Feuille d'exercices numéro 6

Un polynôme est dit « unitaire » s'il n'est pas nul et si le coefficient de son terme de plus haut degré est 1.

☞ **Exercice 1.** **(a)** Montrer que si un nombre premier p divise tous les coefficients du produit $P(X)Q(X)$, où $P(X)$ et $Q(X)$ sont deux polynômes à coefficients entiers (c'est-à-dire appartenant à $\mathbb{Z}[X]$), alors il divise tous les coefficients de $P(X)$ ou tous les coefficients de $Q(X)$.

(b) Montrer qu'un polynôme à coefficients entiers est irréductible sur $\mathbb{Z}$ si et seulement si il est irréductible sur $\mathbb{Q}$.

(c) Montrer le lemme de Gauss : Si le produit de deux polynômes unitaires de $\mathbb{Q}[X]$ est dans $\mathbb{Z}[X]$, alors ces deux polynômes sont eux aussi dans $\mathbb{Z}[X]$.

☞ **Exercice 2.** Démontrer que l'anneau de polynômes $\mathbb{Z}[X]$ n'est pas principal. (Essayer d'appliquer le théorème de Bézout aux polynômes $X+1$ et $X-1$.)

☞ **Exercice 3.** Soient les polynômes $P(X) = 2X^7 + X^3 - 1$ et $Q(X) = X^3 + 4$ qu'on considère comme des éléments de $\mathbb{Q}[X]$. Appliquer l'algorithme d'Euclide pour déterminer s'ils sont premiers entre eux.

☞ **Exercice 4.** *Soit p un nombre premier et $n \geq 1$ un entier non divisible par p.*

(a) Montrer que le polynôme $X^n - 1$ est premier avec son polynôme dérivé sur le corps $\mathbb{Z}/p\mathbb{Z}$.

(b) Montrer que $X^n - 1$ ne contient pas de facteur carré sur le corps $\mathbb{Z}/p\mathbb{Z}$.

☞ **Exercice 5.** **(a)** Démontrer le critère d'Eisenstein : *Soit $P(X) = a_n X^n + \cdots + a_0$ un polynôme à coefficients entiers et soit p un nombre premier. Si p ne divise pas a_n, mais divise $a_0, \ldots, a_{n-1}$, et si p^2 ne divise pas a_0, alors $P(X)$ est irréductible sur $\mathbb{Q}$.*

(b) Montrer que le polynôme $P(X) = \frac{2}{9}X^5 + \frac{5}{3}X^4 + X^3 + \frac{1}{3}$ est irréductible sur $\mathbb{Q}$.

(c) Montrer que pour p premier, le polynôme $P(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ est irréductible sur $\mathbb{Q}$. (Considérer le polynôme $X^p - 1$ et poser $X = Y + 1$.)

☞ **Exercice 6.** **(a)** Montrer que le polynôme $X^4 + 2 \in (\mathbb{Z}/5\mathbb{Z})[X]$ est irréductible.

(b) On considère le polynôme $P(X) = X^4 + 15X^3 + 7 \in \mathbb{Q}[X]$. Montrer qu'il est irréductible.

☞ **Exercice 7.** *Soit $\mathscr{A}$ un anneau commutatif unitaire. Une « $\mathscr{A}$-algèbre unitaire » $\mathscr{B}$ est un $\mathscr{A}$-module (disons à gauche) muni d'une multiplication $\mathscr{A}$-bilinéaire $\mathscr{B} \times \mathscr{B} \to \mathscr{B}$ et d'une unité $1 \in \mathscr{B}$ en faisant un anneau unitaire. Un morphisme de $\mathscr{A}$-algèbres unitaires est un morphisme d'anneau unitaires $\mathscr{A}$-linéaire.*

(a) Montrer que tout anneau unitaire est une $\mathbb{Z}$-algèbre unitaire et que tout morphisme d'anneaux unitaires est un morphisme de $\mathbb{Z}$-algèbres unitaires.

