Polynômes cyclotomiques, intégralité : correction

Exercice 1.

1. Si $m_{s,\mathrm{K}}$ n'était pas irréductible dans K[X], on pourrait écrire $m_{s,\mathrm{K}} = \mathrm{AB}$, pour deux polynômes $\mathrm{A}, \mathrm{B} \in \mathrm{K}[\mathrm{X}]$ non constants. Quitte à multiplier A par le coefficient dominant de B et réciproquement, on peut supposer A et B unitaires. Comme $\mathrm{A}(s)\mathrm{B}(s) = m_{s,\mathrm{K}}(s) = 0$ et que $\deg m_{s,\mathrm{K}} = \deg \mathrm{A} + \deg \mathrm{B}$, l'un des deux polynômes, A ou B, admet s comme racine et est de degré strictement inférieur à celui de $m_{s,\mathrm{K}}$, ce qui est absurde. Le polynôme $m_{s,\mathrm{K}}$ est donc irréductible dans K[X].

   Soit $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ s'annulant en s. Par division euclidienne, on peut trouver deux polynômes $\mathrm{Q}, \mathrm{R} \in \mathrm{K}[\mathrm{X}]$ tels que $\mathrm{P} = \mathrm{Q}\, m_{s,\mathrm{K}} + \mathrm{R}$ avec $\deg \mathrm{R} < \deg m_{s,\mathrm{K}}$. On voit alors que $\mathrm{R}(s) = 0$ ce qui entraîne, par minimalité de $m_{s,\mathrm{K}}$, que $\mathrm{R} = 0$. Le polynôme P est donc bien divisible par $m_{s,\mathrm{K}}$ dans K[X].

   Si $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ est unitaire, irréductible, et admet $s \in \mathrm{L}$ comme racine, l'élement s est bien algébrique sur K, ce qui entraîne l'existence du polynôme minimal $m_{s,\mathrm{K}}$. La discussion précédente entraîne que P est divisible par $m_{s,\mathrm{K}}$. Puisque P est irréductible et unitaire, cela entraîne que P est égal à $m_{s,\mathrm{K}}$ à une constante près, constante qui ne peut valoir que 1 puisque les deux polynômes sont unitaires. On a donc bien $\mathrm{P} = m_{s,\mathrm{K}}$.

2. Soit $d = [\mathrm{L} : \mathrm{K}]$. On rappelle que c'est la dimension du K-espace vectoriel L. La famille $(1, s, s^2, \ldots, s^d)$, de longueur $d+1$, est donc liée, ce qui entraîne l'existence d'éléments $a_0, \ldots, a_d \in \mathrm{K}$ non tous nuls tels que

$$a_d s^d + a_{d-1} s^{d-1} + \cdots + a_1 s + a_0 = 0.$$

   En particulier, s est une racine du polynôme $\mathrm{P}(\mathrm{X}) = a_d \mathrm{X}^d + \cdots + a_1 \mathrm{X} + a_0$, de degré inférieur ou égal à d. La question précédente affirme alors que $m_{s,\mathrm{K}}$ divise ce polynôme, d'où $\deg m_{s,\mathrm{K}} \leq \deg \mathrm{P} \leq d$.

3. Rappelons que $s \in \mathrm{L}$ est *entier* sur A s'il existe un polynôme unitaire non nul $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ tel que $\mathrm{P}(s) = 0$. La première question entraîne que P est alors un multiple de $m_{s,\mathrm{K}}$ dans K[X]. Ainsi, toutes les racines de m_s dans $\overline{\mathrm{K}}$ sont des racines de P. Le polynôme P étant unitaire, toutes ses racines sont donc des éléments de la clôture intégrale $\mathrm{A}_{\overline{\mathrm{K}}}$ de A dans $\overline{\mathrm{K}}$. Il en va donc de même des racines de $m_{s,\mathrm{K}}$ et, d'après les relations coefficients-racines, de ses coefficients. Mais les coefficients de $m_{s,\mathrm{K}}$ sont également dans K. Puisque par définition $\mathrm{A}_{\overline{\mathrm{K}}} \cap \mathrm{K} = \mathrm{A}_{\mathrm{K}}$, on a bien $m_{s,\mathrm{K}} \in \mathrm{A}_{\mathrm{K}}[\mathrm{X}]$.

