# Polynômes cyclotomiques, $\mathbb{Z}[X]$ & $\sum_{i=1}^{n} \alpha_i^k$

## Notations :

Pour un entier naturel $n$ donné, on note :
- $G_n = X^n - 1$ (en hommage au grand Gauss) ;
- $\mathbb{U}_n = \mathcal{Z}_{G_n}$, l'ensemble des zéros de $G_n$, c'est-à-dire l'ensemble des racines $n$-ième de l'unité ;
- $\mathbb{V}_n = \{z \in \mathbb{U}_n \mid \forall\, r \in [\![1, n-1]\!], z^r \neq 1\}$, ce sont les racines primitives $n$-ième de l'unité ;
- $\varphi(n) = \text{card}(\mathbb{V}_n)$ et $\Phi_n = \prod_{z \in \mathbb{V}_n} (X - z)$ ($\leftarrow$ *ce sont eux les polynômes cylcotomiques*).

# 1 Factorisation dans $\mathbb{Z}[X]$

On considère un nombre premier $p$ et $P, Q \in \mathbb{Z}[X]$, deux polynômes à coefficients entiers.

▷ **1.1.** Factorisation $\mathbb{Z}[X]$

1. Redonner, pour tout $n \in \mathbb{Z}$, l'expression de $[P \times Q]_n$, en fonction des nombres $([P]_i)_{0 \leqslant i \leqslant n}$ et $([Q]_j)_{0 \leqslant j \leqslant n}$.
2. On va montrer, par contraposée, l'implication : $(\forall\, n \in \mathbb{N},\ p | [PQ]_n) \Longrightarrow (\forall\, n \in \mathbb{N},\ p | [P]_n$ ou $\forall\, n \in \mathbb{N},\ p | [Q]_n)$.
   (a) Supposons donc que $\{n$ tel que $p \nmid [P]_n\}$ et $\{n$ tel que $p \nmid [Q]_n\}$ sont non vides (et inclus dans $\mathbb{N}$). Soient $m = \min\{n$ tel que $p \nmid [P]_n\}$ et $m' = \min\{n$ tel que $p \nmid [Q]_n\}$. Montrer que $p$ ne divise pas $[PQ]_{m+m'}$
   (b) Conclure.

▷ **1.2.** Contenu d'un polynôme de $\mathbb{Z}[X]$

On note, pour $R \in \mathbb{Z}[X]^*$, $c(R) = \bigwedge_{k=0}^{\deg R} [R]_k$ (PGCD des coefficients de $R$), appelé « contenu de $R$ »(et $c(0) = 0$).

Par exemple, $c(2X^3 + 4X - 6) = 2 \wedge 0 \wedge 4 \wedge 6 = 2$ ou $c(6X^4 + 10X^2 - 15X) = 6 \wedge 0 \wedge 10 \wedge 0 \wedge 15 = 1$.

1. Montrer que $P_1 := \dfrac{P}{c(P)}$ est un polynôme à coefficients entiers, puis que $c(P_1) = 1$.
2. En exploitant l'exercice précédent, et les polynômes $P_1$ et $Q_1$, montrer que $c(P \times Q) = c(P) \times c(Q)$

▷ **1.3.** Factorisation(/irréductibilité) dans $\mathbb{Q}[X]/\mathbb{Z}[X]$

1. Soit $R \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$. Montrer que $R$ est irréductible dans $\mathbb{Z}[X]$ ssi $R$ est irréductible dans $\mathbb{Q}[X]$.
2. Soit $p$ un nombre premier et $R = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. On note $\overline{R} = \sum_{k=0}^{n} \overline{a_k} X^k$ (avec $\overline{a_k} = a_k \% p$).
   Montrer que $\overline{R}(X^p) = (\overline{R}(X))^p$. *On pourra raisonner par récurrence forte sur $n = \deg R$.*

# 2 Décomposition des polynômes $G_n$. Polynômes cyclotomiques

▷ **2.1.**

1. Effectuer, *en parallèle*, l'algorithme d'Euclide pour les nombres 14 et 3 et pour les polynômes $G_{14}$ et $G_3$. Donner un couple d'entiers $(u, v)$ et un couple de polynômes $(U, V)$ tels que $14u + 3v = 1$ et $G_{14} \times U + G_3 \times V = G_1$.
2. Montrer que pour tous entiers $m > n \geqslant 1$, $G_m \wedge G_n = G_{m \wedge n}$
3. Factoriser $G_3$ et $G_4$ sur $\mathbb{C}[X]$, puis sur $\mathbb{R}[X]$.

4. Factoriser $G_n$ sur $\mathbb{R}[X]$. On notera, pour $1 \leqslant k \leqslant n$, $c_{k,n} = \cos\dfrac{2k\pi}{n}$.

Soit $n \in \mathbb{N}$, fixé. On cherche à factoriser $G_n$ en produit de polynômes de $\mathbb{Q}[X]$ (donc de $\mathbb{Z}[X]$) (questions 2.4).

▷ **2.2.**

On commence par trouver une factorisation

1. On note, pour tout $k \in \mathbb{N}$, $z_k = e^{\frac{2ik\pi}{n}}$. On sait que $\mathbb{U}_n = \{z_k ; k \in [\![1, n]\!]\}$.
   Montrer que $z_k \in \mathbb{V}_n \iff \exists\, u \in \mathbb{Z}$ tel que $(z_k)^u = z_1 \iff k \wedge n = 1$.
2. Montrer que $\mathbb{U}_n = \uplus_{d|n} \mathbb{V}_d$.
   Donner la description des éléments de $\mathbb{U}_{12}$ regroupés selon les $\mathbb{V}_k$ auxquels ils appartiennent.
3. Déduire de la réunion disjointe précédente, que $G_n = \prod_{d|n} \Phi_d$. Que vaut $\Phi_{12}$ ?
4. Montrer, par récurrence forte sur $m \in \mathbb{N}^*$ que $\Phi_m \in \mathbb{Z}[X]$ et est unitaire.
5. Quel est le de degré de $\Phi_m$ ? En déduire la valeur de $\sum_{d|n} \varphi(d)$, en fonction de $n$.
6. Montrer que si $p$ est un nombre premier et $k \geqslant 1$ est un entier, alors
$$\Phi_{p^k} = X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + \cdots + X^{p^{k-1}} + 1$$
7. Calculer $\Phi_n$, pour $n \in \{5, 6\}$.

▷ **2.3.**

1. Soit $n \in \mathbb{N}$, $n \geqslant 2$. Calculer $\Phi_n(0)$
2. Calculer, pour $n \geqslant 2$, $\Phi_n(1)$ en fonction de la décomposition en facteurs premiers de $n$. *Raisonner par récurrence, en utilisant la première question.*

▷ **2.4.**

On démontre maintenant qu'il n'y a pas d'autres factorisations dans $\mathbb{Z}[X]$, ie que $\Phi_n$ est irréductible.

Supposons pour cela que $\Phi_n = \lambda \prod_{i=1}^{r} P_i$ où chaque $P_r$ est un polynôme irréductible et unitaire de $\mathbb{Q}[X]$ et $\lambda \in \mathbb{Q}$.

1. Montrer que $\lambda = 1$.
2. Soit $z$ une racine de $P_1$ et $p$ premier tel que $p \nmid n$. Montrer qu'il existe $i$ tel que $P_i(z^p) = 0$.
3. Montrer que $\overline{\Phi_n}$ (défini en I.5) n'est divisible par le carré d'aucun polynôme non constant dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.
   *Par l'absurde, on montrer qu'il existe $Q$ tel que $\overline{Q}|\overline{G_n}$ et $\overline{Q}|\overline{G_n'}$ puis $\overline{Q}|X\overline{G_n'} - \overline{n}\overline{G_n}$...*
4. (**) Montrer que $i = 1$, i.e. $P_1(z^p) = 0$, puis que pour tout $k$ entier, premier avec $n$, $P_1(z^k) = 0$.
5. Conclure

# 3 Sommes des puissances des racines

Soit $Q$ un polynôme de degré $n$ de $\mathbb{C}[X]$ : $Q(X) = \sum_{k=0}^{n} b_k X^k$.

On note $\alpha_1, \cdots, \alpha_n$ ses racines complexes, distinctes ou non et on a donc : $Q(X) = b_n \prod_{i=1}^{n} (X - \alpha_i)$.

On note, pour tout $k \in \mathbb{N}^*$ : $T_k = \sum_{i=1}^{n} \alpha_i^k$ et $T_0 = n$.

L'objectif est de calculer les termes de la suite $(T_k)_{k\in\mathbb{N}}$ à partir des coefficients du polynôme $Q$.

▷ **3.1.** Exploiter le polynôme $Q$

1. Soit $i \in [\![1, n]\!]$. On note $Q_i$ le polynôme (justifié par la question suivante) défini par : $Q_i(X) = \dfrac{Q(X)}{X - \alpha_i}$.
   Montrer que $Q'$ est une combinaison linéaire des $Q_i$ que l'on déterminera.

2. En remarquant que $Q_i(X) = \dfrac{Q(X) - Q(\alpha_i)}{X - \alpha_i}$, montrer que l'on a :

$$Q_i(X) = \sum_{r=1}^{n} \left( \sum_{k=r}^{n} b_k \alpha_i^{k-r} \right) X^{r-1}$$

3. Déduire des questions précédentes que l'on a :

$$\forall r \in [\![1, n]\!], \qquad r b_r = \sum_{j=0}^{n-r} b_{r+j} T_j$$

▷ **3.2.** Relation de récurrence

1. Soit $k \in [\![1, n-1]\!]$. Exprimer $T_k$ en fonction de $T_0, \cdots, T_{k-1}$ et des coefficients du polynôme $Q$.
2. Soit $k \geqslant n$.
   (a) Montrer que l'on a : $\displaystyle\sum_{j=0}^{n} b_j T_{k-n+j} = 0$.
   (b) Exprimer alors $T_k$ à l'aide de $T_{k-n}, T_{k-n+1}, \cdots, T_{k-1}$ et des coefficients du polynôme $Q$.
3. Conclure.

▷ **3.3.**

Soit $P \in \mathbb{Z}[X]$, un polynôme unitaire de degré $n \geqslant 1$, irréductible dans $\mathbb{Q}[X]$ et dont toutes les racines complexes sont de module 1.
L'objectif est de montrer que toutes les racines de $P$ sont alors des racines de l'unité. Soient $z_1, \dots z_n$ les racines complexes de $P$ comptées avec leurs multiplicités, de sorte que

$$P = \prod_{i=1}^{n} (X - z_i)$$

Pour tout entier $k$, $S_k = z_1^k + z_2^k + \cdots + z_n^k$.