(b) Soit $\mathscr{B}$ une $\mathscr{A}$-algèbre unitaire telle qu'il existe $b \in \mathscr{B}$ tel que pour tout éléments x dans une $\mathscr{A}$-algèbre unitaire $\mathscr{C}$, il existe un unique morphisme de $\mathscr{A}$-algèbres $f : \mathscr{B} \to \mathscr{C}$ tel que $f(b) = x$. Montrer que $\mathscr{B}$ est isomorphe à l'algèbre des polynômes en une variable $\mathscr{A}[X]$.

(c) Soit $P(X) \in \mathscr{A}[X]$. On considère l'unique morphisme d'algèbres $f : \mathscr{A}[X] \to \mathscr{A}[X]$ tel que $f(X) = P(X)$. Montrer que f est un isomorphisme si et seulement si $P(X)$ est de la forme $P(X) = aX + b$ avec a inversible dans $\mathscr{A}$.

☞ **Exercice 8.** *Soient n et m deux entiers naturels non nuls.*

(a) Montrer que si $n = qm + r$ avec $0 \leq r < m$, alors le reste de la division euclidienne de $X^n - 1$ par $X^m - 1$ est $X^r - 1$.

(b) En utilisant l'algorithme d'Euclide, en déduire que $\mathrm{PGCD}(X^n - 1, X^m - 1) = X^{\mathrm{PGCD}(n,m)} - 1$.

☞ **Exercice 9.** *Soit K un corps fini commutatif. On note K^* le groupe multiplicatif (groupe des éléments inversibles) de K.*

(a) Soit k la borne supérieure des ordres des éléments du groupe K^*. Montrer que pour tout $x \in K^*$, on a

$x^k = 1$. (Utiliser le théorème de structure des groupes abéliens finis.)

(b) En déduire que K^* est un groupe cyclique.

☞ **Exercice 10.** *Le polynôme* $\Phi_n(X) = \prod_{\zeta}(X - \zeta)$, *où le produit est étendu aux racines primitives* $n^{\text{ièmes}}$ *de l'unité* ($n \geq 1$) *est appelé « polynôme cyclotomique ». Son degré est clairement* $\phi(n)$, *où* ϕ *est l'indicatrice d'Euler, et c'est un polynôme unitaire (le coefficient du terme de plus haut degré vaut* 1*).*

(a) Calculer $\Phi_1(X)$ à $\Phi_8(X)$.

(b) Montrer que $X^n - 1 = \prod_{d|n} \Phi_d(X)$, où le produit est étendu à tous les diviseurs de n. En déduire une formule donnant $\Phi_n(X)$ en fonction des $\Phi_d(X)$ tels que d soit un diviseur strict (i.e. $\neq n$) de n.

(c) Soit $\Psi_n(X)$ ($n \geq 1$) une suite de polynômes telle que $X^n - 1 = \prod_{d|n} \Psi_d(X)$ pour tout $n \geq 1$. Montrer que $\Psi_n(X) = \Phi_n(X)$.([1])

(d) Montrer par récurrence sur n que $\Phi_n(X) \in \mathbb{Z}[X]$.

(e) Montrer que la fonction $x \mapsto \Phi_n(x)$ (de $\mathbb{R}$ vers $\mathbb{R}$) est strictement croissante sur l'intervalle $[1, +\infty)$.

(f) Montrer que pour $n \geq 2$, $\Phi_n(0) = 1$, puis que $X^{\phi(n)}\Phi_n(1/X) = \Phi_n(X)$ (on dit que $\Phi_n(X)$ est un « polynôme réciproque »).