   Réciproquement, si $m_{s,\mathrm{K}} \in \mathrm{A}_{\mathrm{K}}[\mathrm{X}]$, l'élément $s \in \mathrm{L}$ est entier sur A_{K}. Il appartient donc à la clôture intégrale de A_{K} dans L. Mais A_{L}, qui contient A_{K}, est intégralement close dans L (c'est un résultat du cours : une clôture intégrale est intégralement close). L'élément s appartient donc à A_{L}, c'est-à-dire qu'il est entier sur A.

   Remarque. En particulier, si A est intégralement clos dans son corps des fractions (c'est-à-dire si $\mathrm{A} = \mathrm{A}_{\mathrm{K}}$), un élement $s \in \mathrm{L}$ est entier sur K si et seulement si son polynôme minimal $m_{s,\mathrm{K}}$ est dans A[X]. D'après la question 4 de l'exercice 1 du TD 3, c'est le cas de $\mathbf{Z}$ (ou de tout anneau factoriel, c'est la même preuve).

4. Soit $f \in \mathrm{A}[\mathrm{X}]$ un polynôme unitaire et g un facteur irréductible de f dans K[X]. Les facteurs irréductibles ne sont définis qu'à multiplication près par une unité de A. Puisque ce sont des facteurs irréductibles d'un polynôme unitaire, leurs coefficients dominants

sont tous inversibles, et on peut supposer les facteurs unitaires. Soit L/K une extension de K dans laquelle g possède une racine s. D'après la première question, $g = m_{s,\mathrm{K}}$. Puisque s est également une racine de f, s est entier sur A et la question précédente entraîne que $g = m_{s,\mathrm{K}}$ soit à coefficients dans $\mathrm{A}_\mathrm{K} = \mathrm{A}$. Les facteurs irréductibles de f sont donc à coefficients dans A.

Exercice 2.

1. L'intersection d'une famille quelconque de sous-corps reste un sous-corps.
2. La sous-$\mathbf{Q}$-algèbre $\mathbf{Q}[\mathrm{S}]$ est par définition un anneau intègre contenant S. L'ensemble K des $z_1/z_2 \in \mathbf{C}$, où (z_1, z_2) décrit $\mathbf{Q}[\mathrm{S}] \times (\mathbf{Q}[\mathrm{S}] \setminus \{0\})$, est un sous-corps de $\mathbf{C}$ isomorphe à $\mathrm{Frac}(\mathbf{Q}[\mathrm{S}])$. Le corps K contient S, donc il contient également $\mathbf{Q}(\mathrm{S})$. Réciproquement, tout sous-corps de $\mathbf{C}$ contenant $\mathbf{Q}[\mathrm{S}]$, en particulier $\mathbf{Q}(\mathrm{S})$, doit contenir les éléments de K. On a donc bien $\mathbf{Q}(\mathrm{S}) = \mathrm{K} \simeq \mathrm{Frac}(\mathbf{Q}[\mathrm{S}])$.
3. Par définition, $\mathbf{Q}[s] \subset \mathbf{Q}(s)$. On va démontrer que $\mathbf{Q}[s]$ est un corps, ce qui donnera l'inclusion réciproque. Soit $m_s \in \mathbf{Q}[\mathrm{X}]$ le polynôme minimal de s. Si $\alpha \in \mathbf{Q}[s]$ est non nul, il existe un polynôme $\mathrm{P} \in \mathbf{Q}[\mathrm{X}]$ tel que $\alpha = \mathrm{P}(s)$ et ce polynôme n'est pas divisible par m_s. Par irréductibilité de m_s, cela entraîne que P et m_s sont premiers entre eux. On peut alors trouver une relation de Bézout : il existe $\mathrm{A}, \mathrm{B} \in \mathbf{Q}[\mathrm{X}]$ tels que $\mathrm{A}m_s + \mathrm{BP} = 1$. En spécialisant en s, il vient $1 = \mathrm{B}(s)\mathrm{P}(s)$, ce qui démontre que $\mathrm{P}(s) = \alpha$ est inversible dans $\mathbf{Q}[s]$ (et son inverse est $\mathrm{B}(s)$.
4. Par définition, si s est transcendant, le morphisme d'anneaux $\mathbf{Q}[\mathrm{X}] \to \mathbf{Q}[s]$ est injectif et donc est un isomorphisme. On a donc $\mathbf{Q}[s] \simeq \mathbf{Q}[\mathrm{X}]$, ce qui entraîne $\mathbf{Q}(s) = \mathrm{Frac}(\mathbf{Q}[s]) \simeq \mathrm{Frac}(\mathbf{Q}[\mathrm{X}]) = \mathbf{Q}(\mathrm{X})$.