1. Pourquoi est-ce que pour tout entier $k \in \mathbb{N}$, $S_k \in \mathbb{Z}$.
2. Montrer qu'il existe deux entiers $k$ et $\ell$ $(0 \leqslant k < \ell)$ tels que $S_{k+i} = S_{\ell+i}$ pour tout $i \in \{0, 1, \dots n\}$.

On fixe $k$ et $\ell$.

3. Montrer que $\displaystyle\sum_{i=1}^{n} F(z_i)(z_i^\ell - z_i^k) = 0$, pour tout polynôme $F \in \mathbb{C}[X]$ de degré inférieur ou égal à $n$.
4. Montrer que $z_1, z_2, \dots z_n$ sont deux à deux distincts.
   En déduire que $z_i^{\ell-k} = 1$, pour tout $i \in \{1, 2, \dots n\}$ et conclure.

# 4 Application à la résolution d'un problème diophantien

Soit $p$ et $q$ deux nombres premiers vérifiant $3 \leqslant p < q$. On note $< p, q >= \{mp + nq, m, n \in \mathbb{N}\}$.
*Soulignons, que les nombres $m$ et $n$ sont des entiers naturels et non des entiers relatifs.*

▷ **4.1.**

1. Montrer que tout nombre entier $R \geqslant (p-1)(q-1)$ appartient à $< p, q >$.
2. Le nombre $(p-1)(q-1) - 1$ appartient-il à $< p, q >$ ?

▷ **4.2.**

On définit les polynômes $H = \displaystyle\sum_{s \in \mathbb{N} \setminus < p,q >} X^s$ et $K = 1 + (X-1)H(X)$, qui sont donc à coefficients entiers.

1. Quels sont les degré de $H$ et de $K$ ?
2. Calculer $K$ pour le choix $(p, q) = (3, 5)$.

▷ **4.3.**

Considérons deux polynômes $S, T \in \mathbb{Z}[X]$ tel que pour tout $k \in \mathbb{N}$, $[S]_k \in \{0, 1\}$ et $T = (X-1)S$

1. Exprimer pour tout $k \in \mathbb{N}$, $[T]_k$ en fonction des coefficients de $S$. En déduire que $[T]_k \in \{-1, 0, 1\}$.

2. Soient $k_1 < k_2 \in \mathbb{N}$ tel que $[T]_{k_1} \neq 0$, $[T]_{k_2} \neq 0$ et pour tout $k \in [\![k_1+1, k_2-1]\!]$, $[T]_k = 0$.
   Montrer que $[T]_{k_1} \times [T]_{k_2} = -1$.
3. En déduire que $K$ n'a que des coefficients égaux à $-1$, 0 ou 1 et que les 1 et $-1$ s'alternent dans la suite des coefficients (il ne peut y avoir que des zéros comme coefficient entre ces nombres).

On admet (raisonnement combinatoire) que

$$G_p \times G_q \times K = G_{pq} \times G_1$$

4. Quelles sont les racines de $K$, avec quelle multiplicité ?

On peut appliquer la factorisation de la partie précédente, $p$ étant premier $\mathbb{U}_p = \uplus_{d|p} \mathbb{V}_d = \mathbb{V}_1 \uplus \mathbb{V}_p = \{1\} \uplus \mathbb{V}_p$.

$$X^p - 1 = G_p = (X-1)\Phi_p$$

On peut faire la division euclidienne : $\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1 = \sum_{h=0}^{p-1} X^h$.

On a donc $G_p G_q K = (X-1)^2 \Phi_p \Phi_q K = G_{pq}(X-1) = (X-1)\prod_{d|pq} \Phi_d = (X-1)^2 \Phi_p \Phi_q \times \prod_{d|pq, d\notin\{1,p,q\}} \Phi_d$.

On peut simplifier par $(X-1)^2\Phi_p\Phi_q$ : $K = \prod_{d|pq, d\notin\{1,p,q\}} \Phi_d$.

Mais l'ensemble des diviseurs de $pq$ est $\{1, p, q, pq\}$ car $p$ et $q$ sont des nombres premiers. Donc $K = \Phi_{pq}$

▷ **4.4.**

D'après la question II.1., il existe $\alpha, \beta \in \mathbb{N}$ tel que $pq + 1 = \alpha p + \beta q$.

1. Vérifier que $1 \leqslant \alpha \leqslant q-1$ et $1 \leqslant \beta \leqslant p-1$.
2. Montrer la formule :

$$K = \left(\sum_{i=0}^{\alpha-1} X^{ip}\right) \times \left(\sum_{j=0}^{\beta-1} X^{jq}\right) - X^{-pq} \left(\sum_{i=\alpha}^{q-1} X^{ip}\right) \times \left(\sum_{j=\beta}^{p-1} X^{jq}\right).$$

3. Montrer que le nombre $N$ de coefficients non nuls $[K]_j$ de $K$ est égal à $2\alpha\beta - 1$.
4. En déduire que $N \leqslant \dfrac{pq-1}{2}$.

   On pourra commencer par montrer que $N$ est inférieur à $\dfrac{p^2q^2+1}{2pq}$.

# Correction des exercices

## ▷ Corrigé de l'exercice 1.1

1. Formule du cours. Elle marche même pour $n \geqslant \deg P + \deg Q \ldots$ :

$$\boxed{\forall\, n \in \mathbb{N}, [P \times Q]_n = \sum_{i=0}^{n} [P]_i \times [Q]_{n-i} = \sum_{i+j=n}^{n} [P]_i \times [Q]_j}$$

2. D'après la formule précédente, en séparant la somme en trois parties :

$$[PQ]_{m+m'} = \sum_{i=0}^{m+m'} [P]_i [Q]_{m+m'-i} = \sum_{i=0}^{m-1} [P]_i [Q]_{m+m'-i} + [P]_m [Q]_{m'} + \sum_{i=m+1}^{m+m'} [P]_i [Q]_{m+m'-i}$$

Or, pour tout $i \leqslant m-1$, $p|[P]_i$. Donc , par combinaison linéaire entière : $p \Big| \sum_{i=0}^{m-1} [P]_i [Q]_{m+m'-i}$.

Et, pour tout $i \geqslant m+1$, $m+m'-i \leqslant m'-1$, donc $p|[Q]_{m+m'-i}$, par définition de $m'$.

Donc , par combinaison linéaire entière : $p \Big| \sum_{i=m+1}^{m+m'} [P]_i [Q]_{m+m'-i}$.

Donc $p|[PQ]_{m+m'}$ si et seulement si $p|[P]_m [Q]_{m'}$.

Or $p$ est un nombre premier, donc $p$ divise $[P]_m \times [Q]_{m'}$ si et seulement si il divise l'un des deux termes.

Mais ceci est faux par définition de $m$ et de $m'$.

$$\boxed{\text{Par conséquent } p \text{ ne divise pas } [PQ]_{m+m'}.}$$

3. En notant $\mathcal{P}_P$ : « $\{n$ tel que $p \not| [P]_n\}$ est non vide » ; $\mathcal{P}_Q$ : « $\{n$ tel que $p \not| [Q]_n\}$ est non vide »et $\mathcal{P}_{PQ}$ : « $\{n$ tel que $p \not| [PQ]_n\}$ est non vide », on a démontré : $\mathcal{P}_P$ et $\mathcal{P}_Q \Longrightarrow \mathcal{P}_{PQ}$.
La contraposée de cette implication affirme donc : $NON(\mathcal{P}_{PQ}) \Longrightarrow NON(\mathcal{P}_P)$ ou $NON(\mathcal{P}_Q)$.
Or $NON(\mathcal{P}_P)$ signifie $\{n$ tel que $p \not| [P]_n\}$ est vide, i.e. $\forall\, n \in \mathbb{N}$, $p|[P]_n$.
On a donc montré :

$$\boxed{\begin{array}{c}\text{Si } p \text{ divise tous les coefficients d'un produit de polynômes entiers } P \times Q, \\ \text{alors } p \text{ divise tous les coefficients de } P \text{ ou } p \text{ divise tous les coefficients de } Q.\end{array}}$$

## ▷ Corrigé de l'exercice 1.2

1. Puisque $c(P)$ est le PGCD des nombres $[P]_k$, alors pour tout $k \in \mathbb{N}$, $c(P)$ divise $[P]_k$.

$$\boxed{\text{Donc pour tout entier } k \in \mathbb{N},\ [P_1]_k = \frac{[P]_k}{c(P)} \in \mathbb{Z} \text{ et donc } P_1 \in \mathbb{Z}[X].}$$

Notons $\delta = c(P_1)$, le PGCD des coefficients de $P_1$. Alors, pour tout $k \in \mathbb{N}$, $\delta|[P_1]_k = \dfrac{[P]_k}{c(P)}$, donc $c(P)\delta|[P]_k$.

Comme $c(P)\delta$ divise tous les nombres $[P]_k$, il divise alors leurs PGCD, donc $c(P)$.
Donc $\delta$ divise 1, il vaut donc 1.

$$\boxed{c(P_1) = 1}$$

2. Considérons donc $P_1 = \dfrac{P}{c(P)}$ et $Q_1 = \dfrac{Q}{c(Q)}$.

On a donc $c(P_1) = c(Q_1) = 1$ et $P \times Q = c(P)P_1 \times c(Q)Q_1 = c(P)c(Q)P_1 \times Q_1$.
Si $c(P_1Q_1) \neq 1$, considérons $p$ un diviseur premier de $c(P_1 \times Q_1)$,
donc par transitivité $p$ divise tous les coefficients $[P_1Q_1]_n$
D'après la question 2, alors $p$ divise tous les coefficients de $P_1$ ou bien $p$ divise tous les coefficients de $Q_1$.

Ainsi $p$ divise $c_1(P)=1$ ou bien $p$ divise $c_1(Q)=1$.

Cela est impossible car $p \geqslant 2$, donc $c(P_1Q_1)=1\,(=c(P1)c(Q_1))$.

Enfin, montrons que $c(\lambda T)=|\lambda|c(T)$, pour tout $\lambda \in \mathbb{Z}$ et $P \in \mathbb{Z}[X]$

$$\begin{aligned} d|c(\lambda T) &\iff \forall\, n\in\mathbb{N}, d \mid [\lambda T]_n \iff \forall\, n\in\mathbb{N}, d \mid \lambda [T]_n \\ &\iff \forall\, n\in\mathbb{N}, \frac{d}{\lambda} \mid [T]_n \iff \frac{d}{\lambda} \mid c(T) \iff d \mid \lambda c(T) \end{aligned}$$

Les diviseurs de $c(\lambda T)$ et ceux de $\lambda c(T)$ sont les mêmes ; ces deux nombres sont associés.

Comme $c(T)>0$ et $c(\lambda T)>0$ : $c(\lambda T)=|\lambda|c(T)$.

