# Réductibilité des polynômes cyclotomiques

Clara Genes

25 mars 2024

## 1 Disclaimers initiaux

Ce document est long MAIS il contient énormément de détails. J'ai mis une page entière d'introduction et rappels que vous êtes censés à peu près maîtriser [1]. Ensuite j'ai mis le développement, mais avec un taux de détails insupportable. Il y a 6 étapes.

- l'**étape 1** est juste pour se mettre dans le bain, il n'y a pas le temps de la présenter
- l'**étape 2** est importante
- l'**étape 3** est importante car permet de conclure. Mathématiquement intéressante ? Je doute un peu...
- l'**étape 4** peut être prise pour acquise le jour de l'oral, ça peut faire une question gratuite
- l'**étape 5** est crutiale
- l'**étape 6** est simplement la conclusion

Ensuite, j'ai rajouté une partie pour des détails en plus [2] et élargir un peu le théorème : en enlevant des hypothèses, en étudiant la réciproque etc... Je ne pense pas que la réciproque soit à savoir car utilise le théorème fort de progression arithmétique de Dirichlet qui est au delà du hors-programme. Le cas avec une hypothèse en moins n'utilise que des choses au programme mais est dangereuse. [3]

En bref : pas de panique, c'est long mais il y a beaucoup de trucs inutiles. Bonne lecture !

**Références :**

Cours d'Algèbre, Daniel Perrin p. ±85
Carnet de voyage en Algébrie, Marie Peronnier et Philippe Caldero p. 220
Exercices d'algèbre, Pascal Ortiz, p.143

1. Ou en tout cas planifier d'à peu près le maîtriser pour votre oral
2. Insupportable, j'ai dis
3. En voilà une belle raison de ne pas en parler au jury...

# 2 Introduction

Un petit récap non exhaustif de ce que l'on sait sur les polynômes cyclotomiques.

**Définition 1.** Soit $k = \mathbb{F}_p$ ou $\mathbb{Q}$. Pour tout $n \in \mathbb{N}^*$ tel que $\text{pgcd}(n,p) = 1$ si $k = \mathbb{F}_p$, on pose $P_n = X^n - 1$ et $K_n$ corps de décomposition de $P_n$ sur $k$. On pose enfin l'ensemble $\mu_n^*(K_n) \coloneqq \{z \in \mathbb{K}_n | z^n = 1 \text{ et } z^k \neq 1 \text{ pour tout } k < n\}$. On définit alors le $n$-ième polynôme cyclotomique comme

$$\Phi_{n,k}(X) = \prod_{z \in \mu_n^*(K_n)} (X - z).$$

**Proposition 2.** Pour tout $n \in \mathbb{N}^*$, le polynôme $\Phi_{n,\mathbb{Q}}$ est un polynôme unitaire, à coefficients entiers et irréductible dans $\mathbb{Z}[X]$ (et donc dans $\mathbb{Q}[X]$). Il est de degré $\varphi(n)$ où $\varphi$ est l'indicatrice d'Euler et on a l'égalité

$$X^n - 1 = \prod_{d|n} \Phi_d(n).$$

En particulier, si $\xi$ est une racine $n$-ième primitive de l'unité dans un corps de caractéristique nulle, son polynome minimal sur $\mathbb{Q}$ est $\Phi_{n,\mathbb{Q}}$ et $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$. Finalement, $\Phi_{n,\mathbb{F}_p}$ s'obtient à partir de $\Phi_{n,\mathbb{Q}}$ par réduction modulo $p$.

*Démonstration.* Cours d'algèbre, Daniel Perrin pages 81-83. □

**Exemple 3.**

- $\Phi_1(X) = X - 1$.
- $\Phi_2(X) = X + 1$.
- $\Phi_p(X) = 1 + X + \cdots + X^{p-1}$, $p$ premier.
- $\Phi_8(X) = X^4 + 1$.