Exercice 3. D'après la propriété universelle, il existe un unique morphisme de $\mathbf{C}$-algèbres $\mathbf{C}[\mathrm{X}, \mathrm{Y}] \to \mathbf{C}[\mathrm{T}]$ envoyant X sur T^2 et Y sur T^3. Puisque ce morphisme envoie $\mathrm{Y}^2 - \mathrm{X}^3$ sur $(\mathrm{T}^3)^2 - (\mathrm{T}^2)^3 = 0$, ce morphisme induit par passage au quotient un morphisme d'anneaux $\varphi : \mathrm{A} = \mathbf{C}[\mathrm{X}, \mathrm{Y}]/(\mathrm{Y}^2 - \mathrm{X}^3) \to \mathbf{C}[\mathrm{T}]$.
Ce morphisme est injectif : soit $f \in \mathbf{C}[\mathrm{X}, \mathrm{Y}]$ tel que $f(\mathrm{T}^2, \mathrm{T}^3) = 0$. Faisons la division euclidienne dans $\mathbf{C}[\mathrm{X}][\mathrm{Y}]$ de f par le polynôme (unitaire) $\mathrm{Y}^2 - \mathrm{X}^3$: il existe $\mathrm{Q}, \mathrm{R} \in \mathbf{C}[\mathrm{X}][\mathrm{Y}]$ tels que $f = \mathrm{Q}(\mathrm{Y}^2 - \mathrm{X}^3) + \mathrm{R}$, avec $\deg_\mathrm{Y} \mathrm{R} \leq 1$. Écrivons $\mathrm{R} = \mathrm{R}_0(\mathrm{X}) + \mathrm{R}_1(\mathrm{X})\mathrm{Y}$ et évaluons en $(\mathrm{T}^2, \mathrm{T}^3)$. Il vient

$$0 = f(\mathrm{T}^2, \mathrm{T}^3) = \mathrm{R}_0(\mathrm{T}^2) + \mathrm{R}_1(\mathrm{T}^2)\mathrm{T}^3.$$

Dans cette écriture, $\mathrm{R}_0(\mathrm{T}^2)$ contient uniquement des monômes de degré pair et $\mathrm{R}_1(\mathrm{T}^2)\mathrm{T}^3$ contient uniquement des monômes de degré impair. Une telle décomposition est donc unique, ce qui entraîne $\mathrm{R}_0 = \mathrm{R}_1 = 0$, et f est divisible par $\mathrm{Y}^2 - \mathrm{X}^3$, ce qui donne l'injectivité de φ.
Le morphisme φ réalise donc un isomorphisme entre $\mathrm{A} = \mathbf{C}[\mathrm{X}, \mathrm{Y}]/(\mathrm{Y}^2 - \mathrm{X}^3)$ et une sous-$\mathbf{C}$-algèbre de $\mathbf{C}[\mathrm{T}]$ (qui est précisément la $\mathbf{C}$-algèbre $\mathbf{C}[\mathrm{T}^2, \mathrm{T}^3]$ engendrée par T^2 et T^3). En particulier, A est un anneau intègre. Le plongement $\varphi : \mathrm{A} \to \mathbf{C}[\mathrm{T}]$ se prolonge en un plongement $\mathrm{Frac}(\mathrm{A}) \to \mathrm{Frac}(\mathbf{C}[\mathrm{T}]) = \mathbf{C}(\mathrm{T})$ dont il est facile de voir que c'est un isomorphisme : son image est en effet un sous-corps de $\mathbf{C}(\mathrm{T})$ contenant à la fois $\mathbf{C}$ et $\mathrm{T} = \mathrm{T}^3/\mathrm{T}^2$.
La clôture intégrale de A est donc isomorphe à la clôture intégrale B de $\mathbf{C}[\mathrm{T}^2, \mathrm{T}^3]$ dans son corps des fractions $\mathbf{C}(\mathrm{T})$. Celle-ci contient T, racine du polynôme unitaire $\mathrm{P}(\mathrm{Z}) = \mathrm{Z}^2 - \mathrm{T}^2$ à coefficients dans $\mathbf{C}[\mathrm{T}^2, \mathrm{T}^3]$. On a donc $\mathrm{B} \supset \mathbf{C}[\mathrm{T}]$.
Or, $\mathbf{C}[\mathrm{T}]$, comme tout anneau factoriel, est intégralement clos. (C'est exactement la même preuve que celle qui a été donnée pour $\mathbf{Z}$ et qui sera redonnée en cours). Les racines dans $\mathbf{C}(\mathrm{T})$ de tout polynôme unitaire à coefficients dans $\mathbf{C}[\mathrm{T}]$, donc *a fortiori* d'un polynôme à coefficients dans $\mathbf{C}[\mathrm{T}^2, \mathrm{T}^3]$, sont donc dans $\mathbf{C}[\mathrm{T}]$.