Bilan : $c(PQ)=c(c(P)P_1c(Q)Q_1)=|c(P)c(Q)|c(P_1Q_1)=c(P)c(Q)$

$$\boxed{c(PQ)=c(P)c(Q)}$$

### ▷ Corrigé de l'exercice 1.3

1. Si $R$ n'est pas irréductible dans $\mathbb{Z}[X]$,

il existe deux polynômes $R_1$ et $R_2 \in \mathbb{Z}[X]$ tels que $R=R_1\times R_2$ et $\deg R_1>0$, $\deg R_2>0$.

Alors comme $R_1$ et $R_2$ sont aussi à coefficients dans $\mathbb{Z}$ donc dans $\mathbb{Q}$, $R$ n'est pas irréductibles dans $\mathbb{Q}[X]$.

Par contraposée : $R$ irréductible dans $\mathbb{Q}[X]$ implique $R$ irréductible dans $\mathbb{Z}[X]$.

Réciproquement, supposons que $R(\in \mathbb{Z}[X])$ n'est pas irréductible dans $\mathbb{Q}[X]$,

il existe deux polynômes $R_1$ et $R_2 \in \mathbb{Q}[X]$ tels que $R=R_1\times R_2$ et $\deg R_1>0$, $\deg R_2>0$.

Pour tout $n\in\mathbb{N}$, $[R_1]_n=\dfrac{a_n}{b_n}\in\mathbb{Q}$, fraction écrite sous forme irréductible ($a_n\wedge b_n=1$).

Notons $m_1=PPCM(b_i)$ et donc pour tout $n\in\mathbb{N}$, $b_n|m_1$, notons $c_n=\dfrac{m_1}{b_n}\in\mathbb{Z}$ et $S_1=m_1\times R_1$.

On a donc pour tout entier $n\in\mathbb{N}$, $[S_1]_n=m_1\dfrac{a_n}{b_n}=c_na_n\in\mathbb{Z}$. Donc $S_1\in\mathbb{Z}[X]$.

Puis considérons $T_1=\dfrac{S_1}{c(S_1)}$, on a donc $T_1\in\mathbb{Z}[X]$ et $c(T_1)=1$.

De même, il existe $m_2\in\mathbb{N}$ tel que $S_2=m_2\times R_2\in\mathbb{Z}[X]$. Soit $T_2=\dfrac{S_2}{c(S_2)}$, on a $T_2\in\mathbb{Z}[X]$ et $c(T_2)=1$.

Ensuite : $m_1m_2R=m_1R_1\times m_2R_2=S_1\times S_1\in\mathbb{Z}[X]$

Donc $c(S_1)c(S_2)=c(S_1S_2)=c(m_1m_2R)=|m_1m_2|\times c(\underbrace{R}_{\in\mathbb{Z}[X]})=m_1\times m_2\times c(R)$.

Enfin $T_1\times T_2=\dfrac{S_1}{c(S_1)}\times\dfrac{S_2}{c(S_2)}=\dfrac{S_1S_2}{c(S_1)c(S_2)}=\dfrac{m_1m_1R}{m_1m_2c(R)}=\dfrac{R}{c(R)}$.

Ainsi $R=c(R)T_1\times T_2$ n'est pas irréductible dans $\mathbb{Z}[X]$.

Par contraposée : $R$ irréductible dans $\mathbb{Z}[X]$ implique $R$ irréductible dans $\mathbb{Q}[X]$.

$$\boxed{R\in\mathbb{Z}[X] \text{ est irréductible dans } \mathbb{Z}[X] \text{ ssi } R \text{ est irréductible dans } \mathbb{Q}[X].}$$

2. Posons, pour tout $n\in\mathbb{N}\cup\{-\infty\}$, $\mathcal{H}_n$ : « Si $R\in\mathbb{Z}[X]$ avec $\deg R=n$ alors $\overline{R}(X^p)=[\overline{R}(X)]^p$. »

— Si $R=0$, alors $\overline{R}(X^p)=0=[\overline{R}(X)]^p$. Donc $\mathcal{H}_{-\infty}$ est vraie.

— Soit $R$ un polynôme de degré 0, donc $R$ est constant. On peut supposer $R=a_0$.
$\overline{R}(X^p)=\overline{a_0}=\overline{R}(X)]^p$. Donc $\mathcal{H}_0$ est vraie.

— Soit $n\in\mathbb{N}$. Supposons que $\mathcal{H}_k$ est vraie, pour tout $k\leqslant n$ et $k\in\mathbb{N}\cup\{-\infty\}$.
Soit $R$ un polynôme de degré $n+1$, supposons $R\in\mathbb{Z}[X]$, $\deg R=n+1$ et $[R]_{n+1}=a$.
$R=aX^{n+1}+R_1$ avec $\deg R_1\leqslant n$.

On applique la formule du binôme de Newton : $\dfrac{\mathbb{Z}}{p\mathbb{Z}}[X]$ est un anneau commutatif :

$$[\overline{R}(X)]^p=\left(\overline{a}X^n+\overline{R_1}(X)\right)^p=\sum_{i=0}^{p}\overline{\binom{p}{i}}(\overline{a}X^n)^i(\overline{R_1}(X))^{p-i}$$

Or $\dbinom{p}{i}=\dfrac{p(p-1)!}{i(i-1)!((p-1)-(i-1))!}=\dfrac{p}{i}\dbinom{p-1}{i-1}$, donc $p|i\times\dbinom{p}{i}$.

Et $p$ est premier donc pour tout $i\in[\![1,p-1]\!]$, $p\wedge i=1$ ; d'après le théorème de Gauss : $p|\dbinom{p}{i}$.

Finalement, il ne reste plus que :

$$[\overline{R}(X)]^p = \underbrace{(\overline{a}X^n)^0(\overline{R_1}(X))^p}_{i=0} + 0 + \cdots + 0 + \underbrace{(\overline{a}X^n)^p(\overline{R_1}(X))^0}_{i=p} = (\overline{R_1}(X))^p + \overline{a}^p X^{pn}$$

Puis comme $\mathcal{H}_{\deg R_1}$ est vraie, on a $[\overline{R}(X)]^p = \overline{R_1}(X^p) + \overline{a}^p(X^p)^n = \overline{R_1}(X^p) + \overline{a}(X^p)^n$,
en exploitant le petit théorème de Fermat : $\overline{a}^p = \overline{a}[p]$ puisque $p$ est premier.
Et donc $[\overline{R}(X)]^p = (\overline{R_1}(X) + \overline{a}X^n) \circ X^p = \overline{R}(X^p)$.
Par conséquent, $\mathcal{H}_n$ est vraie.

Pour tout polynôme $R \in \mathbb{Z}[X]$, $\overline{R}(X^p) = [\overline{R}(X)]^p$.

## ▷ Corrigé de l'exercice 2.1

1. On a donc, en appliquant l'algorithme d'Euclide :

$$\begin{aligned} 14 &= 3 \times 4 + 2 \\ 3 &= 2 \times 1 + 1 \\ 2 &= 1 \times 2 + 0 \end{aligned}$$

| $u_n$ | $v_n$ | $q_n$ | $au_n + bv_n$ |
|---|---|---|---|
| 1 | 0 | | 14 |
| 0 | 1 | 4 | 3 |
| 1 | −4 | 1 | 2 |
| −1 | 5 | 2 | 1 |

Donc $14 \wedge 3 = 1$ et $(-1) \times 14 + 5 \times 3 = 1$.

Et pour les polynômes :

$$\begin{aligned} X^{14} - 1 &= (X^3 - 1) \times (X^{11} + X^8 + X^5 + X^2) + (X^2 - 1) \\ X^3 - 1 &= (X^2 - 1) \times (X + 1) + (X - 1) \\ X^2 - 1 &= (X - 1) \times (X + 1) + 0 \end{aligned}$$

| $U_n$ | $V_n$ | $Q_n$ | $AU_n + BV_n$ |
|---|---|---|---|
| 1 | 0 | | $G_{14}$ |
| 0 | 1 | $X^{11} + X^8 + X^5 + X^2$ | $G_3$ |
| 1 | $-(X^{11} + X^8 + X^5 + X^2)$ | $X + 1$ | $G_2$ |
| $-(X + 1)$ | $X^{12} + X^{11} + X^9 + X^8 + X^6 + X^5 + X^3 + X^2 + 1$ | $(X + 1)$ | $G_1$ |

Donc $G_{14} \wedge G_3 = G_1$ et $-(X + 1) \times G_{14} + (X^{12} + X^{11} + X^9 + X^8 + X^6 + X^5 + X^3 + X^2 + 1) \times G_3 = G_1$.

2. Soit $m > n \geqslant 1$, deux entiers.
On remarque que pour tout entier $q \in \mathbb{N}$ tel que $m - qn > 0$,

$$G_m = G_n \times (X^{m-n} + X^{m-2n} + \cdots + X^{m-qn}) + X^{m-qn} - 1 = G_n \times \sum_{k=1}^{q} X^{m-kn} + G_{m-qn}$$

En effet, par telescopage :

$$G_n \times \sum_{k=1}^{q} X^{m-kn} = \sum_{k=1}^{q} X^{m-kn+n} - \sum_{k=1}^{q} X^{m-kn} = \sum_{k=0}^{q-1} X^{m-kn} - \sum_{k=1}^{q} X^{m-kn} = X^m - X^{m-qn} = G_m - G_{m-qn}$$

Ainsi, si $q$ est le quotient de la division euclidienne de $m$ par $n$, et $r$ son reste : $G_m = G_n \times \sum_{k=1}^{q} X^{m-qn} + G_r$
Or $\deg G_r = r < n = \deg G_n$. On a donc écrit ici la division euclidienne de $G_m$ par $G_n$.
On a donc $G_m \wedge G_n = G_n \wedge G_r$ où $r$, reste de la division euclidienne de $m$ par $n$.
Notons $(r_i)$ la suite des restes dans l'algorithme d'Euclide appliqué à $m$ et $n$. Et $r_{N-1}$, le dernier reste non nul.
Alors, on a un invariant de boucle : pour tout $k \leqslant N - 1$ : $G_{r_k} \wedge G_{r_{k+1}}$.
Cet invariant vaut $G_{r_0} \wedge G_{r_1} = G_m \wedge G_n$ au début de l'algorithme,
et il a pour valeur $G_{r_{N-1}} \wedge G_{r_N} = G_{m \wedge n} \wedge 0 = G_{m \wedge n}$ en fin d'algorithme.

Pour tous entiers $m > n \geqslant 1$, $G_m \wedge G_n = G_{m \wedge n}$.