**Proposition 4.** Soit $p$ un nombre premier et $P(X) = \sum_{k=0}^{n} a_i X^i \in \mathbb{Z}[X]$. Notons $\bar{P}$ la réduction de $P$ modulo $p$, *i.e.* le polynôme $P$ vu dans $\mathbb{F}_p[X]$. Alors Si $p \nmid a_n$ et si $\bar{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors $P$ est irréductible dans $\mathbb{Q}[X]$.

*Démonstration.* Cours d'algèbre, Danier Perrin page 77. □

La réciproque de ce théorème n'est pas vraie ! Nous allons le voir en particulier pour les polynômes cyclotomiques.

# 3 Développement

**Théorème 5.** *Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = 1, 2, 4, p^\alpha, 2p^\alpha$ avec $p$ premier impair.*

On décompose $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec les $p_i$ premier distincts et les $\alpha_i$ dans $\mathbb{N}^*$. Par le théorème des restes chinois, on a

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^* .$$

Si $p$ est premier impair, $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$ est cyclique. Plus généralement, on a l'isomorphisme de groupes $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \cong \mathbb{Z}/(p-1)p^{\alpha-1}\mathbb{Z}$ donc est cyclique. Ainsi,

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \left( \prod_{i=1}^{r} \mathbb{Z}/(p_i - 1)p_i^{\alpha_i - 1}\mathbb{Z} \right) \times (\mathbb{Z}/2^\alpha\mathbb{Z})^\times .$$

Or,

- si $\alpha = 1$, on a trivialement $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$ cyclique,
- si $\alpha = 2$, on a $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ cyclique,
- si $\alpha \geqslant 3$, on a $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$. qui n'est pas cyclique.

Ainsi, pour que $(\mathbb{Z}/n\mathbb{Z})^\times$ soit cyclique, il faut et il suffit que $n$ soit de la forme $1, 2, 4, p^\alpha$ ou $2p^\alpha$.

Pour plus de détails : Daniel Perrin, Cours d'algèbre pages 25-28.

**Théorème 6.** *Soit $n$ un entier naturel non nul. Si le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique, alors pour tout $p$ premier ne divisant pas $n$, le polynôme $\Phi_n$ est réductible dans $\mathbb{F}_p[X]$*

*Démonstration.*

- **Etape 1 : Soit $K$ un corps de caractéristique $p$, alors**

$$\begin{array}{rccc} \boldsymbol{F} & : & \boldsymbol{K[X]} & \longrightarrow & \boldsymbol{K[X]} \\ & & \boldsymbol{P = \sum a_i X^i} & \longmapsto & \boldsymbol{F(P) := \sum (a_i)^p X^i} \end{array}$$

  **est un morphisme d'anneaux.**

L'application $F$ respecte évidemment l'axiome de l'unité. Pour ce qui est de la somme et du produit, puisque $f : a \in K \longmapsto a^p \in K$ est un morphisme de corps, on a

$$(a_k + b_k)^p = a_k^p + b_k^p \qquad \text{et} \qquad \left( \sum_{k=0}^{l} a_k b_{l-k} \right)^p = \sum_{k=0}^{l} a_k^p b_{l-k}^p .$$

Ce qui donne $F$ morphisme d'anneaux. En particulier, on a pour tout $a \in K$, $F(X-a) = X-a^p$.

- **Etape 2 : Soit $\alpha$ une racine de $\overline{\Phi}_n$ dans $K$. Alors $\alpha^n = \overline{1}$ et $n$ est l'ordre de $\alpha$ dans $K^*$.**

Puisque $X^n - 1 = \prod_{d|n} \Phi_d(X)$, on a l'égalité modulo $p$ suivante

$$X^n - \overline{1} = \prod_{d|n} \overline{\Phi}_d. \tag{3.1}$$

Puisque $K$ est de caractéristique $p$, il contient $\mathbb{F}_p$ comme sous-corps et donc $\mathbb{F}_p[X] \subset K[X]$. Ainsi, on peut évaluer (3.1) en $\alpha$ en la voyant comme égalité dans $K[X]$ et puisque, par définition $\overline{\Phi}_n(\alpha) = 0$, alors $\alpha^n = \overline{1}$. Il reste alors à montrer que $n$ est effectivement l'ordre de $\alpha$.
D'après ce qui précède, on sait que $\alpha^n = \overline{1}$ ainsi, on veut montrer que si $d$ divise $n$ alors $\alpha^d \neq \overline{1}$. Par l'absurde, supposons qu'il existe $d$ différent de $n$ le divisant tel que $\alpha^d = \overline{1}$. Par l'égalité polynomiale