Cela montre que la clôture intégrale de $\mathbf{C}[\mathrm{T}^2, \mathrm{T}^3]$ est $\mathrm{B} = \mathbf{C}[\mathrm{T}]$, et donc que la clôture intégrale de $\mathbf{C}$ est isomorphe à $\mathbf{C}[\mathrm{T}]$.

Exercice 4.

1. Puisque $\mathrm{K}/\mathbf{Q}$ est de degré 2, K est un $\mathbf{Q}$-plan vectoriel. On peut compléter $1 \in \mathrm{Q} \subset \mathrm{K}$ en une $\mathbf{Q}$-base $(1, \theta)$ de K. En particulier, on a $\mathrm{K} = \mathbf{Q}(\theta)$ (on a évidemment $\mathbf{Q}(\theta) \subset \mathrm{K}$, et comme K est de dimension 2 et que $\mathbf{Q}(\theta)$ contient strictement $\mathbf{Q}$, un argument de dimension conclut.) La famille $(1, \theta, \theta^2)$ est donc liée et il existe $a, b, c \in \mathbf{Q}$ non tous nuls tels que $a\theta^2 + b\theta + c = 0$. En outre, par liberté de $(1, \theta)$, a est nécessairement non nul et, quitte à diviser par lui, on peut supposer $a = 1$. Écrivons le discriminant $b^2 - 4c$ sous la forme $r^2\mathrm{D}$, où r est un entier et D un entier (éventuellement négatif) sans facteur carré. On peut alors écrire θ sous la forme $(-b \pm r\sqrt{\mathrm{D}})/2$. On a donc $\mathrm{K} \subset \mathbf{Q}(\sqrt{\mathrm{D}})$, mais un argument de dimension ($\dim_{\mathbf{Q}} \mathrm{K} = 2, \dim_{\mathbf{Q}} \mathbf{Q}(\sqrt{\mathrm{D}}) \leq 2$) montre que $\mathrm{K} = \mathbf{Q}(\sqrt{\mathrm{D}})$.
2. La famille $(1, \sqrt{\mathrm{D}})$ est une $\mathbf{Q}$-base de K. Tout élément α de K s'écrit donc $r + s\sqrt{\mathrm{D}}$, avec $r, s \in \mathbf{Q}$. En écrivant r et s comme deux fractions que l'on réduit ensuite au même dénominateur, on a donc $\alpha = a/c + b/c\sqrt{\mathrm{D}}$, avec $\mathrm{pgcd}(a, b, c) = 1$.
   Sous cette forme, le polynôme minimal de α s'écrit
   $$m_\alpha(\mathrm{X}) = \left(\mathrm{X} - \left(\frac{a}{c} + \frac{b}{c}\sqrt{\mathrm{D}}\right)\right)\left(\mathrm{X} - \left(\frac{a}{c} - \frac{b}{c}\sqrt{\mathrm{D}}\right)\right) = \mathrm{X}^2 - \frac{2a}{c}\mathrm{X} + \frac{a^2 - \mathrm{D}b^2}{c^2}.$$
   La question 3 du premier exercice, jointe à la remarque que $\mathbf{Z}$ est intégralement clos, montre alors que α est entier sur $\mathbf{Z}$ si et seulement si les coefficients de son polynôme minimal, $2a/c$ et $(a^2 - b^2\mathrm{D})/c^2$, sont entiers.