3. Ces calculs sont célèbres :

$$\boxed{\begin{array}{c} G_3 = X^3 - 1 = (X-1)(X-j)(X-j^2) = (X-1)(X^2+X+1) \\ G_4 = X^4 - 1 = (X-1)(X-i)(X+1)(X+i) = (X-1)(X+1)(X^2+1) \end{array}}$$

4. Selon la parité de $n$, $-1$ est une racine ($n$ pair) ou non ($n$ impair) de $G_n$.
On commence par factoriser $G_n$ sur $\mathbb{C}[X]$ : on connait exactement les racines de $G_n$, ce sont les éléments de $\mathbb{U}_n$.
On sait également décrire parfaitement $\mathbb{U}_n$ : $\mathbb{U}_n = \{\exp\dfrac{2ik\pi}{n}, k \in [\![0, n-1]\!]\}$

$$G_n = \prod_{z\in\mathbb{U}_n}(X-z) = \prod_{k=0}^{n-1}(X - e^{\frac{2ik\pi}{n}}) = (X-1)\prod_{k=1}^{n-1}(X - e^{\frac{2ik\pi}{n}})$$

Puis, notons que $\overline{e^{\frac{2ik\pi}{n}}} = e^{-\frac{2ik\pi}{n}} = e^{2i\pi - \frac{2ik\pi}{n}} = e^{\frac{2i(n-k)\pi}{n}}$.
Si $n$ est impair, supposons $n = 2h+1$

$$\begin{aligned} G_n &= (X-1)\prod_{k=1}^{h}(X - e^{\frac{2ik\pi}{n}})\prod_{k=h+1}^{2h}(X - e^{\frac{2ik\pi}{n}}) = (X-1)\prod_{k=1}^{h}(X - e^{\frac{2ik\pi}{n}})\underbrace{\prod_{j=1}^{h}(X - e^{\frac{2i(n-j)\pi}{n}})}_{j=n-k=2h+1-k} \\ &= (X-1)\prod_{k=1}^{h}(X - e^{\frac{2ik\pi}{n}})\overline{(X - e^{\frac{2ik\pi}{n}})} = (X-1)\prod_{k=1}^{h}(X^2 - 2\mathrm{Re}(e^{\frac{2ik\pi}{n}})X + |e^{\frac{2ik\pi}{n}}|^2) \\ &= (X-1)\prod_{k=1}^{h}(X^2 - 2c_{k,n}X + 1) \end{aligned}$$

Si $n$ est pair, supposons $n = 2h$

$$\begin{aligned} G_n &= (X-1)\prod_{k=1}^{h-1}(X - e^{\frac{2ik\pi}{n}})(X+1)\prod_{k=h+1}^{2h-1}(X - e^{\frac{2ik\pi}{n}}) = (X-1)(X+1)\prod_{k=1}^{h-1}(X - e^{\frac{2ik\pi}{n}})\underbrace{\prod_{j=1}^{h-1}(X - e^{\frac{2i(n-j)\pi}{n}})}_{j=n-k=2h-k} \\ &= (X-1)(X+1)\prod_{k=1}^{h-1}(X - e^{\frac{2ik\pi}{n}})\overline{(X - e^{\frac{2ik\pi}{n}})} = (X-1)(X+1)\prod_{k=1}^{h-1}(X^2 - 2c_{k,n}X + 1) \end{aligned}$$

$$\boxed{G_{2h} = (X-1)(X+1)\prod_{k=1}^{h-1}(X^2 - 2c_{k,n}X + 1) \text{ et } G_{2h+1} = (X-1)\prod_{k=1}^{h}(X^2 - 2c_{k,n}X + 1)}$$

## ▷ Corrigé de l'exercice 2.2

1. Raisonnons par triple implications.
• Si $z_k \in \mathbb{V}_n$, alors pour tout $u \in [\![1, n-1]\!]$, $z_k^u \neq 1$.
Or $z_k^u \in \mathbb{U}_n$ et $\mathrm{card}(\mathbb{U}_n \setminus \{1\} = n-1$.
Donc :
— ou bien $[\![1, n-1]\!] \to \mathbb{U}_n \setminus \{1\}$, $u \mapsto z_k^u$ est surjective et donc injective,
Dans ce cas $z_1$ admet un antécédent et donc il existe $u \in [\![1, n-1]\!] \subset \mathbb{Z}$ tel que $z_k^u = z_1$.
— ou bien $[\![1, n-1]\!] \to \mathbb{U}_n \setminus \{1\}$, $u \mapsto z_k^u$ n'est pas surjective et donc n'est pas injective,
Il existe $u_1 < u_2 \in [\![1, n-1]\!]$ tel que $z_k^{u_1} = z_k^{u_2}$ et donc $z_k^{u_2-u_1} = \dfrac{z_k^{u_2}}{z_k^{u_1}} = 1$,
et donc $z_k \in \mathbb{V}_{u_2-u_1}$, ce qui est faux.
Finalement : il existe $u \in [\![1, n-1]\!] \subset \mathbb{Z}$ tel que $z_k^u = z_1$.
• S'il existe $u \in \mathbb{Z}$ tel que $z_k^u = z_1$ On a donc $\exp\dfrac{2iku\pi}{n} = \exp\dfrac{2i\pi}{n}$ donc $\dfrac{2uk\pi}{n} \equiv \dfrac{2\pi}{n}[2\pi]$
donc $\dfrac{uk}{n} \equiv \dfrac{1}{n}[1]$ puis $ku \equiv 1[n]$.
Donc, il existe $v) \in \mathbb{Z}$ tel que $uk + vn = 1$. Ainsi $k \wedge n = 1$ d'après Bézout.
• Enfin, supposons que $k \wedge n = 1$.
Soit $r \in \mathbb{N}^*$ tel que $z_k \in \mathbb{V}_r$, comme $z_k^n = 1$, nécessairement, $r \leqslant n$.

Puis on a $1 = z_k^r = \exp\dfrac{2ikr\pi}{n}$, donc $rk \equiv 0[n]$, donc $n|kr$.
Or $n \wedge k = 1$, donc $n|r$. Ainsi $r \in n\mathbb{Z} \cap [1, n]$, bilan $r = n$.

$$\boxed{z_k \in \mathbb{V}_n \iff \exists\ u \in \mathbb{Z} \text{ tel que } (z_k)^u = z_1 \iff k \wedge n = 1.}$$

2. On rappelle que $n$ et $d$ (par la suite) sont des entiers naturels, donc positifs.
Soit $d$, un diviseur de $n$. Donc il existe $n_1 \in \mathbb{N}$ tel que $n = n_1 d$.
Soit $z \in \mathbb{V}_d$, alors $z^d = 1$ et donc $z^n = z^{n_1 d} = (z^d)^{n_1} = 1^{n_1} = 1$. Donc $z \in \mathbb{U}_n$.
Par conséquent $\mathbb{V}_d \subset \mathbb{U}_n$, on a donc $\bigcup_{d|n} \mathbb{V}_d = \mathbb{U}_n$
Réciproquement, soit $z \in \mathbb{U}_n$ (fixé !), i.e. $z^n = 1$.
L'ensemble $\{k \in [\![1, n]\!] \text{ tel que } z^k = 1\}$ est donc non vide (il contient $n$) , inclus dans $\mathbb{N}$,
il admet un plus petit élément $k_0$( qui dépend de $z$).
Alors $z \in \mathbb{V}_{k_0}$, par définition de $k_0$ et $\mathbb{V}_{k_0}$.
Puis, si on note $\delta = k_0 \wedge n$, il existe $u, v \in \mathbb{Z}$ tel que $\delta = uk_0 + vn$ et donc

$$z^\delta = (z^{k_0})^u \times (z^n)^v = 1^u \times 1^v = 1$$

Nécessairement, $\delta = k_0$ et donc $k_0 = \delta$ divise $n$.
On a la double inclusion, reste à montrer que la réunion est disjointe.
Si $z \in \mathbb{V}_d \cap \mathbb{V}_{d'}$, alors, SPDG, on peut supposer $d \leqslant d'$.
Donc $z^d = 1$ et pour tout $k < d'$, $z^k \neq 1$. Donc $d = d'$. La réunion est disjointe.

$$\boxed{\mathbb{U}_n = \uplus_{d|n} \mathbb{V}_d}$$

On a alors pour $\mathbb{U}_{12}$ :

$$\boxed{\mathbb{U}_{12} = \{\underbrace{1}_{\in\mathbb{V}_1}, \underbrace{-1}_{\in\mathbb{V}_2}, \underbrace{\overbrace{e^{\frac{i\pi}{3}}}^{=j}, \overbrace{e^{-\frac{i\pi}{3}}}^{=j^2}}_{\in\mathbb{V}_3}, \underbrace{\overbrace{e^{\frac{i\pi}{4}}}^{=i}, \overbrace{e^{-\frac{i\pi}{4}}}^{=-i}}_{\in\mathbb{V}_4}, \underbrace{e^{\frac{i\pi}{3}}, e^{-\frac{i\pi}{3}}}_{\in\mathbb{V}_6}, \underbrace{e^{\frac{i\pi}{6}}, e^{-\frac{i\pi}{6}}, e^{\frac{5i\pi}{6}}, e^{-\frac{5i\pi}{6}}}_{\in\mathbb{V}_{12}}\}}$$

3. Il s'agit simplement d'une décomposition d'un produit (car la réunion est disjointe) :

$$\boxed{G_n = \prod_{z\in\mathbb{U}_n} (X - z) = \prod_{z\in\uplus_{d|n}\mathbb{V}_d} (X - z) = \prod_{d|n} \left( \prod_{z\in\mathbb{V}_d} (X - z) \right) = \prod_{d|n} \Phi_d}$$

On a alors, d'après la question précédente : $G_{12} = \Phi_1 \times \Phi_2 \times \Phi_3 \times \Phi_4 \times \Phi_6 \times \Phi_{12}$.
Et d'après la décomposition précédente,

$$\Phi_{12} = (X - e^{\frac{i\pi}{6}})(X - e^{-\frac{i\pi}{6}})(X - e^{\frac{5i\pi}{6}})(X - e^{-\frac{5i\pi}{6}}) = (X^2 - 2\cos\frac{\pi}{6} + 1)(X^2 - 2\cos\frac{5\pi}{6} + 1)$$

Or en notant $C = \cos\dfrac{\pi}{6} = \dfrac{\sqrt{3}}{2}$, on a $\cos\dfrac{5\pi}{6} = -\cos(\pi - \dfrac{5\pi}{6}) = -\cos\dfrac{\pi}{6} = -C$, donc

$$\boxed{\Phi_{12} = (X^2 - 2CX + 1)(X^2 + 2CX + 1) = X^4 + (2 - 4C^2)X^2 + 1 = X^4 + (2 - 3)X + 1 = X^4 - X^2 + 1}$$

(On peut aussi calculer par division euclidienne de polynômes entiers successivement $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$ et $\Phi_6 = X^2 - X + 1\ldots$)

4. $G_m = \Phi_m \times \prod_{d|m, d\neq m} \Phi_d$, donc $\Phi_m$ est le quotient de la division euclidienne de $G_m$ par $\prod_{d|m, d<m} \Phi_d$.
Montrons d'abord que :
pour $A, B \in \mathbb{Z}[X]$ tels que $B|A$ dans $\mathbb{Q}[X]$, alors si $B$ est unitaire, les coefficients de $\mathbb{Q}$ sont entiers.