$$X^d - 1 = \prod_{k|d} \Phi_k(X),$$

on obtient $\Phi_k(\alpha) = 0$ pour un $k$ divisant $d$ donc divisant $n$ strictement. Alors on aurait $\alpha$ comme racine double de $P(X) = X^n - 1$ ce qui est impossible puisque son polynôme dérivé est $P'(X) = nX^{n-1}$. En effet, par hypothèse $p$ ne divisant pas $n$ et $K$ étant de caractéristique $p$, on obtient que $\alpha \neq 0$ n'est pas racine de $P'$ donc est racine simple de $P$ donc son ordre est $n$.

- **Etape 3 : Soit $m = o(p)$ l'ordre de $p$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Alors $m$ est l'entier minimal tel que $\alpha^{p^m} = \alpha$**

Puisque $p$ ne divise pas $n$, ils sont premiers entre-eux. Donc $\overline{p}$ est bien élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ et parler de son ordre dans ce groupe a bien un sens.
Par définition de $m$, on a l'existence d'un $k \in \mathbb{Z}$ tel que $p^m = 1 + nk$. Ainsi,

$$\alpha^{p^m} = \alpha^{nk+1} = \alpha^{nk}\alpha = (\alpha^n)^k\alpha = \overline{1}^k\alpha = \alpha.$$

On souhaite donc montrer que $m$ est minimal. Par l'**étape 2**, $\alpha$ est inversible dans $K$ et son ordre divise $n$. Alors, puisque $n$ est l'ordre de $\alpha$, on a la suite d'équivalences suivante.

$$\begin{aligned}\alpha^{p^m} = \alpha &\iff \alpha^{p^m-1} = 1 \iff n|p^m - 1 \iff \exists k \in \mathbb{Z}, p^m = nk + 1 \\ &\iff \overline{p^m} = \overline{1} \text{ dans } (\mathbb{Z}/n\mathbb{Z})^\times \iff \overline{p}^m = \overline{1}.\end{aligned}$$

Et donc $m$ est minimal non nul si et seulement si $m$ est l'ordre de $p$. Ce qui est le cas par hypothèse.

- **Etape 4 : Soit $Q(X) = \prod_{i=0}^{m-1} \left(X - \alpha^{p^i}\right)$. Alors $Q$ est un polynôme de $\mathbb{F}_p[X]$ qui a $\alpha$ comme racine.**

Par l'**étape 1** on a

$$\begin{aligned}F(Q(X)) =& F\left(\prod_{i=0}^{m-1}\left(X - \alpha^{p^i}\right)\right) = \prod_{i=0}^{m-1} F\left(X - \alpha^{p^i}\right) = \prod_{i=0}^{m-1}\left(X - \alpha^{p^{i+1}}\right) = \prod_{i=1}^{m}\left(X - \alpha^{p^i}\right) \\ =& \prod_{i=1}^{m-1}\left(X - \alpha^{p^i}\right) \times \left(X - \alpha^{p^m}\right) \overset{\text{étape 3}}{=} \prod_{i=1}^{m-1}\left(X - \alpha^{p^i}\right) \times (X - \alpha) \\ =& \prod_{i=0}^{m-1}\left(X - \alpha^{p^i}\right) = Q(X)\end{aligned}$$

Ainsi $F$ stabilise $Q$ et donc en notant $a_i$ les coefficients de $Q$, on a pour tout $i \leqslant m$, $a_i = a_i^p$. En particulier, les coefficients de $Q$ sont racines de $X^p - X$ *i.e.* sont éléments de $\mathbb{F}_p$ et $Q(X)$ est un polynôme de $\mathbb{F}_p[X]$. De plus, par définition,

$$Q(X) = \prod_{i=1}^{m-1} \left(X - \alpha^{p^i}\right) \times (X - \alpha)$$

donc $\alpha$ en est racine.