3. Soit d le pgcd de a et c. Puisque $(a^2 - b^2\mathrm{D})/c^2$ est entier, d^2 divise alors $b^2\mathrm{D}$. Mais comme D est sans facteur carré, cela implique que d divise b^2. Comme on a supposé que a, b et c étaient premiers entre eux dans leur ensemble, on a donc $d = 1$ et a et c sont premiers entre eux. Le fait que $2a/c$ soit entier entraîne donc $c = 1$ ou $c = 2$.
4. Dans la fin de l'exercice, les congruences sont toujours modulo 4. L'anneau $\mathcal{O}_\mathrm{K}$ contient $\sqrt{\mathrm{D}}$, donc $\mathbf{Z}[\sqrt{\mathrm{D}}] \subset \mathcal{O}_\mathrm{K}$. Réciproquement, soit $\alpha \in \mathcal{O}_\mathrm{K}$, et écrivons-le $\alpha = a/b + b/c\sqrt{\mathrm{D}}$ avec $\mathrm{pgcd}(a, b, c) = 1$ et $c > 0$. D'après les questions précédentes, on doit avoir $c = 1$ ou 2 et $(a^2 - b^2\mathrm{D})/c^2$ entier. Or, si $c = 2$, au moins un entier parmi a et b doit être impair. Puisque $(a^2 - b^2\mathrm{D})/4$ est entier, $0 \equiv a^2 - b^2\mathrm{D}$. Mais a ou b doit être impair (donc de carré congru à 1 modulo 4) et D, sans facteur carré, ne peut pas être divisible par 4. On vérifie alors que cela ne peut se produire que si a et b sont tous les deux impairs, auquel cas $a^2 - b^2\mathrm{D} \equiv 1 - \mathrm{D}$. Ainsi, le cas $c = 2$ ne peut se produire que quand a et b sont tous deux impairs et que $\mathrm{D} \equiv 1$. En particulier, si $\mathrm{D} \not\equiv 1$, α s'écrit $a + b\sqrt{\mathrm{D}}$ avec a et b entiers donc $\mathcal{O}_\mathrm{K} = \mathbf{Z}[\sqrt{\mathrm{D}}]$.
5. On a vu plus haut que si $\mathrm{D} \equiv 1$, tout $\alpha \in \mathcal{O}_\mathrm{K}$ s'écrit nécessairement soit sous la forme $a + b\sqrt{\mathrm{D}}$ avec a et b entiers, soit $(a + b\sqrt{\mathrm{D}})/2$ avec a et b tous deux impairs. Comme
   $$a + b\sqrt{\mathrm{D}} = a - b + 2b\frac{1 + \sqrt{\mathrm{D}}}{2} \text{ et } \frac{(2a' + 1) + (2b' + 1)\sqrt{\mathrm{D}}}{2} = a' - b' + (2b' + 1)\frac{1 + \sqrt{\mathrm{D}}}{2},$$
   on a bien dans ce cas $\mathcal{O}_\mathrm{K} \subset \mathbf{Z}\left[\frac{1 + \sqrt{\mathrm{D}}}{2}\right]$.
   Réciproquement, le polynôme minimal de $\frac{1 + \sqrt{\mathrm{D}}}{2}$ est $\mathrm{X}^2 - \mathrm{X} + (1 - \mathrm{D})/4$, ce qui montre que si $\mathrm{D} \equiv 1$, cet élément est entier. On a donc bien $\mathcal{O}_\mathrm{K} = \mathbf{Z}\left[\frac{1 + \sqrt{\mathrm{D}}}{2}\right]$.

Exercice 5.