Supposons donc $A = BQ$, avec $Q \in \mathbb{Q}[X]$. On trouve alors pour tout entier $n$, $[A]_n = \sum_{k=0}^{n} [B]_k [Q]_{n-k}$.

Supposons que $d_A = \deg A$ et $d_B = \deg B$, on a donc $d_Q := \deg Q = d_A - d_B$, puis

$$[A]_{d_A} = [B]_{d_B} \times [Q]_{d_Q} \Rightarrow [Q]_{d_Q} = \frac{[A]_{d_A}}{[B]_{d_B}} = [A]_{d_A} \in \mathbb{Z} \text{ ( car } B \text{ unitaire, donc } [B]_{d_B} = 1).$$

Montrons alors par récurrence (forte), pour $k \in [\![0, d_Q]\!]$, $\mathcal{H}_k$ : « $[Q]_{d_Q - k} \in \mathbb{Z}$ ».
— On vient de voir que $[Q]_{d_Q} \in \mathbb{Z}$, donc $\mathcal{H}_0$ est vraie.
— Soit $k \in [\![0, d_Q - 1]\!]$ tel que $\mathcal{H}_0$, $\mathcal{H}_1, \cdots, \mathcal{H}_k$ sont vraies.

$$[Q]_{d_Q-(k+1)}[B]_{d_B} = [Q]_{d_Q-k-1}[B]_{d_B} = \underbrace{[A]_{d_Q+d_B-k-1}}_{\in\mathbb{Z}} - \sum_{i=0}^{d_B-1} \underbrace{[B]_i}_{\in\mathbb{Z}} \underbrace{[Q]_{d_Q+d_B-k-1-i}}_{=[Q]_r \in \mathbb{Z}}$$

car $r = d_Q - k + \underbrace{d_B - 1 - i}_{\geqslant 0} \geqslant d_Q - k$ et en appliquant $\mathcal{H}_r$.

On termine en notant que $[B]_{d_B} = 1$. Donc $\mathcal{H}_{k+1}$ est vraie.

Ainsi, si $B|A$, avec $A, B \in \mathbb{Z}[X]$ et $B$ unitaire, alors $Q = \dfrac{A}{B}$ est un polynôme à coefficients entiers.

Posons maintenant, pour $m \in \mathbb{N}^*$, $\mathcal{Q}_m$ : « $\Phi_m$ est unitaire et à coefficients entiers. »
— $\Phi_1 = X - 1$, donc $\mathcal{Q}_1$ est vraie.
— Soit $m \in \mathbb{N}$, $m \geqslant 2$, supposons que $\mathcal{Q}_1$, $\ldots \mathcal{Q}_{m-1}$ sont vraies.
$G_m = \Phi_m \prod_{d|m, d<m} \Phi_d$, on a donc pour $d|m$ et $d < m$, $\Phi_d$ est unitaire à coefficients entiers.
Le produit de tels polynômes est unitaire, à coefficients entiers : $B = \prod_{d|m, d<m} \Phi_d \in \mathbb{Z}[X]$ et est unitaire.
$G_m$ est également à coefficients entiers, donc $\Phi_m = \dfrac{G_m}{B}$ est à coefficients entiers.
Puis le coefficient dominant de $\Phi_m$ est égale à celui de $G_m$ divisé par celui de $B$, i.e. $\dfrac{1}{1} = 1$.
Donc $\mathcal{Q}_m$ est vérifiée.

$\Phi_m \in \mathbb{Z}[X]$ et est unitaire.

Enfin, $\Phi_m = \prod_{z \in \mathbb{V}_m} (X - z)$, produit de $\text{card}(\mathbb{V}_m)$ polynôme de degré 1, donc son degré est $\text{card}(\mathbb{V}_m)\times = \varphi(m)$

$$\deg \Phi_m = \varphi(m)$$

5.

On a donc, d'après la question précédente : $\deg G_n = \deg \left( \prod_{d|n} \Phi_d \right) = \sum_{d|n} \deg \Phi_d = \sum_{d|n} \varphi(d)$.

6. Soit $p$ un nombre premier

$\Phi_{p^k} = \{\omega_{p^k}^r ; r \in \mathbb{N}_{p^k} \text{ et } r \wedge p^k = 1\} = \{\omega_{p^k}^r ; r \in \mathbb{N}_{p^k} \text{ et } r \wedge p = 1\} = \left\{\omega_{p^k}^r ; r \in \mathbb{N}_{p^k} \setminus \{p, 2p, 3p, \ldots p^{k-1}p\}\right\}$

On a alors

$$X^{p^k} - 1 = \prod_{z \in \mathbb{U}_{p^k}} (X - z) = \left( \prod_{r \in \{p, 2p, \ldots (p^{k-1})p\}} (X - \omega_{p^k}^r) \right) \times \Phi_{p^k} = \left( \prod_{j=1}^{p^{k-1}} (X - \omega_{p^k}^{jp}) \right) \times \Phi_{p^k}$$

Or $\omega_{p^k}^p = \exp\left(i\dfrac{2p\pi}{p^k}\right) = \exp\left(i\dfrac{2\pi}{p^{k-1}}\right) = \omega_{p^{k-1}}$.

$$\prod_{j=1}^{p^{k-1}} (X - \omega_{p^k}^{jp}) = \prod_{j=1}^{p^{k-1}} \left( X - \left(\omega_{p^k}^p\right)^j \right) = \prod_{j=1}^{p^{k-1}} \left( X - \left(\omega_{p^{k-1}}\right)^j \right) = \prod_{z \in \mathbb{U}_{p^{k-1}}} (X - z) = X^{p^{k-1}} - 1$$

Par ailleurs, on a le telescopage :

$$(X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + \cdots + X^{p^{k-1}} + 1)(X^{p^{k-1}} - 1) = X^{(p-1)p^{k-1}+p^{k-1}} - 1 = X^{p^k} - 1$$

On fait la division par $X^{p^{k-1}} - 1 = \prod_{j=1}^{p^{k-1}} (X - \omega_{p^k}^{jp})$.

$$\boxed{\Phi_{p^k} = X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + \cdots + X^{p^{k-1}} + 1}$$

7. Comme 5 est un nombre premier, tous les nombres $k \in [\![1;4]\!]$ sont premiers avec 5.
Donc $\Phi_5 \times (X-1) = X^5 - 1$, donc

$$\boxed{\Phi_5 = \frac{X^5-1}{X-1} = 1 + X + X^2 + X^3 + X^4}$$

$\mathbb{P}_6 = \{\omega^6, \omega_6^5\}$.
Donc, comme $\omega_6^5 = \overline{\omega_6} = \cos\dfrac{2\pi}{6} - i\sin\dfrac{2\pi}{6} = \dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$,

$$\boxed{\Phi_6 = (X-\omega_6)(X-\omega_6^5) = X^2 - 2\mathrm{Re}(\omega_6) + |\omega_6|^2 = X^2 - X + 1}$$

## ▷ Corrigé de l'exercice 2.3

1. Soit $n \in \mathbb{N}$, $n \geqslant 2$.
D'après le lemme d'Euclide : $k \wedge n = (n-k) \wedge k$, donc $k \wedge n = 1 \iff (n-k) \wedge n = 1$.

$$\omega_n^k \in \mathbb{P}_n \iff \overline{\omega_n^k} = \omega_n^{n-k} \in \mathbb{P}_n$$

On peut donc séparer en deux les racines $n$-ieme primitive selon le signe de leur partie imaginaire : *Pour $n \geqslant 1$, ni 1, ni $-1$ ne sont racines $n$-ième primitive !!*

$$\Phi_n = \prod_{z\in\mathbb{P}_n, \mathrm{Im}(z)>0} (X-z)(X-\overline{z}) = \prod_{z\in\mathbb{P}_n, \mathrm{Im}(z)>0} (X^2 - \mathrm{Re}(z)X + |z|^2)$$

Or si $z$ est une racine $n$-ième, $|z|^2 = 1$.
En prenant la valeur en 0

$$\boxed{\Phi_n(0) = \prod_{z\in\mathbb{P}_n; \mathrm{Im}(z)>0} 1 = 1}$$

2. Notons, pour tout $n \in \mathbb{N}$, $n \geqslant 2$,

$$\mathcal{H}_n : \text{« } \Phi_n(1) = \begin{cases} p & \text{si } n = p^r, \text{ avec } p \text{ nombre premier} \\ 1 & \text{sinon} \end{cases} \text{ »}$$

— $\Phi_2(1) = 1 + 1 = 2$. Donc $\mathcal{H}_2$ est vraie.
— Soit $n \in \mathbb{N}$, $n \geqslant 2$, on suppose que $\mathcal{H}_k$ est vraie pour tout $k \in [\![2, n]\!]$.
Si $n+1 = p^k$,
avec la question 3.(a), on voit que $\Phi_{p^k}(1) = (p-1)1 + 1 = p$.
Supposons que $n+1 = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $r \geqslant 2$.

$$X^{n+1} - 1 = (X-1) \times \left( \prod_{k|n+1, k\notin\{1,n+1\}} \Phi_k \right) \times \Phi_{n+1}$$

Donc

$$\left( \prod_{k|n+1, k\notin\{1,n+1\}} \Phi_k \right) \times \Phi_{n+1} = \frac{X^{n+1}-1}{X-1} = \sum_{k=0}^{n} X^k$$

En regardant en 1 comme $\mathcal{H}_r$ est vraie,
et que pour beaucoup de diviseurs $d$ de $n+1$, $\Phi_d(1)=1$ :

$$\Phi_{n+1}(1)\times\left(\Phi_{p_1}(1)\Phi_{p_1^2}(1)\dots\Phi_{p_1^{\alpha_1}}(1)\right)\times\dots\times\left(\Phi_{p_r}(1)\dots\Phi_{p_r^{\alpha_r}}(1)\right)\times 1=n+1$$

$$\Phi_{n+1}(1)\times p_1^{\alpha_1}\times\dots p_r^{\alpha_r}=\Phi_{n+1}(1)\times(n+1)=(n+1)$$

Donc $\Phi_{n+1}(1)=1$.

Ainsi, tous les cas sont vérifiées : $\mathcal{H}_{n+1}$ est vraie.

