mathrm{Re}\,(\omega))^2} && \text{Croissance de la racine carrée} \\ &\geqslant |q - \mathrm{Re}\,(\omega)| \\ &\geqslant q - \mathrm{Re}\,(\omega) && q - \mathrm{Re}\,(\omega) \geqslant 0 \\ &> q - 1 \end{aligned}$$

Or, $\Phi_n(q) = |\Phi_n(q)|$ est le produit des $|q - \omega|$ lorsque ω décrit P_n, l'ensemble des racines primitives n-ièmes de l'unité. Dès lors, $\Phi_n(q)$ est un produit de termes strictement plus grands que $q - 1$ donc (produit d'inégalités positives) est strictement plus grand que $q - 1$, ce qui est absurde puisque $\Phi_n(q) | q - 1$ et $q - 1 \neq 0$ (si $a|b$ et si $b \neq 0$ alors $|a| \leqslant |b|$).

$\boxed{\text{Le théorème de Wedderburn est démontré.}}$

Partie IV. Irréductibilité des polynômes cyclotomiques

1.(a)

- Si P est le polynôme nul, alors $P(\omega) = 0$ donc le polynôme nul appartient à I : I est non vide.
- Soient A_1 et A_2 deux éléments de I. Alors $A_1(\omega) = A_2(\omega) = 0$ donc $(A_1 + A_2)(\omega) = 0$ et $-A_1(\omega) = 0$ donc $A_1 + A_2$ et $-A_1$ appartiennent à I : I est stable par somme et par opposé, donc I est un sous-groupe de $\mathbb{Q}[X]$.
- Enfin, soit $P \in \mathbb{Q}[X]$ et soit $A \in I$. Alors $(PA)(\omega) = P(\omega)A(\omega) = 0$ donc $P \times A \in I$: I est absorbant pour le produit.

I est un idéal de $\mathbb{Q}[X]$.

1.(b) Il suffit de prouver que E est non vide. En effet, il ne contient que des degrés de polynômes non constants donc en particulier de polynômes non nuls donc des entiers (supérieurs ou égaux à 1). En d'autres termes, E est une partie de $\mathbb{N}^*$ et donc il suffit de prouver qu'elle est non vide pour prouver qu'elle admet un plus petit élément. Or, $X^n - 1$ est un élément de I (car ω est une racine n-ième de l'unité) donc $n \in E$ ce qui permet de conclure.

E admet un plus petit élément d.

> On aurait aussi pu dire que Φ_n appartient à I car ω est une racine primitive n-ième de l'unité donc annule Φ_n par définition de Φ_n, et donc $\deg(\Phi_n) \in E$ (Φ_n non constant car est divisible par $X - \omega$). Attention cependant, car on ne connaît pas son degré ! Il n'est pas de degré n ! Il est de degré $\varphi(n)$ où $\varphi(n)$ est le nombre d'entiers de $[\![\, 0\,;\, n-1 \,]\!]$ premiers avec n (la fonction φ est appelée indicatrice d'Euler et est au programme de deuxième année).

1.(c) d étant un plus petit élément, il appartient à E donc il existe $A \in I$ (non constant) de degré d. I étant absorbant pour le produit, si on note α le coefficient dominant (non nul par définition) de A, alors $(1/\alpha) \times A \in I$ et c'est un polynôme unitaire.

I contient un polynôme unitaire de degré d.

1.(d) Soit $P \in I$. Effectuons la division euclidienne de P par M : il existe Q et $R \in \mathbb{Q}[X]$ uniques tels que $P = QM + R$ donc $R = P - QM$ (avec $\deg(R) < \deg(M)$). $P \in I$ et $M \in I$ donc (I absorbant) $QM \in I$ et I est un groupe donc $P - QM \in I$. Or, M est de degré minimal parmi les polynômes non constants de I donc R est constant, et puisque $R \in I$, alors $R(\omega) = 0$ donc R est le polynôme nul, c'est-à-dire que M divise P.

M divise tous les éléments de I.

> La réciproque est vraie, c'est-à-dire que tout multiple de M appartient à I car I est absorbant. En d'autres termes, I est exactement l'ensemble des multiples de M c'est-à-dire :
>
> $$I = \{QM \mid Q \in \mathbb{Q}[X]\}$$
>
> On dit que M est le polynôme minimal de ω sur $\mathbb{Q}$, cf. cours de deuxième année et DS n° 5 (sujet B) d'il y a deux ans !

2.(a) Puisque ω est une racine primitive n-ième de l'unité, ω est racine de Φ_n donc $\Phi_n(\omega) = A(\omega)B(\omega) = 0$. Un produit de facteurs est nul si et seulement si l'un au moins des facteurs est nul.

ω est racine de A ou de B.

2.(b) $A \in I$ puisque ω est une racine de A donc, d'après la question 1.(d), A est divisible par M, et $\Phi_n = AB$ ce qui permet de conclure.

Il existe $P \in \mathbb{Q}[X]$ tel que $\Phi_n = M \times P \times B$.

2.(c) Soit z une racine primitive n-ième de l'unité. D'après la question 3.(c) de la partie I, il existe u premier avec n tel que $z = \omega^u$. Notons $u = p_1 \times \cdots \times p_k$ avec les p_i des nombres premiers (pas forcément distincts). Puisque u est premier avec n, alors les p_i sont tous premiers avec n (en effet, si l'un des p_i n'est pas premier avec n, il existe $d > 1$ qui divise n et p_i donc d divise u et n ce qui est exclu), c'est-à-dire ne divisent pas n car ils sont premiers. D'après le lemme-clef, ω est racine de M donc ω^{p_1} est racine de M. On applique le lemme-clef avec ω^{p_1} à la place de z (penser à « truc ») : $(\omega^{p_1})^{p_2} = \omega^{p_1 p_2}$ est encore racine de M, et on continue jusqu'à obtenir $z = \omega^u = \omega^{p_1 \cdots p_k}$ racine de M.

Toutes les racines primitives de l'unité sont racines de M.

2.(d) Les racines primitives de l'unité étant deux à deux distinctes, d'après le cours,

$$\prod_{\omega \in \mathrm{P}_n} (\mathrm{X} - \omega) | \mathrm{M}$$

c'est-à-dire que Φ_n divise M. Or, M divise Φ_n : ceux deux polynômes sont associés donc ont le même degré, et comme $\Phi_n = \mathrm{M} \times \mathrm{P} \times \mathrm{B}$, $\deg(\mathrm{PB}) = \deg(\mathrm{P}) + \deg(\mathrm{B}) = 0$ et en particulier $\deg(\mathrm{B}) = 0$: B est constant.

B est constant : Φ_n est irréductible.

> Si p est premier, on a vu (question 3.(b) de la partie II) que Φ_p est de degré $p-1$. Puisqu'il y a une infinité de nombres premiers, pour tout n, il existe un polynôme Φ_p tel que $\deg(\Phi_p) \geqslant n$. Par conséquent, alors que les irréductibles sur $\mathbb{C}[\mathrm{X}]$ et sur $\mathbb{R}[\mathrm{X}]$ sont assez simples (cf. cours), sur $\mathbb{Q}$, il existe des polynômes irréductibles de degré arbitrairement grand !