1. La partition en racines primitives $\mu_n = \bigsqcup_{d|n} \mu_d^*$ (où l'on a noté μ_d^* l'ensemble des racines d-ièmes primitives de l'unité) fournit une factorisation $\mathrm{X}^n - 1 = \prod_{d|n} \Phi_d(\mathrm{X})$ (qui est d'ailleurs la décomposition en facteurs irréductibles dans $\mathbf{Z}[\mathrm{X}]$ de ce polynôme). Si d divise n, on a donc
$$\frac{\mathrm{X}^n - 1}{\mathrm{X}^d - 1} = \prod_{\substack{d'|n \\ d' \nmid d}} \Phi_{d'}(\mathrm{X}),$$
ce qui entraîne le résultat.

2. Par définition, $\Phi_n(\mathrm{X}) = \prod_{\zeta \in \mu_n^*} (\mathrm{X} - \zeta)$. Si $\zeta \in \mu_n^*$, on a $|\zeta| = 1$ et donc $\forall r \geq 1, |r - \zeta| \geq r - 1$. En outre, l'égalité est stricte dès que $\zeta \neq 1$. Ainsi, si $r \geq 2$ et $n \geq 2$, on a $\Phi_n(r) > (r-1)^{\varphi(n)} \geq r - 1$.

3. Soit n un entier impair. On va montrer que $\zeta \mapsto -\zeta$ met en bijection μ_{2n}^* et μ_n^*.
En effet, si ζ est une racine primitive $2n$-ième de l'unité, ζ^n est un élément d'ordre 2 dans $\mathbf{C}^\times$, donc $\zeta^n = -1$. On a donc $(-\zeta^k) = (-1)^k \zeta^k = 1$ si et seulement si k est pair et $\zeta^k = 1$ ou k est impair et $\zeta^k = -1$, c'est-à-dire si et seulement si k est un multiple de n. La racine $-\zeta$ est donc bien d'ordre n.
Réciproquement, si ζ est d'ordre n, on a $(-\zeta)^k = 1$ si et seulement si k est pair et multiple de n (car on n'a $\zeta^k = -1$ pour aucun k) et $-\zeta$ est d'ordre $2n$. L'involution $\zeta \mapsto -\zeta$ réalise donc une bijection entre μ_{2n}^* et μ_n^*. Le polynôme cyclotomique $\Phi_{2n}(\mathrm{X})$ est donc le polynôme unitaire dont les racines, simples, sont les $-\zeta$ pour ζ parcourant μ_n^*, c'est-à-dire $\Phi_n(-\mathrm{X})$ (qui est unitaire car $\varphi(n)$ est pair).
Supposons maintenant n pair. Le même genre de calcul montre que si ζ est une racine primitive $2n$-ième, $-\zeta$ est aussi une racine primitive $2n$-ième et leur carré commun ζ^2 est une racine primitive n-ième. Cela démontre que l'application $\zeta \mapsto \zeta^2$ envoie surjectivement μ_{2n}^* sur μ_n^* et que l'image réciproque de toute racine primitive n-ième contient exactement 2 racines primitives $2n$-ièmes.
Les racines de $\Phi_n(\mathrm{X}^2)$ sont donc exactement les $\varphi(2n) = 2\varphi(n)$ racines primitives de l'unité, ce qui montre (les deux polynômes étant clairement unitaires), que $\Phi_{2n}(\mathrm{X}) = \Phi_n(\mathrm{X}^2)$.

Exercice 6.

1. D'après les relations coefficients-racines, le terme constant de Φ_n est, au signe près, le produit des racines primitives n-ièmes de l'unité. C'est donc lui-même une racine de l'unité. Comme $\Phi_n \in \mathbf{Z}[\mathrm{X}]$, on a $\Phi_n(0) = \pm 1$.