☞ **Exercice 11.** *Soit* $n \geq 1$ *un entier. Soit* $\zeta \in \mathbb{C}$ *une racine primitive* $n^{\text{ième}}$ *de l'unité (donc racine du polynôme cyclotomique* $\Phi_n(X)$*).*

(a) Montrer que l'idéal $\mathscr{I}_\zeta$ de l'anneau principal $\mathbb{Q}[X]$ défini par $\mathscr{I}_\zeta = \{P(X) \in \mathbb{Q}[X] \mid P(\zeta) = 0\}$ est engendré par un polynôme irréductible unitaire à coefficients entiers (qu'on notera $\chi_\zeta(X)$).

Soit p *un nombre premier tel que* $\tau = \zeta^p$ *soit encore une racine primitive* $n^{\text{ième}}$ *de l'unité.*

(b) Montrer que si $\chi_\tau(X) \neq \chi_\zeta(X)$, il existe des polynômes $A(X)$ et $B(X)$ à coefficients entiers tels que $\Phi_n(X) = \chi_\zeta(X)\chi_\tau(X)A(X)$ et $\chi_\tau(X^p) = \chi_\zeta(X)B(X)$.

On note $P(X) \mapsto \overline{P}(X)$ le morphisme canonique (d'anneaux unitaires) $\mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$.

(c) Montrer que p ne divise pas n, puis que $\overline{\Phi_n}(X)$ n'a pas de facteur carré.

(d) Montrer que $\overline{\chi_\tau}(X^p) = (\overline{\chi_\tau}(X))^p$. (Utiliser la formule du binôme.)

(e) Déduire de ce qui précède que $\chi_\tau(X) = \chi_\zeta(X)$.

(f) En déduire que $\Phi_n(X)$ est irréductible sur $\mathbb{Z}$.

---

1. Ceci constitue la véritable définition des polynômes cyclotomiques, la définition donnée au début de l'exercice n'en étant en fait qu'une construction.

Solutions des exercices de la feuille 6

☞ **Exercice 1.** **(a)** C'est une conséquence immédiate du fait que tout anneau de polynômes sur un corps (ici $(\mathbb{Z}/p\mathbb{Z})[X]$) est intègre. Rappelons-en la démonstration. Soient $P(X)$ et $Q(X)$ deux éléments de $K[X]$ tels que $P(X)Q(X) = 0$. Supposons $P(X)$ et $Q(X)$ non nuls, et soient aX^n et bX^p les termes de plus haut degré de $P(X)$ et $Q(X)$. On a $a \neq 0$ et $b \neq 0$, mais ceci est incompatible avec le fait que le terme de plus haut de degré de $P(X)Q(X)$ est abX^{n+p} et le fait que $ab \neq 0$ (tout corps est un anneau intègre).

(b) Le fait que tout polynôme irréductible sur $\mathbb{Q}$ soit irréductible sur $\mathbb{Z}$ est trivial. Pour prouver la réciproque, il suffit de montrer que tout polynôme $P(X)$ à coefficients entiers réductible sur $\mathbb{Q}$ est réductible sur $\mathbb{Z}$. Supposons donc que $P(X) = A(X)B(X)$, avec $A(X)$ et $B(X)$ dans $\mathbb{Q}[X]$. On peut écrire $A(X)B(X)$ sous la forme $\frac{1}{n}A'(X)B'(X)$ où $A'(X)$ et $B'(X)$ sont à coefficients entiers et où l'entier n n'a pas de facteur divisant tous les coefficients de $A'(X)$ ou tous les coefficients de $B'(X)$. On a alors l'égalité $nP(X) = A'(X)B'(X)$ entre polynômes à coefficients entiers. Si le nombre premier p divise n, il divise tous les coefficients de $nP(X)$, donc tous ceux de $A'(X)$ ou tous ceux de $B'(X)$ d'après **(a)**, ce qui est impossible. On a donc $n = \pm 1$, et $P(X)$ est réductible sur $\mathbb{Z}$.