La récurrence est démontrée :

$$\boxed{\text{Pour tout } n\geqslant 2,\ \Phi_n(1)=\begin{cases}p & \text{si } n=p^r,\ \text{avec } p \text{ nombre premier}\\ 1 & \text{sinon}\end{cases}.}$$

## ▷ Corrigé de l'exercice 2.4

1. $z$ est une racine de $P_1$, donc de $\Phi_n$. Ainsi pour tout $k<n$, $z^k\neq 1$ et $z^n=1$.
Comme $p$ est un nombre premier et que $p\not| n$, alors $p\wedge n=1$. Puis $(z^p)^r=z^{pr}$.
D'après la question précédente, on a : $(z^p)^s=1\iff n|ps\iff n|s\iff s\in n\mathbb{Z}$.
Ainsi, pour tout $s\in[\![1,n-1]\!]$, $(z^p)^s\neq 1$ et donc $z^p\in\mathbb{V}_n$.
Donc $z^p$ est une racine de $\Phi_n$, ainsi $\Phi_n(z^p)=0=\prod_{i=1}^{r}P_i(z^p)$ Or $\mathbb{C}$ est intègre, donc

$$\boxed{\text{il existe } i\in\mathbb{N}_r \text{ tel que } P_i(z^p)=0.}$$

2. Supposons que $\overline{\Phi_n}$ est divisible par le carré d'un polynôme $Q$ (non constant),
Ainsi, supposons qu'il existe $Q,T\in\mathbb{Z}[X]$ tel que $\overline{\Phi_n}=\overline{Q}^2\overline{T}$ et $\deg\overline{Q}>0$.
Alors comme $\Phi_n$ divise $G_n$, il existe $S\in\mathbb{Z}[X]$ tel que $\overline{G_n}=X^n-\overline{1}=\overline{Q}^2\underbrace{\overline{TS}}_{\overline{R}}$.
On peut dériver cette égalité polynômiale : $\overline{n}X^{n-1}=\overline{Q}\left(2\overline{Q'R}+\overline{QR'}\right)$.
Donc $\overline{Q}$ divise $\overline{n}X^{n-1}$, et divise $X^n-\overline{1}$,
et $\overline{Q}$ divise aussi $X(\overline{n}X^{n-1})-\overline{n}(X^n-\overline{1})=\overline{n}$
Donc $\overline{Q}$ est une constante, non nulle, puisque $\overline{n}\neq 0$, puisque $p\wedge n=1$. On a donc une contradiction :

$$\boxed{\overline{\Phi_n}\text{ n'est divisible par le carré d'aucun polynôme non constant.}}$$

3. Reprenons les notations données plus haut, $P_1(z)=0$ et $P_i(z^p)=0$ avec $i\neq 1$.
La polynôme $R_1(X)=P_i(X^p)$ admet donc $z$ comme racine, comme le polynôme $P_1$.
Ils ne sont pas premiers entre eux dans $\mathbb{Q}[X]$.
Mais si $\Delta=P_1\wedge R_1$, alors $\Delta|P_1$, irréductible par hypothèse. Donc $\Delta=P_1$.
Et finalement, $P_1=\lambda\Delta|R_1$ (dans $\mathbb{Q}[X]$).
La division euclidienne de $R_1$ par $P_1$ (dans $\mathbb{Q}[X]$) a un reste nul, mais elle s'effectue uniquement avec des nombres entiers car $P_1$ est unitaire (remarque vue en cours).
Donc il existe $S_1\in\mathbb{Z}[X]$ tel que $R_1=S_1\times P_1$.
Prenons maintenant les classes modulo $p$ (puisqu'on est dans $\mathbb{Z}[X]$) :

$$\overline{P_1}|\overline{R_1}=\overline{P_i(X^p)}=[\overline{P_i}(X)]^p$$

Soit $\overline{Q}$, un facteur irréductible de $\overline{P_1}$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$, on a donc $\overline{Q}|\overline{P_1}|\overline{P_i}^p$.
Comme $\overline{Q}$ est irréductible, $\overline{Q}|\overline{P_i}$ et donc $\overline{Q}^2|\overline{\Phi_n}=\overline{P_1P_i}\times\prod_{j\neq 1,i}\overline{P_j}$.
D'après la question précédente, cela n'est possible que si $\overline{Q}$ est constant. Donc $\overline{P_1}$ est constant.
Impossible, donc $i=1$

$$\boxed{P_1(z^p)=0.}$$

Le résultat a été montré pour tout nombre premier $p$, premier avec $n$. Montrons par récurrence sur $s\in\mathbb{N}^*$,

$\mathcal{H}_s$ : « Si $k=p_1\cdots p_s$, produit de $s$ nombres premiers (qui peuvent se répéter) tel que $k\wedge n=1$, alors $P_1(z^k)=0$ ».

— Si $k = p_1$, c'est toute la partie précédente.
— Soit $s \in \mathbb{N}^*$. Supposons que $\mathcal{H}_s$ est vraie.
Soit $k = p_1 \cdots p_s p_{s+1}$, produit de $s+1$ nombres premiers (qui peuvent se répéter) tel que $k \wedge n = 1$,
On note $k' = p_1 \cdots p_s$, on a alors $k' \wedge n = 1$, on peut appliquer $\mathcal{H}_s$.
Donc $P_1(z^{k'}) = 0$. Notons $z' = z^{k'}$, c'est une racine de $P_1$,
on a donc, puisque $p_{s+1} \wedge n = 1$, $P_1((z')^{p_{s+1}}) = 0$ (question précédente pour $(z,p) \leftarrow (z', p_{s+1})$).
Et donc finalement, $P_1(z^k) = 0$. Donc $\mathcal{H}_{s+1}$ est vraie.

Pour tout $k$ entier, premier avec $n$, $P_1(z^k) = 0$.

4. Soit $z \in \mathbb{V}_n$, alors on montre que $\mathbb{V}_n = \{z^k \ ; \ k \wedge n = 1\}$.*C'est vrai pour tous, mais on se contente de* $z = e^{\frac{2i\pi}{n}}$.
Et donc tous les éléments de $\mathbb{V}_n$ sont des racines de $P_1$, donc $\Phi_n = P_1$.

Ainsi $\Phi_n$ est irréductible dans $\mathbb{Z}[X]$.

## ▷ Corrigé de l'exercice 3.1

1. C'est un résultat de cours, qui s'obtient par télescopage.
Soit $m \geqslant 1$, (en posant $h = k+1$) :

$$\begin{aligned}(X-a)\left(\sum_{k=0}^{m-1} a^k X^{m-1-k}\right) &= \sum_{k=0}^{m-1} a^k X^{m-k} - \sum_{k=0}^{m-1} a^{k+1} X^{m-1-k} \\ &= X^m + \sum_{k=1}^{m-1} a_k X^{m-k} - \sum_{h=1}^{m-1} a_h X^{m-h} - a^m\end{aligned}$$

Pour tout $a \in \mathbb{C}$, et tout entier naturel $m \geqslant 1$, $X^m - a^m = (X-a)\left(\sum_{k=0}^{m-1} a^k X^{m-1-k}\right)$.

2. Soit $i \in [\![1, n]\!]$. On note $Q_i$ le polynôme défini par :

$$Q_i(X) = \frac{Q(X)}{X-\alpha_i} = \frac{b_n \prod_{j=1}^{n}(X-\alpha_j)}{X-\alpha_i} = b_n \prod_{j\neq i}(X-\alpha_j)$$

La formule de dérivation d'un produit donne :

$$Q' = b_n \sum_{i=1}^{n}\left(\prod_{j\neq i}(X-\alpha_j)\right) = \sum_{i=1}^{n} Q_i$$

3. Comme $Q(\alpha_i) = 0$, on a bien $Q_i(X) = \dfrac{Q(X) - Q(\alpha_i)}{X-\alpha_i}$.
Or, par linéarité (les termes en $k=0$ s'annulent) :

$$Q(X) - Q(\alpha_i) = \sum_{s=1}^{n} b_s (X^s - \alpha_i^s) = \sum_{s=1}^{n} b_s (X-\alpha_i)\left(\sum_{k=0}^{s-1} \alpha_i^k X^{s-1-k}\right)$$

d'après la première réponse.
On trouve donc

$$Q_i = \frac{Q - Q(\alpha_i)}{X-\alpha_i} = \sum_{0\leqslant k<s\leqslant n} b_s \alpha_i^k X^{s-1-k}$$

Puis en faisant le changement de variable $r = s-k$ ($k$ remplacé par $r$), on a

$$0 \leqslant s-r < s \leqslant n \iff s \in [\![1,n]\!], r \in [\![1,s]\!] \iff 1 \leqslant r \leqslant s \leqslant n$$

Donc

$$\boxed{Q_i = \sum_{1\leqslant r\leqslant s\leqslant n} b_s \alpha_i^{s-r} X^{r-1} = \sum_{r=1}^{n} \left( \sum_{s=r}^{n} b_s \alpha_i^{s-r} \right) X^{r-1}}$$

4. Donc on trouve :

$$Q' = \sum_{r=1}^{n} r b_r X^{r-1} = \sum_{i=1}^{n} Q_i = \sum_{r=1}^{n} \left( \sum_{i=1}^{n} \sum_{s=r}^{n} b_s \alpha_i^{s-r} \right) X^{r-1}$$

L'écriture sur la base $(1, X, \dots X^{n-1})$ est unique, donc

$$\forall\ r \in \mathbb{N}_n, \qquad r b_r = \sum_{s=r}^{n} b_s \left( \sum_{i=1}^{n} \alpha_i^{s-r} \right) = \sum_{s=r}^{n} b_s T_{s-r}$$

Reste à faire le changement de variable $j = s - r$ :

$$\boxed{\forall r \in [\![1, n]\!], \qquad r b_r = \sum_{j=0}^{n-r} b_{r+j} T_j}$$

## ▷ Corrigé de l'exercice 3.2

1. On a donc trouvé donc une relation de récurrence triangulaire entre les $T_k$ :

$$r b_r = (b_r T_0 + b_{r+1} T_1 + \cdots + b_n T_{n-r})$$

Donc $T_{n-r} = \dfrac{1}{b_n} (r b_r - b_r T_0 - b_{r+1} T_1 - \cdots - b_{n-1} T_{n-r-1})$.
En notant $k$, le nombre $n - r$ :

$$\boxed{\text{Pour } k \in [\![1, n-1]\!], \qquad T_k = \frac{1}{b_n} (r b_r - b_r T_0 - b_{r+1} T_1 - \cdots - b_{r+k-1} T_{k-1}).}$$

2. Soit $k \geqslant n$.

On sait que pour tout $i \in \mathbb{N}_n$, $Q(\alpha_i) = 0$, donc $\displaystyle\sum_{h=0}^{n} b_h \alpha_i^h = 0$.
On multiplie par $\alpha_i^{k-n}$, puis on additionne pour $i$ de 1 à $n$ :

$$\boxed{0 = \sum_{i=1}^{n} \left( \alpha_i^{k-n} \sum_{h=0}^{n} b_h \alpha_i^h \right) = \sum_{h=0}^{n} \sum_{i=1}^{n} b_h \alpha_i^{k+h-n} = \sum_{h=0}^{n} b_h T_{k-n+h}}$$

3. Comme pour plus haut, on trouve

$$b_0 T_{k-n} + b_1 T_{k-n+1} + \cdots + b_n T_k$$

$$\boxed{T_k = \frac{-1}{b_n} (b_0 T_{k-n} + b_1 T_{k-n+1} + \cdots + b_{n-1} T_{k-1}) = \frac{-1}{b_n} \sum_{j=k-n}^{k-1} b_{j-k+n} T_j}$$

## ▷ Corrigé de l'exercice 3.3

1. On démontre le résultat par récurrence forte sur $k$.
Notons, pour tout $k \in \mathbb{N}$, $\mathcal{P}_k$ : « $S_k \in \mathbb{Z}$ ».
— $S_0 = n \in \mathbb{N}$. Donc $\mathcal{P}_0$ est vraie.
— Non nécessaire : $S_1 = z_1 + z_2 + \cdots + z_n = -[P]_{n-1} \in \mathbb{Z}$.
Donc $\mathcal{P}_0$ est vraie.