2. Puisque p ne divise pas n, le polynôme $\mathrm{X}^n - 1 \in \mathbf{F}_p[\mathrm{X}]$ est séparable. Supposons que p divise $\Phi_n(a)$. Comme Φ_n est un diviseur de $\mathrm{X}^n - 1$, cela entraîne $p | a^n - 1$ et a est donc un inversible modulo p, d'ordre d divisant n. Si on avait $d < n$, on aurait $\overline{\Phi_d(a)} = 0$ (la barre représentant la réduction modulo p). Dans $\mathbf{F}_p$, la classe de a annulerait donc à la fois Φ_d et Φ_n, ce qui contredit la séparabilité de $\mathrm{X}^n - 1$ dans $\mathbf{F}_p[\mathrm{X}]$. La classe de a modulo p est donc d'ordre exactement n.
Réciproquement, supposons que a est d'ordre n modulo p. Dans $\mathbf{F}_p[\mathrm{X}]$, a annule donc le polynôme $\mathrm{X}^n - 1$ et donc l'un des polynômes cyclotomiques $\Phi_d(\mathrm{X})$ pour d divisant n. Mais puisqu'il n'annule aucun des $\mathrm{X}^d - 1$ pour d diviseur strict de n, il ne peut annuler aucun des Φ_d correspondant. On a donc bien $\overline{\Phi_n(a)} = 0$, soit p divise $\Phi_n(a)$.

3. Le groupe $\mathbf{F}_p^\times$, cyclique d'ordre $p-1$, contient un élément d'ordre n si et seulement si n divise $p-1$, c'est-à-dire si p est congru à 1 modulo n. D'après la question précédente, $p \equiv 1 \pmod{n}$ si et seulement s'il existe un entier relatif a tel que p divise $\Phi_d(a)$.
4. Supposons que l'ensemble des nombres premiers congrus à 1 modulo n soit fini, disons $\{p_1, \ldots, p_k\}$. Comme $\Phi_n(\mathrm{X})$ a pour terme dominant $\mathrm{X}^{\varphi(n)}$, on peut trouver un entier M suffisamment grand pour que $\Phi_n(\mathrm{M} \cdot p_1 \cdots p_k)$ soit strictement supérieur à 1. Il admet donc un diviseur premier p. D'après la question précédente, on a $p \equiv 1 \pmod{n}$. Mais puisque le terme constant de Φ_n est ± 1, on a forcément

$$\forall i \in \{1, \ldots, k\}, \Phi_n(\mathrm{M} \cdot p_1 \cdots p_k) \equiv \pm 1 \pmod{p_i},$$

donc $p \notin \{p_1, \ldots, p_k\}$, ce qui constitue une contradiction. L'ensemble des nombres premiers congrus à 1 modulo n est donc infini.

Remarque. Le théorème de la progression arithmétique de Dirichlet (1837) affirme que si a et n sont premiers entre eux, il existe une infinité de nombres premiers congrus à a modulo n.

Exercice 7.

1. Puisque f est un morphisme d'anneaux, $\Phi_n(f(\zeta_n)) = f(\Phi_n(\zeta_n)) = 0$, et $f(\zeta_n)$ est encore une racine primitive n-ième de l'unité. Le morphisme f, injectif car $\mathbf{Q}(\zeta_n)$ est un corps, réalise donc une bijection $\mu_n^* \to \mu_n^*$. En particulier, $\operatorname{im} f = \mathbf{Q}(\zeta_n)$.
   Le polynôme minimal de ζ_n est précisément Φ_n. Le corps $\mathbf{Q}(\zeta_n)$ est donc isomorphe au quotient $\mathbf{Q}[\mathrm{X}]/(\Phi_n(\mathrm{X}))$. Un morphisme $f : \mathbf{Q}(\zeta_n) \to \mathbf{C}$ est donc complètement caractérisé par l'image $\zeta' = f(\zeta_n)$, qui peut être une racine quelconque de $\Phi_n(\mathrm{X})$, c'est-à-dire une racine primitive n-ième de l'unité quelconque.
2. Les racines primitives n-ièmes de l'unité sont exactement les ζ_n^r, pour r premier avec n, et $\zeta_n^r = \zeta_n^{r'}$ si et seulement si r et r' sont congrus modulo n. Cette remarque et la question précédente montrent donc l'existence d'une bijection $(\mathbf{Z}/n\mathbf{Z})^* \to \mathrm{Aut}(\mathbf{Q}(\zeta_n))$ telle que l'image de $\overline{r}$ est l'unique plongement $\mathbf{Q}(\zeta_n) \to \mathbf{C}$ donné par $\zeta_n \mapsto \zeta_n^r$ (on a vu qu'un tel plongement est nécessairement un automorphisme de $\mathbf{Q}(\zeta_n)$). Il reste à voir que cette bijection est bien un morphisme de groupes. Il est évident qu'elle envoie $\overline{1}$ sur l'identité. Maintenant, si $f, g \in \mathrm{Aut}(\mathbf{Q}(\zeta_n))$ envoient ζ_n sur ζ_n^r et ζ_n^s, respectivement, on a bien $g \circ f(\zeta_n) = g(\zeta_n^r) = g(\zeta_n)^r = (\zeta_n^s)^r = \zeta_n^{rs}$.
   En particulier, si $n = p$ est premier, $(\mathbf{Z}/n\mathbf{Z})^\times = \mathbf{F}_p^\times$ est cyclique.