(c) Soient $A(X)$ et $B(X)$ deux polynômes unitaires à coefficients rationnels tels que $P(X) = A(X)B(X)$ soit à coefficients entiers. On peut supposer que $A(X) = \frac{a}{b}A'(X)$ et $B(X) = \frac{c}{d}B'(X)$ où $\frac{a}{b}$ et $\frac{c}{d}$ sont des fractions irréductibles et où les coefficients de $A'(X)$ (resp. $B'(X)$) sont premiers entre eux dans leur ensemble. Comme $A(X)$ est unitaire, $\frac{a}{b}$ (qu'on peut supposer être une fraction irréductible) doit être l'inverse du coefficient du terme de plus haut degré de $A'(X)$, mais comme ce dernier est entier, on doit avoir $a = \pm 1$. De même, on a $c = \pm 1$. On peut sans perte de généralité supposer que $a = c = 1$. On a alors $A'(X)B'(X) = bdP(X)$. Tout nombre premier qui divise bd doit alors diviser tous les coefficients du produit $A'(X)B'(X)$ donc tous les coefficients de $A'(X)$ ou tous ceux de $B'(x)$, ce qui est impossible. On voit donc que $bd = \pm 1$, donc que $b = \pm d = \pm 1$, et donc que $A(X)$ et $B(X)$ sont à coefficients entiers.

☞ **Exercice 2.** Si on pouvait appliquer le théorème de Bézout, on aurait deux polynômes $A(X)$ et $B(X)$ tels que $A(X)(X+1) + B(X)(X-1) = 1$. En faisant $X = 1$, on obtient $2A(1) = 1$, égalité impossible dans $\mathbb{Z}$.

☞ **Exercice 3.** La division euclidienne de $P(X)$ par $Q(X)$ a pour reste $R(X) = 32X - 5$, celle de $Q(X)$ par $R(X)$ a pour reste $\frac{31197}{32768}$. Le reste suivant est nul. Le dernier reste non nul est donc un élément inversible de $\mathbb{Q}[X]$, c'est-à-dire équivalent (associé) à 1. Les polynômes $P(X)$ et $Q(X)$ sont donc premiers entre eux.

☞ **Exercice 4.** **(a)** Le polynôme dérivé de $P(X) = X^n - 1$ est $P'(X) = nX^{n-1}$. On a par ailleurs $XP'(X) - nP(X) = nX^n - nX^n + n = n$, et comme n est inversible dans $\mathbb{Z}/p\mathbb{Z}$, on voit que $P(X)$ et $P'(X)$ sont premiers entre eux.

(b) Si on pouvait écrire $P(X) = X^n - 1 = A(X)A(X)B(X)$, avec $A(X)$ de degré au moins 1, on aurait $P'(X) = 2A'(X)A(X)B(X) + A(X)A(X)B'(X)$, soit un polynôme divisible par $A(X)$, ce qui contredit le résultat de la question précédente.

☞ **Exercice 5.** **(a)** Il suffit de montrer que $P(X)$ est irréductible sur $\mathbb{Z}$. Supposons que $P(X) = U(X)V(X)$ où $U(X) = u_kX^k + \cdots + u_0$ et $V(X) = v_lX^l + \cdots + v_0$ sont deux polynômes non constants à coefficients entiers. On a $a_0 = u_0v_0$, et donc p divise u_0 ou v_0 mais pas les deux à la fois. On peut supposer que $p|u_0$ et $p \not| v_0$. Par ailleurs, p ne peut pas diviser tous les u_i car a_n serait divisible par p. Il existe donc un plus petit i tel que $p \not| u_i$, et on a $a_i = u_0v_i + \cdots + u_iv_0$. Comme $i < n$, $p|a_i$ et donc $p|u_iv_0$, mais comme $p \not| u_i$, on voit que $p|v_0$, ce qui est contradictoire. Ainsi, $P(X)$ est irréductible sur $\mathbb{Z}$, et donc sur $\mathbb{Q}$.

(b) Il suffit de montrer que $9P(X)$ est irréductible sur $\mathbb{Z}$. Le critère d'Eisenstein s'applique avec $p = 3$.