— Soit $n \in \mathbb{N}$. Supposons que pour tout $k \geqslant n$, $S_k \in \mathbb{Z}$.
En première partie on a vu que $[P]_n S_{n+1}$ est une combinaison linéaire de la forme produit de $[P]_k$ par $S_h$ $(h < n+1)$.
Or $[P]_k \in \mathbb{Z}$, car $P \in \mathbb{Z}[X]$, $S_h \in \mathbb{Z}$, par hypothèse de récurrence.
Donc $[P]_n S_{n+1} \in \mathbb{Z}$. Et comme $P$ est unitaire, $[P]_n = 1$ et donc $\mathcal{P}_{n+1}$ est vérifiée.

Donc pour tout entier $k \in \mathbb{N}$, $S_k \in \mathbb{Z}$.

2. Comme pour tout $i \in \mathbb{N}$, $|z_i| \in 1$, alors

$$|S_k| \leqslant \sum_{i=1}^{n} |z_i|^k \leqslant \sum_{i=1}^{n} 1 = n$$

Donc $S_k \in [\![-n, n]\!]$.
Ainsi, pour tout $k \in \mathbb{N}$,

$$(S_k, S_{k+1}, \dots S_{k+n}) \in [\![-n, n]\!]^{n+1}$$

Or l'ensemble $[\![-n, n]\!]^{n+1}$ est fini (il possède au plus $(2n+1)^{n+1}$ nombres - $n$ est fixé !).
Donc nécessairement, il existe $k \neq \ell \in \mathbb{N}$ tel que $(S_k, S_{k+1}, \dots S_{k+n}) = (S_\ell, S_{\ell+1}, \dots S_{\ell+n})$

Il existe deux entiers $k$ et $\ell$ $(0 \leqslant k < \ell)$ tels que $S_{k+i} = S_{\ell+i}$ pour tout $i \in \{0, 1, \dots n\}$.

On fixe $k$ et $\ell$.

3. Soit $F \in \mathbb{C}_n[X]$, on peut supposer que $F = \sum_{j=0}^{d} a_j X^j$ (avec $d \leqslant n$).

$$\sum_{i=1}^{n} F(z_i)(z_i^\ell - z_i^k) = \sum_{j=0}^{d} a_j \left( \sum_{i=1}^{n} z_i^{\ell+j} - \sum_{i=1}^{n} z_i^{k+j} \right) = \sum_{j=0}^{d} a_j (S_{\ell+j} - S_{k+j}) = 0$$

4. On a déjà fait cette première question d'un DS1 mais elle n'est pas facile.
On note pour $\alpha$, l'une des racines $z_i$ de $P$,

$$\mathcal{I}_\alpha = \{T \in \mathbb{Q}[X] \mid T(\alpha) = 0\}$$

$\mathcal{I}_\alpha$ est non vide, puis $P \in \mathcal{I}_\alpha$. L'ensemble $\{\deg P, P \in \mathcal{I}_\alpha, P \neq 0\}$ est non vide.
On note $r = \min\{\deg P, P \in \mathcal{I}_\alpha\}$ et $T_r \in \mathcal{I}_\alpha$ tel que $\deg T_r = r$.
On peut faire la division euclidienne de $P$ par $T_r$, dans le corps de base :

$$P = T_r Q + R$$

Ainsi $Q, R \in \mathbb{Q}[X]$ et $R(\alpha) = P(\alpha) - Q(\alpha)T_r(\alpha) = 0$.
Donc $R \in \mathcal{I}_\alpha$, et $\deg R < \deg Q$. La seule possibilité est $R = 0$, sinon on a une contradiction.
Donc $T_r$ divise $P$. Mais par hypothèse, $P$ est irréductible donc $P = T_r$.
Puis
Si $\alpha$ est une racine double de $P$, alors $\alpha$ est aussi une racine de $P'$.
$P'$, comme $P$ est un polynôme à coefficients entiers.
Donc $P' \in \mathcal{I}_\alpha$, avec $\deg P' < r$. Impossible.

Ainsi toutes les racines de $P$ sont distinctes (aucune n'est double)

On a donc en prenant $F = L_i = \prod_{j \neq i} \dfrac{X - z_j}{z_i - z_j}$ (polynôme de degré $n-1$, au plus) :

$$0 = \sum_{j=1}^{n} F(z_j)(z_j^\ell - z_j^k) = (z_i^\ell - z_i^k) = z_i^k (z_i^{\ell-k} - 1)$$

Or $|z_i| = 1$, donc $z_i^k \neq 0$, ainsi

$$z_i^{\ell-k} = 1, \text{ pour tout } i \in \{1, 2, \dots n\}.$$

Donc les racines de $P$ sont toutes des racines $\ell - k$-ième de l'unité.

### ▷ Corrigé de l'exercice 4.1

1. Soit $R \geqslant (p-1)(q-1)$.
$p$ et $q$ sont premiers entre eux, puisque ce sont deux nombres premiers.
Donc il existe $u, v \in \mathbb{Z}$ tel que $up + vq = 1$. En multipliant par $R$, on a $Ru \times p + Rv \times q = R$.
Le problème est que ces nombres sont des entiers relatifs, et non naturels, a priori. *Considérons un autre couple* $(a, b) \in \mathbb{Z}^2$ *tel que* $ap + bq = R = Rup + Rvq$.
*On a donc* $(a - Ru)p = (Rv - b)q$. *Donc* $p|(Rv - b)q$ *et comme* $p \wedge q = 1$, $p|Rv - b$.
*Par conséquent : il existe* $s \in \mathbb{Z}$ *tel que* $b = Rv - ps$
*et ensuite* $ap = Rup + Rvq - bq = Rup + pqs = p(Ru + qs)$ *donc* $a = Ru + q$.
*On cherche donc deux nombres* $a$ *et* $b$ *tels que* $a \equiv Ru[q]$ *et* $b \equiv Rv[p]$ *et* $a, b > 0$. Faisons la division euclidienne de $Ru$ par $q$. Il existe donc $a \in [\![0, q-1]\!]$ (reste de la D.E.) tel que $Ru \equiv a[q]$.
Et il existe $s \in \mathbb{Z}$ tel que $Ru = sq + a$, on a alors $R = Rup + Rvq = sqp + ap + Rvq = ap + (sp + Rv)q$.
Notons $b = sp + Rv \in \mathbb{Z}$. On a donc $R = ap + bq$.
Or $0 \leqslant a \leqslant q - 1$, donc $p > 0 : 0 \leqslant ap \leqslant p(q-1) = pq - p$
Et $R \geqslant (p-1)(q-1) = pq - p - q + 1$, donc $ap \leqslant R + q - 1$ et $bq = R - ap \geqslant 1 - q$.
Or si $b < 0$, $b \leqslant -1$ et donc $bq < -q$ $(q > 0)$. Ceci n'est donc pas possible donc $b \geqslant 0$.

> Ainsi, pour tout $R \geqslant (p-1)(q-1)$, il existe $a, b \in \mathbb{N}$ tel que $R = ap + bq \in < p, q >$

2. Supposons par l'absurde qu'il existe $a, b \in \mathbb{N}$, tel que $ap + bq = (p-1)(q-1) - 1 = pq - p - q$.
Donc $(a + 1 - q)p + (b + 1)q = 0$. Ainsi $q|(a + 1 - q)p$ et comme $p \wedge q = 1$, $q|a + 1 - q$ et donc $q|a + 1$.
Mais $a \in \mathbb{N}$, donc $a + 1 > 0$ et donc il existe $s \in \mathbb{N}^*$ tel que $a + 1 = sq$ et donc $a + 1 - q = (s-1)q$.
On a alors $0 = (s-1)qp + (b+1)q$, donc $(s-1)p + (b+1) = 0$, alors que $s - 1, p, b + 1 \in \mathbb{N}$.
Nécessairement : $s - 1 = 0$ et $b + 1 = 0$, donc $b = -1$. Contradiction.

> $(p-1)(q-1) - 1$ n'appartient pas à $< p, q >$.

### ▷ Corrigé de l'exercice 4.2

1. D'après les questions précédentes, pour tout $k \geqslant R(= (p-1)(q-1))$, $k \in < p, q >$, donc $[H]_k = 0$.
Ainsi $\deg H < R$.
Et $R - 1 \notin < p, q >$, donc $[H]_{R-1} \neq 0$ et donc donc $\deg H \geqslant R - 1$.

> Par double inégalité : $\deg H = R - 1 = (p-1)(q-1) - 1 = pq - p - q$.

Puis $\deg((X-1)H) = \deg(X-1) + \deg H = 1 + \deg H \geqslant 1$, donc $\deg K = \max(0, \deg((X-1)H) = 1 + \deg H$.

> $\deg K = R = (p-1)(q-1)$.