Exercice 8.

1. Soit $x \in \mathrm{A}$, non nul. L'application $a \mapsto ax : \mathrm{A} \to \mathrm{A}$ est un morphisme d'anneaux injectif car A est intègre et donc surjectif (car A est fini). Chaque élément admet donc un inverse à gauche, à savoir l'antécédent de 1 par cette application. On montre de même l'existence d'un inverse à droite. Nécessairement ces deux inverses sont les mêmes. Il va donc uniquement s'agir de démontrer que A est commutatif.
2. K est évidemment stable par addition et multiplication et inverse, et contient 0 et 1. Puisqu'il est commutatif, c'est bien un corps. L'anneau A est alors un K-espace vectoriel et il est donc de cardinal q^n, où $n = \dim_{\mathrm{K}} \mathrm{A}$.
3. $\begin{array}{ccc} \mathrm{A}^\times = \mathrm{A} \setminus \{0\} \times \mathrm{A} & \to & \mathrm{A} \\ (u, x) & \mapsto & uxu^{-1} \end{array}$ définit bien une action de $\mathrm{A}^\times$ sur A. L'orbite de 0 est le singleton $\{0\}$ donc l'action se restreint en une action de $\mathrm{A}^\times$ sur lui-même. Si $x \in \mathrm{A}^\times$, $\mathrm{Stab}(x) \cup \{0\} = \left\{ a \in \mathrm{A} \,\middle|\, ax = xa \right\}$ est évidemment stable par addition, multiplication

et contient le centre. Il est donc en particulier stable par multiplication par un élément de K. En résumé, c'est un K-espace vectoriel.

4. D'après la question précédente, le stabilisateur d'un point x a un cardinal de la forme $q^d - 1$, pour $d \leq n$. D'après la formule des classes, $q^d - 1$ divise $q^n - 1$, et leur quotient est précisément le cardinal de l'orbite de x. Il reste donc à voir que le fait que $q^d - 1$ divise $q^n - 1$ entraîne $d|n$.

   Écrivons la division euclidienne de n par d : $n = da + r$. On a alors $q^n - 1 = q^r(q^{da} - 1) + q^r - 1$. Puisque $q^d - 1$ divise $q^n - 1$ et qu'il divise $q^{da} - 1 = (q^d - 1)(1 + q^d + \cdots + q^{d(a-1)})$, cela entraîne que $q^d - 1$ divise $q^r - 1$. Mais $r < d$, donc la seule possibilité est que $r = 0$. On a donc bien montré que d divise n.

5. C'est une conséquence immédiate de la première question de l'exercice 5.

6. La partition de $\mathrm{A}^\times$ en orbites fait intervenir $(q-1)$ points fixes (les éléments de $\mathrm{K} \setminus \{0\}$) et des orbites plus grosses de cardinal de la forme ci-dessus. On a donc une décomposition de la forme

$$q^n - 1 = (q-1) + \sum_i \frac{q^n - 1}{q^{d_i} - 1},$$

   où les d_i sont des diviseurs stricts de n. Attendu que $\Phi_n(q)$ divise le terme de gauche et tous les termes de la somme, il doit également diviser $q-1$. En particulier, $|\Phi_n(q)| \leq q-1$.

7. D'après la deuxième question de l'exercice 5, l'inégalité ci-dessus force $n = 1$. L'anneau A est donc confondu avec son centre K, ce qui le rend commutatif.