(c) On a $P(X) = \frac{X^p - 1}{X - 1}$. Si $P(X)$ était réductible, il en serait de même du polynôme en Y : $P(Y+1)$. Or, $P(Y+1) = \frac{(Y+1)^p - 1}{Y} = C_p^0Y^{p-1} + C_p^1Y^{p-2} + \cdots + C_p^{p-1}$. Or tous ces coefficients du binôme sont divisbles par p sauf $C_p^0 = 1$, et $C_p^{p-1} = p$ n'est par divisible par p^2. Le critère d'Eisenstein s'applique.

☞ **Exercice 6.** **(a)** Les éléments de $\mathbb{Z}/5\mathbb{Z}$ sont 0, 1, 2, 3 et 4, et leurs puissances $4^{\text{ièmes}}$ sont 0, 1, 1, 1

et 1. Il en résulte que X^4+2 n'a pas de racine dans $\mathbb{Z}/5\mathbb{Z}$. S'il est réductible, il doit s'écrire $X^4+2=(X^2+aX+b)(X^2+cX+d)$. On peut en effet se ramener à des polynômes unitaires en divisant l'un des facteurs et en multipliant l'autre par un scalaire non nul convenable. On a alors $a+c=0$, $ac+b+d=0$ et $bd=2$, donc $b+d=a^2$. Mais les seuls carrés de $\mathbb{Z}/5\mathbb{Z}$ sont 0, 1 et -1, ce qui implique que $-b^2=2$ ou que $b(1-b)=2$ ou que $b(1+b)=-2$. En essayant toutes les valeurs possibles pour b, on voit qu'aucune de ces égalités ne peut être satisfaite.

(b) Si le polynôme X^4+15X^3+7 était réductible sur $\mathbb{Q}$, il le serait qur $\mathbb{Z}$, et sa réduction modulo 5 le serait sur $\mathbb{Z}/5\mathbb{Z}$. Mais cette réduction est X^4+2 qui ne l'est pas.

☞ **Exercice 7.** **(a)** Ceci résulte simplement du fait que l'additivité $f(x+y)=f(x)+f(y)$ entraîne la $\mathbb{Z}$-linéarité.

(b) Par hypothèse, il existe un unique morphisme de $\mathscr{A}$-algèbres $\varphi:\mathscr{B}\to\mathscr{A}[X]$ tel que $\varphi(b)=X$. Si $P(X)=a_nX^n+\cdots+a_0\in\mathscr{A}[X]$, on peut poser $\psi(P(X))=a_nb^n+\cdots+a_0$. On définit ainsi une application $\psi:\mathscr{A}[X]\to\mathscr{B}$. Il est par ailleurs immédiat que $\psi\circ\varphi=1_{\mathscr{B}}$ et que $\varphi\circ\psi=1_{\mathscr{A}[X]}$.

(c) Supposons d'abord que $P(X)=aX+b$ avec a inversible. On pose $Q(X)=\dfrac{Y-b}{a}$, et on a un unique morphisme de $\mathscr{A}$-algèbres $g:\mathscr{A}[X]\to\mathscr{A}[X]$ tel que $g(X)=Q(X)$. On voit alors que $g(f(X))=X$ et que $f(g(X))=X$. Il en résulte que $g\circ f$ et $f\circ g$ sont l'identité de $\mathscr{A}[X]$.

Réciproquement, supposons que f soit un isomorphisme et notons g son inverse. Posons $P(X)=a_nX^n+\cdots+a_0$ et soit $Q(X)=b_pX^p+\cdots+b_0$ l'image de X par g. On a $g(P(X))=g(a_nX^n+\cdots+a_0)=a_ng(X)^n+\cdots+a_0=a_nQ(X)^n+\cdots+a_0$. Mais par ailleurs, $g(P(X))=g(f(X))=X$. Ceci implique que $n+p=1$ et que $a_nb_p=a_1b_1=1$. Les deux polynômes $P(X)$ et $Q(X)$ sont donc de degré 1, avec un coefficient du terme de degré 1 inversible.