2. Pour ce couple, $R = (p-1)(q-1) = 2 \times 4 = 8$.
Les termes suivants $(\geqslant 8)$ ne sont pas intéressants à étudier.
On a, de plus, $0 = 0 \times 3 + 0 \times 5$, $3 = 1 \times 3 + 0 \times 5$, $5 = 0 \times 3 + 1 \times 5$, $6 = 2 \times 3 + 0 \times 5$ dans $< 3, 5 >$.
Donc $H = X^1 + X^2 + X^4 + X^7$. Puis

> $K = 1 + (X-1)H = 1 - X + X^3 - X^4 + X^5 - X^7 + X^8$

### ▷ Corrigé de l'exercice 4.3

1. Pour tout $k \in \mathbb{N}$, $[T]_k = \sum_{i=0}^{k} [(X-1)]_i [S]_{k-i} = [X-1]_0 [S]_k + [X-1]_1 [S]_{k-1} + 0 + \cdots = -[S]_k + [S]_{k-1}$.
Or $[S]_k, [S]_{k-1} \in \{0, 1\}$, donc

> $[T]_k = [S]_{k-1} - [S]_k \in \{-1, 0, 1\}$

2. Pour tout $k \in [\![k_1 + 1, k_2 - 1]\!]$, $[T]_k = 0 = [S]_{k-1} - [S]_k$, donc $[S]_k = [S]_{k-1}$.
La suite $([S]_k)_{k_1 \leqslant k \leqslant k_2 - 1}$ est donc une suite constante.
Alors que $[T]_{k_2} = [S]_{k_2 - 1} - [S]_{k_2} \neq 0$, donc $[S]_{k_2} \neq [S]_{k_2 - 1} = [S]_{k_1}$.

et de même $[T]_{k_1} = [S]_{k_1-1} - [S]_{k_1} \neq 0$, donc $[S]_{k_1-1} \neq [S]_{k_1}$.
Ainsi, ou bien $\forall\, k \in [\![k_1, k_2-1]\!]$, $[S]_{k-1} = 0$, $[S]_{k_1-1} = 1$ et $[S]_{k_2} = 1$,
ou bien $\forall\, k \in [\![k_1, k_2-1]\!]$, $[S]_{k-1} = 1$, $[S]_{k_1-1} = 0$ et $[S]_{k_2} = 0$,
Et donc, dans le premier cas : $[T]_{k_1} = [S]_{k_1-1} - [S]_{k_1} = 1-0 = 1$ et $[T]_{k_2} = [S]_{k_2-1} - [S]_{k_2} = 0-1 = -1$.
dans le second cas : $[T]_{k_1} = [S]_{k_1-1} - [S]_{k_1} = 0-1 = -1$ et $[T]_{k_2} = [S]_{k_2-1} - [S]_{k_2} = 1-0 = 1$.
Dans tous les cas :

$$\boxed{[T]_{k_1} \times [T]_{k_2} = -1.}$$

3. Le polynôme $H$ vérifie les même conditions que le polynôme $S$ des questions précédentes, donc $(X-1)S$.
Ainsi les coefficients de $K-1 = (X-1)S$ sont tous égaux à $-1$, 0 et 1 et que les 1 et $-1$ s'alternent dans la suite des coefficients de $K-1$.
Par ailleurs, $[(X-1)H]_0 = -[S]_0 \in \{-1, 0\}$ et donc $[K]_0 = [1 + (X-1)H]_0 = 1 - [S]_0 \in \{0, 1\}$.
Si $[K]_0 = 0$, alors nous avons l'alternance de $-1$ et 1 dans les coefficients non nuls de $K-1$ donc de $K$.
Si $[K]_0 = 1$, alors $[S]_0 = 0$, et donc le premier coefficient non nul pour $(X-1)S$ est donné en $r$
avec $[(X-1)S]_r = [S]_{r-1} - [S]_r = 0-1 = -1$, donc $[K]_r = -1$, ce qui alterne bien avec $[K]_0 = 1$.

> Donc $K$ n'a que des coefficients égaux à $-1$, 0 ou 1
> et les 1 et $-1$ s'alternent dans la suite des coefficients (non nuls).

On vérifie bien ce résultat sur notre exemple $(p, q) = (3, 5)$.

4. 1 est racine simple de $G_{pq}$ et de $G_1$, donc racine double de $G_{pq}G_1$.
Et 1 est racine simple de $G_p$ et de $G_q$, donc racine double de $G_pG_q$.
Donc 1 n'est pas racine de $K$.
Et, d'après la factorisation précédente : les racines de $K$, sont les racines de $G_{p,q}$ qui non racines de $G_p$ et de $G_q$.

> Donc les racines de $K$ sont les éléments $\mathbb{U}_{pq} \setminus (\mathbb{U}_p \cup \mathbb{U}_q)$, chacune d'ordre 1.

### ▷ Corrigé de l'exercice 4.4

1. Si $\alpha = 0$, alors $\alpha p + \beta q = \beta q = pq + 1$, donc $(\beta - p)q = 1$. Donc $q$ divise 1. Impossible.
Donc nécessairement, $\alpha \neq 0$ i.e. $\alpha \geqslant 1$. Pour les mêmes raisons : $\beta \geqslant 1$.
Puis $1 - \beta q = (\alpha - q)p$. Or $1 - \beta q < 0$, puisque $\beta \geqslant 1$ et $q > 2$. Donc $\alpha - p < 0$, i.e. $\alpha \leqslant p - 1$.
Pour des raisons symétriques : $\beta \leqslant q - 1$.

$$\boxed{1 \leqslant \alpha \leqslant q-1 \text{ et } 1 \leqslant \beta \leqslant p-1.}$$

2. Notons $T = \left(\sum_{i=0}^{\alpha-1} X^{ip}\right) \times \left(\sum_{j=0}^{\beta-1} X^{jq}\right) - X^{-pq} \left(\sum_{i=\alpha}^{q-1} X^{ip}\right) \times \left(\sum_{j=\beta}^{p-1} X^{jq}\right)$. Alors (telescopage)

$$\begin{aligned}
G_p \times G_q \times T &= \left(G_p \sum_{i=0}^{\alpha-1} (X^p)^i\right) \times \left(G_q \sum_{j=0}^{\beta-1} (X^q)^j\right) - X^{-pq} \left(G_p \sum_{i=\alpha}^{q-1} (X^p)^i\right) \times \left(G_q \sum_{j=\beta}^{p-1} (X^q)^j\right) \\
&= \left(\sum_{i=0}^{\alpha-1} (X^p)^{i+1} - (X^p)^i\right) \left(\sum_{j=0}^{\beta-1} (X^q)^{j+1} - (X^q)^j\right) \\
&\quad - X^{-pq} \left(\sum_{i=\alpha}^{q-1} (X^p)^{i+1} - (X^p)^i\right) \left(\sum_{j=\beta}^{p-1} (X^q)^{j+1} - (X^q)^j\right) \\
&= \left(X^{p\alpha} - 1\right)\left(X^{q\beta} - 1\right) - X^{-pq} \left(X^{pq} - X^{p\alpha}\right)\left(X^{pq} - X^{q\beta}\right) \\
&= X^{p\alpha+q\beta} - X^{q\beta} - X^{p\alpha} + 1 - X^{pq} + X^{q\beta} + X^{p\alpha} - X^{p\alpha+q\beta-pq} \\
&= X^{pq+1} - X^{pq} - X + 1 = (X^{pq} - 1)(X - 1) = G_{pq} \times G_1 = G_p \times G_q \times K
\end{aligned}$$

car $p\alpha + q\beta = pq + 1$.

Par régularité dans $\mathbb{K}[X]$, on a donc

$$\boxed{K = T = \left(\sum_{i=0}^{\alpha-1} X^{ip}\right) \times \left(\sum_{j=0}^{\beta-1} X^{jq}\right) - X^{-pq} \left(\sum_{i=\alpha}^{q-1} X^{ip}\right) \times \left(\sum_{j=\beta}^{p-1} X^{jq}\right)}$$

3. Le polynôme $\sum_{i=0}^{\alpha-1} X^{ip}$ possède exactement $\alpha$ coefficients non nuls ;

et le polynôme $\sum_{j=0}^{\beta-1} X^{jq}$ possède exactement $\beta$ coefficients non nuls.

Par développement, $\left(\sum_{i=0}^{\alpha-1} X^{ip}\right) \times \left(\sum_{j=0}^{\beta-1} X^{jq}\right)$ possède $\alpha \times \beta$ coefficients non nuls,

ce sont les coefficients de $X^0$, $X^p \ldots X^{(\alpha-1)p}$ ; $X^q$, $X^{p+q} \ldots X^{(\alpha-1)p+q}$ ; $\cdots$ et $X^{(\beta-1)q} \ldots X^{(\alpha-1)p+(\beta-1)q}$.

De même, par développement, $\left(\sum_{i=\alpha}^{q-1} X^{ip}\right) \times \left(\sum_{j=\beta}^{p-1} X^{jq}\right)$ possède $(q-\alpha)(p-\beta)$ coefficients non nuls,

ce sont les coefficients de $X^{\alpha p+\beta q}$, $X^{(\alpha+1)p+\beta q} \ldots X^{(q-1)p+(p-1)q}$.

Rappelons que $\alpha p + \beta q = pq + 1$, donc $X^{-pq} \left(\sum_{i=\alpha}^{q-1} X^{ip}\right) \left(\sum_{j=\beta}^{p-1} X^{jq}\right)$ possède comme coefficients non nuls,

les coefficients de $X^1$, $X^{p+1} \cdots X^{pq-p-q}$, en nombre égal à $(q-\alpha)(p-\beta)$.

Tous ces coefficients non nuls sont associés à des monômes distincts.

Donc $K$ possède $\alpha\beta + (q-\alpha)(p-\beta) = 2\alpha\beta - p\alpha - q\beta + pq = 2\alpha\beta - 1$ coefficients non nuls.

$$\boxed{\text{Le nombre } N \text{ de coefficients de } K \text{ est égal à } 2\alpha\beta - 1.}$$

4. On sait que $\alpha p + \beta q = pq + 1$, donc $\beta = -\frac{p}{q}\alpha + p + \frac{1}{q}$.

Considérons $N : \alpha \mapsto 2\alpha(-\frac{p}{q}\alpha + p + \frac{1}{q}) - 1$, polynomiale de la variable réelle $\alpha$.

$N'(\alpha) = -4\frac{p}{q}\alpha + 2p + \frac{2}{q}$. Et donc $N'(\alpha) = 0 \iff \alpha = \frac{pq+1}{2p}$

Comme $N''(\alpha) < 0$, c'est un maximum. Donc : $\forall\ \alpha \in \mathbb{R}$, $N(\alpha) \leqslant N\left(\frac{pq+1}{2p}\right) = \frac{(pq+1)^2}{2pq} - 1 = \frac{p^2q^2+1}{2pq}$.

Ainsi, $N \leqslant \frac{pq}{2} + \frac{1}{2pq} \leqslant \frac{pq}{2} + \frac{1}{2}$ Or $p, q$ sont premiers impairs, donc

$$\boxed{N = \lfloor N \rfloor \leqslant \frac{pq}{2} + \frac{1}{2} - 1 = \frac{pq-1}{2}.}$$