- **Etape 5 : Si $m < \varphi(n)$, alors $\overline{\Phi}_n$ est réductible sur $\mathbb{F}_p[X]$.**

On rappelle que $\varphi(n) = \deg(\Phi_n) = \deg(\overline{\Phi}_n)$.

Puisque $\alpha \neq 0$ est racine de $Q$ (**étape 4**), ce dernier n'est pas constant et est de degré $m < \varphi(n)$ par hypothèse. On souhaite alors montrer que $Q$ divise $\overline{\Phi}_n$. Pour ce faire, on écrit la division euclidienne de $\overline{\Phi}_n$ par $Q$ :

$$\overline{\Phi}_n(X) = Q(X)B(X) + R(X), \qquad R = 0 \text{ ou } \deg(R) < m.$$

Ainsi, si on montre que les racines de $Q$ sont racines de $\overline{\Phi}_n$ et sont deux à deux disjointes, alors $R$, de degré strictement plus petit de $m$ aura $m$ racines et donc sera le polynôme nul.

(i) Les racines de $Q$ sont racines de $\overline{\Phi}_n$.

Les racines de $Q$ sont de la forme $\alpha^{p^i}$ et on rappelle que $\overline{\Phi}_n(\alpha) = 0$. Il suffit de montrer que si $\beta$ est racine de $\overline{\Phi}_n$ alors $\beta^p$ l'est aussi. Cette propriété est générale pour tout polynôme $P \coloneqq \sum_{i=0}^r a_i X^i \in \mathbb{F}_p[X]$. En effet,

$$\begin{aligned}
\beta \text{ racine de } P \Longrightarrow \sum_{i=0}^{r} a_i \beta^i = 0 &\Longrightarrow F(P(\beta)) = \left(\sum_{i=0}^{r} a_i \beta^i\right)^p = 0 \\
&\overset{\textbf{étape 1}}{\Longrightarrow} \sum_{i=0}^{r} (a_i)^p (\beta^p)^i = 0 \\
&\overset{a_i \in \mathbb{F}_p}{\Longrightarrow} \sum_{i=0}^{r} a_i (\beta^p)^i = 0 \Longrightarrow \beta^p \text{ racine de } P.
\end{aligned}$$

(ii) Les racines de $Q$ sont distinctes deux à deux.

Soient $0 \leqslant k < k' \leqslant m-1$ tels que $\alpha^{p^k} = \alpha^{p^{k'}}$. Alors on a

$$\begin{aligned}
\alpha^{p^k - p^{k'}} = 1 &\overset{\textbf{étape 2}}{\Longleftrightarrow} n | p^k - p^{k'} \Longleftrightarrow \exists l \in \mathbb{Z} \text{ tel que } p^k = p^{k'} + nl \\
&\Longleftrightarrow p^k \equiv p^{k'}[n] \Longleftrightarrow p^{k-k'} \equiv 1[n] \Longleftrightarrow m | k - k'
\end{aligned}$$

Or $0 \leqslant k - k' \leqslant m - 1$ donc $k = k'$ par minimalité de $m$. □

- **Etape 6, déduction du théorème : Si $n \in \mathbb{N}^*$ est tel que $(\mathbb{Z}/n\mathbb{Z})^\times$ ne soit pas cyclique, alors pour tout $p$ premier ne divisant pas $n$, le polynôme $\overline{\Phi}_n$ est réductible dans $\mathbb{F}_p[X]$.**

Par contraposée, si $\overline{\Phi}_n$ est irréductible sur $\mathbb{F}_p[X]$ alors par l'**étape 5** on a

$$m \geqslant \varphi(n) = \operatorname{card}\left(\mathbb{Z}/n\mathbb{Z}\right)^\times.$$

Or $m$ est l'ordre de l'élément $p$ de $(\mathbb{Z}/n\mathbb{Z})^\times$ donc nécessairement $m = \varphi(n)$ et $p$ est un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$. D'où $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