☞ **Exercice 8.** **(a)** On effectue la division :

$$\begin{array}{rrrrrr|l}
X^n & & & & & -1 & X^m-1 \\
\cline{7-7}
 & X^{n-m} & & & & & X^{n-m}+X^{n-2m}+\cdots+X^{n-qm} \\
 & & X^{n-2m} & & & & \\
 & & & \cdots & & & \\
 & & & & X^{n-qm} & -1 &
\end{array}$$

On voit que la division ne peut pas être continuée car $n-qm=r<m$.

(b) On obtient le PGCD de n et m (en supposant $n>m$) par l'algorithme d'Euclide de la façon suivante :

$$\begin{array}{rcll}
n & = & q_0m+r_1 & 0\le r_1<m \\
m & = & q_1r_1+r_2 & 0\le r_2<r_1 \\
 & \cdots & & \\
r_{k-1} & = & q_kr_k &
\end{array}$$

Le PGCD de n et m est alors r_k. En utilisant la question **(a)**, on a de même :

$$\begin{array}{rcll}
X^n-1 & = & Q_0(X)(X^m-1)+X^{r_1}-1 & 0\le r_1<m \\
X^m-1 & = & Q_1(X)(X^{r_1}-1)+X^{r_2}-1 & 0\le r_2<r_1 \\
 & \cdots & & \\
X^{r_{k-1}}-1 & = & Q_k(X)(X^{r_k}-1) &
\end{array}$$

et on voit que le PGCD de X^n-1 et de X^m-1 est $X^{r_k}-1$.

☞ **Exercice 9.** **(a)** Comme le corps K est fini et commutatif, le groupe multiplicatif K^* est un groupe abélien fini, et il est donc isomorphe à un groupe (additif) de la forme $(\mathbb{Z}/a_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/a_n\mathbb{Z})$, avec $a_1|\ldots|a_n$. On alors $k=a_n$ et l'ordre de tout élément de K^* divise k.

(b) Le polynôme X^k-1 a, d'après la question précédente, tous les éléments de K^* pour racines. Toutefois, sur un corps commutatif, un polynôme ne peut pas avoir plus de racines que son degré. Il en résulte que k est le cardinal de K^*. Comme par finitude de K^* il existe un x d'ordre k dans K^*, cet x est un générateur de K^*, qui est donc cyclique.

☞ **Exercice 10.** **(a)** On a

$$\begin{array}{lcllcl}
\Phi_1(X) & = & X-1 & \Phi_5(X) & = & X^4+X^3+X^2+X+1\\
\Phi_2(X) & = & X+1 & \Phi_6(X) & = & X^2-X+1\\
\Phi_3(X) & = & X^2+X+1 & \Phi_7(X) & = & X^6+X^5+X^4+X^3+X^2+X+1\\
\Phi_4(X) & = & X^2+1 & \Phi_8(X) & = & X^4+1
\end{array}$$

(b) Le polynôme X^n-1 est juste le produit des $X-\zeta$ pour tous les ζ qui sont des racines $n^{\text{ièmes}}$ de l'unité. Les racines $n^{\text{ièmes}}$ de l'unité se répartissent en classes en fonction de leur ordre d qui est un diviseur de n. Or les éléments d'ordre d sont les racines primitives $d^{\text{ièmes}}$ de l'unité. La formule en résulte. En isolant $\Phi_n(X)$, on obtient immmédiatement $\Phi_n(X)=\dfrac{X^n-1}{\prod_{d|n,d<n}\Phi_d(X)}$.

(c) On a $\Psi_1(X)=X-1$, puis par récurrence $\Psi_n(X)=\Phi_n(X)$ en utilisant la formule de la question précédente.