# 4 Pour aller plus loin...ou dans le détail du détail

- **Etape 1, les remarques.**

On a $(a_k b_k)^p = a_k^p b_k^p$ car on est dans un corps commutatif.
On a $(a_k = b_k)^p = a_k^p + b_k^p$ car la caractéristique étant première, on utilise le binôme de Newton et on a le résultat puisque $\binom{k}{p} = 0$ dans $\mathbb{F}_p$ car

$$k\binom{p}{k} = p\binom{p-1}{k-1}, \quad k = 0, \dots, p-1$$

- **Etape 2, les remarques.**

Si $K$ est de caractéristique $p$, il contient un sous-corps isomorphe à $\mathbb{F}_p$ : le morphisme

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & K \\ n & \longmapsto & 1_K \cdot n \end{array}$$

a pour noyau $p\mathbb{Z}$ et se transforme en un isomorphisme $\mathbb{F}_p \to k$ où $k$ est un sous-corps de $K$.

- **Et si $p$ divise $n$ ?**

Si $p$ divise $n$, en notant $n = mp$ on a par le morphisme de Frobenius $P_n = X^n - 1 = (X^m - 1)^p$ et donc $P_n$ possède des racines multiples sur tout corps de décomposition. Le polynôme $\Phi_{n,\mathbb{F}_p}$ n'a pas été défini mais on peut quand même regarder la réduction de $\Phi_{n,\mathbb{Q}}$ modulo $p$. On a le théorème suivant.

**Théorème 7.** *Si $p$ est un diviseur de $n$, la réduction $\overline{\Phi_n}$ est réductible sur $\mathbb{F}_p$ sauf éventuellement si on a $p = 2$ et $n = 2q^\alpha$ avec $q$ premier impair. En particulier, le théorème du développement est encore vrai sans la restriction* $\operatorname{pgcd}(n, p) = 1$.

*Démonstration.* Attention, dans cette démonstration on fait bien la différence entre $\overline{\Phi}_n$ qui est la réduction modulo $p$ et $\Phi_{n,\mathbb{F}_p}$ qui est le polynôme cyclotomique sur $\mathbb{F}_p$ ! !
On pose $n = p^\alpha m$ avec $\operatorname{pgcd}(p, m) = 1$. On a donc, sur $\mathbb{F}_p$, $X^n - 1 = (X^m - 1)^{p^\alpha}$ par Frobenius. Supposons que $\overline{\Phi_n}$ soit irréductible sur $\mathbb{F}_p$. Comme $\overline{\Phi}_n$ divise $X^n - 1$, il divise $X^m - 1$ et puisque l'on a

$$X^m - 1 = \prod_{d|m} \Phi_{d,\mathbb{F}_p}$$

on a par irréductibilité que $\overline{\Phi}_n$ divise l'un des $\Phi_{d,\mathbb{F}_p}$ pour $d$ diviseur de $m$.
En particulier, on a alors en passant aux degrés $\varphi(n) \leqslant \varphi(d)$ et par divisibilité $\varphi(d) \leqslant \varphi(m)$. Mais, par co-primalité, $\varphi(n) = \varphi(m)\varphi(p^\alpha)$ donc nécessairement $\varphi(p^\alpha) = (p-1)p^{\alpha-1} = 1$ imposant donc $p = 2$ *i.e.* $n = 2m$ avec $m$ impair. De plus, si on suppose $d \neq m$ on obtient $\varphi(n) \leqslant \varphi(d) < \varphi(m) = \varphi(n)$ impossible. Donc $d = m$ et finalement $\overline{\Phi}_n$ divise $\Phi_{m,\mathbb{F}_p}$. Par égalité des degrés et unitarité, $\overline{\Phi}_n = \Phi_{m,\mathbb{F}_p}$. On a alors $\Phi_{m,\mathbb{F}_p}$ irréductible avec $\operatorname{pgcd}(m, p) = 1$ et on peut appliquer le développement : $(\mathbb{Z}/m\mathbb{Z})^\times$ est cyclique et donc $m = 1, 2, 4, q^\beta$ ou $2q^\beta$, $q$ premier impair. Par parité, les seules possibilités sont $m = 1$ ou $m = q^\beta$.
Donc on a $n = 2$ ou $n = 2q^\beta$. En particulier, si on se place dans le cas où $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique, on a encore que le polynôme $\Phi_n$ est réductible sur $\mathbb{F}_p$.