(d) On sait déjà que $\Phi_n(X)\in\mathbb{Z}[X]$ pour $n\leq 8$. La formule de la question **(b)** et le lemme de Gauss donnent immédiatement le résultat par récurrence.

(e) Les cas $n=1$ et $n=2$ étant trivaux, on peut supposer $n\geq 3$, ce qui fait que les racines primitives $n^{\text{ièmes}}$ de l'unité sont des nombres non réels (distincts de 1 et de -1) et en nombre pair, chaque élément ayant son conjugué. Le produit $(X-\zeta)(X-\overline{\zeta})$ étant égal à $X^2-(\zeta+\overline{\zeta})X+\zeta\overline{\zeta}$, équation d'une parabole ayant ses branches tournées vers le haut, ne rencontrant pas l'axe des réels et dont le point le plus bas est à l'abscisse $\dfrac{\zeta+\overline{\zeta}}{2}<1$. Comme un produit de fonctions réelles positive strictement croissantes est une fonction positive strictement croissante, on a le résultat annoncé.

(f) On a $\Phi_2(0)=1$, et pour $n\geq 3$, l'ensemble $E_n=\{\zeta_1,\ldots,\zeta_{\phi(n)}\}$ des racines primitives $n^{\text{ièmes}}$ de l'unité ne contient que des non réels et est stable par conjugaison. Les racines se groupent donc par deux (chaque racine avec sa conjuguée) et le produit de toutes les racines est un réel positif de module 1. C'est donc 1.

On peut supposer $n\geq 3$. Comme le conjugué d'un complexe de module 1 est aussi son inverse, on a

$$\begin{array}{rcl}
X^{\phi(n)}\Phi_n(1/X) & = & X^{\phi(n)}(1/X-\zeta_1^{-1})\ldots(1/X-\zeta_{\phi(n)}^{-1})\\
& = & (1-X\zeta_1^{-1})\ldots(1-X\zeta_{\phi(n)}^{-1})\\
& = & \zeta_1\ldots\zeta_{\phi(n)}(1-X\zeta_1^{-1})\ldots(1-X\zeta_{\phi(n)}^{-1})\\
& = & (\zeta_1-X)\ldots(\zeta_{\phi(n)}-X)\\
& = & \Phi_n(X)
\end{array}$$

la dernière égalité parce que $\phi(n)$ est un nombre pair.

☞ **Exercice 11.** **(a)** Comme $\mathbb{Q}[X]$ est un anneau principal, l'idéal $\mathscr{I}_\zeta$ est principal, donc engendré par un polynôme $P(X)$, qui n'est pas nul car $\Phi_n(X)\in\mathscr{I}_\zeta$ puisque $\Phi_n(\zeta)=0$, et qu'on peut supposer unitaire. Il en résulte de plus que $P(X)$ divise $\Phi_n(X)$ et est donc à coefficients entiers par le lemme de Gauss. Si $P(X)$ était réductible, disons $P(X)=A(X)B(X)$ où $A(X)$ et $B(X)$ sont de degrés strictement inférieurs au degré de $P(X)$, ζ serait racine de $A(X)$ ou de $B(X)$ et l'un de ces deux polynômes serait dans $\mathscr{I}_\zeta$, c'est-à-dire un multiple de $P(X)$, ce qui est impossible pour des raisons de degré.

(b) Comme ζ et τ sont deux racines de $\Phi_n(X)$, les polynômes $\chi_\zeta(X)$ et $\chi_\tau(X)$ divisent tous deux $\Phi_n(X)$. De plus, ils sont premiers entre eux. En effet, s'ils avaient un facteur commun (non inversible, c'est-à-dire de degré au moins 1), ils seraient tous deux égaux à ce facteur (modulo la multiplication par un inversible) car ils sont irréductibles. Comme ils sont par ailleurs unitaires, ils seraient égaux, ce qui n'est pas. Il en résulte que le produit $\chi_\zeta(X)\chi_\tau(X)$ divise $\Phi_n(X)$, et qu'on peut écrire : $\Phi_n(X)=\chi_\zeta(X)\chi_\tau(X)A(X)$, avec $A(x)$ à coefficients entiers d'après le lemme de Gauss.