Si $n = 2$, le polynôme est $\overline{\Phi_2} = X + \overline{1}$ vu dans $\mathbb{F}_2$ qui n'est pas très interessant.
Si $n = 2q^\beta$, alors on veut étudier $\Phi_{2q^\beta}$ sur $\mathbb{F}_2$. On peut observer que $\Phi_6 = X^2 - X + 1$ irréductible sur $\mathbb{F}_2$ car n'y a aucune racine et est de degré plus petit que 3 et $\Phi_{14} = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = (X^3 + X + 1)(X^3 + X^2 + 1)$ est réductible. □

- **Une réciproque ?**

Est ce que si pour tout $p$ qui ne divise pas $n$ on a la réductibilité du polynôme cyclotomique, alors $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique ? Ou encore, si $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique, est ce qu'il existe un $p$ premier ne divisant pas $n$ tel que $\Phi_n$ soit irréductible sur $\mathbb{F}_p$ ? **La réponse est oui !**
Montrons-le.

*Démonstration.*

- **Etape a : Soient $n \in \mathbb{N}^*$ et $p$ premier tels que $\text{pgcd}(n, p) = 1$. Alors $\overline{\Phi}_n$ est réductible sur $\mathbb{F}_p$ si et seulement si $p$ est d'ordre strictement inférieur à $\varphi(n)$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$.**

Le sens réciproque est exactement l'**étape 5** du développement. Montrons le sens direct.

On rappelle encore que $\deg(\overline{\Phi}_n) = \varphi(n)$. Supposons que $\overline{\Phi}_n = QR$ avec $Q$ et $R$ polynômes unitaires de $\mathbb{F}_p[X] \backslash \mathbb{F}_p^*$. Nécessairement,

$$\deg(Q) = m \leqslant \frac{\varphi(n)}{2} \qquad \text{ou} \qquad \deg(R) = r \leqslant \frac{\varphi(n)}{2},$$

supposons que ce soit au moins le cas pour $Q$. Soit $Q'$ un facteur irréductible de $Q$ et $x$ une racine de $Q'$ dans une extension. Ainsi $\overline{\Phi}_n$ a une racine dans $\mathbb{F}_{p^m}$ car $Q'$ est le polynôme minimal de $x$, est de degré $m$ et $\mathbb{F}_p$ est un sous corps de ses corps de rupture. On conclut par l'**étape 2** du développement que $x$ est d'ordre $n$ dans $\mathbb{F}_{p^m}^*$. Ce dernier étant cyclique d'ordre $p^m - 1$, on a $n | p^m - 1$ donc $p^m = 1$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ et donc l'ordre $d$ de $p$ divise $m < \varphi(n)$.

- **Etape b : Si $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique, il existe un premier $p$ tel que son ordre dans $(\mathbb{Z}/n\mathbb{Z})^\times$ soit $\varphi(n)$.**

Soit $n \in \mathbb{N}^*$ tel que $(\mathbb{Z}/n\mathbb{Z})^\times$ soit cyclique. Soit alors $a \in \mathbb{N}^*$ tel que $\overline{a}$ engendre $(\mathbb{Z}/n\mathbb{Z})^\times$. Nécessairement, $\text{pgcd}(a, n) = 1$. Le théorème (fort) de la progression arithmétique de Dirichlet nous donne qu'il existe [4] $p$ premier tel que $p \equiv a \mod n$. Donc $p = a$ dans le groupe qui nous intéresse. Alors $p$ est d'ordre l'ordre de $a$ donc d'ordre $\varphi(n)$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ et donc par l'**étape a** $\overline{\Phi}_n$ est irréductible dans $\mathbb{F}_p$. □

4. une infinité de