Comme $0=\chi_\tau(\tau)=\chi_\tau(\zeta^p)$, $\chi_\zeta(X)$ divise $\chi_\tau(X^p)$, et on a $\chi_\tau(X^p)=\chi_\zeta(X)B(X)$, avec $B(X)$ à coefficients entiers toujours par le lemme de Gauss.

(c) Comme τ est une racine primitive $n^{\text{ième}}$ de l'unité, il existe un entier a tel que $\tau^a=\zeta$. On a donc $\zeta^{pa}=\zeta$, d'où $\zeta^{pa-1}=1$, ce qui montre que n divise $pa-1$, donc qu'il existe un entier b tel que $pa-1=bn$, ou encore que p et n sont premiers entre eux. Il résulte alors d'un des exercices précédents que X^n-1 n'a pas de facteur carré dans $\mathbb{Z}/p\mathbb{Z}$, et qu'il en est donc de même de son diviseur $\overline{\Phi_n}(X)$.

(d) En fait, le résultat est valable pour un polynôme $P(X)$ quelconque à coefficients entiers. On sait que le coefficient du binôme $C_p^i = \dfrac{p!}{(p-i)!i!}$ est divisible par p pour i différent de 0 et de p (c'est visible sur la formule utilisant les factorielles sachant que p est premier). Il en résulte que l'application $x \mapsto x^p$ de $\mathbb{Z}/p\mathbb{Z}$ vers lui-même est un morphisme d'anneaux unitaires (appelé « morphisme de Frobenius »). En effet, elle respecte clairement la multiplication et l'unité, et également l'addition puisque $(x+y)^p = x^p + y^p$ d'après la remarque précédente sur les coefficients du binôme. Elle respecte aussi l'opposé (car $1 = -1$ dans le cas $p = 2$) et le zéro. Il en résulte immédiatement que $P(X)^p = P(X^p)$.

(e) Si $\chi_\tau(X) \neq \chi_\zeta(X)$, on peut utiliser la question **(b)**, et on a des polynômes à coefficients entiers $A(X)$ et $B(X)$ tels que $\Phi_n(X) = \chi_\zeta(X)\chi_\tau(X)A(X)$ et $\chi_\tau(X^p) = \chi_\zeta(X)B(X)$. On en déduit que $\overline{\chi_\zeta}(X)\overline{\chi_\tau}(X)$ divise $\overline{\Phi_n}(X)$ et que $\overline{\chi_\zeta}(X)$ divise $\overline{\chi_\tau}(X^p)$, donc $(\overline{\chi_\tau}(X))^p$. Soit $P(X)$ un facteur irréductible de $\overline{\chi_\zeta}(X)$. Alors $P(X)$ divise à la fois $\overline{\chi_\zeta}(X)$ et $\overline{\chi_\tau}(X)$, ce qui fait que $\overline{\Phi_n}(X)$ a un facteur carré, ce qui ne se peut pas.

(f) Si ζ et ζ' sont deux racines primitives $n^{\text{ièmes}}$ de l'unité, il existe un entier a tel que $\zeta' = \zeta^a$. Comme a peut être décomposé en facteurs premiers, il résulte de la question précédente que $\chi_\zeta(X) = \chi_{\zeta'}(X)$. Ainsi, toutes les racines primitives $n^{\text{ièmes}}$ de l'unité sont racines de $\chi_\zeta(X)$ qui est donc de degré au moins $\phi(n)$. Comme par ailleurs, $\chi_\zeta(X)$ divise $\Phi_n(X)$ qui est lui aussi de degré $\phi(n)$, ces deux polynômes sont associés, et donc égaux puisqu'unitaires. Il en résulte que $\Phi_n(X)$ est irréductible.