Polynômes cyclotomiques, intégralité

Exercice 1. (Polynôme minimal et intégralité)
Soit A un anneau intègre et K = Frac(A) son corps de fractions. Si L/K est une extension finie, on note $\mathrm{A_L}$ la clôture intégrale de A dans L. Si $s \in \mathrm{L}$, on note $m_{s,\mathrm{K}}(\mathrm{X}) \in \mathrm{K[X]}$ un polynôme unitaire de degré minimal strictement positif ayant s comme racine.

1. Montrer que $m_{s,\mathrm{K}}$ est irréductible dans K[X]. Montrer que si $\mathrm{P} \in \mathrm{K[X]}$ et $\mathrm{P}(s) = 0$, alors $m_{s,\mathrm{K}}$ divise P dans K[X]. Montrer que si P est irréductible et unitaire et que P a une racine $s \in \mathrm{L}$, alors $\mathrm{P} = m_{s,\mathrm{K}}$.
2. Montrer que $\deg m_{s,\mathrm{K}} \leq [\mathrm{L} : \mathrm{K}]$.
3. Montrer que $s \in \mathrm{L}$ est entier sur A si et seulement si $m_{s,\mathrm{K}}$ est à coefficients dans $\mathrm{A_K}$. En déduire que si A est intégralement clos dans K, alors s est entier sur A si et seulement si $m_{s,\mathrm{K}} \in \mathrm{A[X]}$.
4. Supposons maintenant que A est intégralement clos. Montrer que si $f \in \mathrm{A[X]}$ est unitaire, alors les facteurs irréductibles de f dans K[X] sont tous à coefficients dans A.

Exercice 2. (Sous-corps engendré par une partie)
Soit $\mathrm{S} \subset \mathbf{C}$ un sous-ensemble. On note $\mathbf{Q}(\mathrm{S})$ l'intersection des sous-corps $\mathrm{K} \subset \mathbf{C}$ contenant S.

1. Montrer que $\mathbf{Q}(\mathrm{S})$ est un sous-corps de $\mathbf{C}$.
2. Montrer que $\mathbf{Q}(\mathrm{S})$ est égal à $\mathrm{Frac}(\mathbf{Q}[\mathrm{S}])$, où $\mathbf{Q}[\mathrm{S}]$ est la sous-$\mathbf{Q}$-algèbre de $\mathbf{C}$ engendrée par S.
3. Montrer que si $s \in \mathbf{C}$ est algébrique sur $\mathbf{Q}$, alors $\mathbf{Q}(s) = \mathbf{Q}[s]$. Donner une base de $\mathbf{Q}(s)$ sur $\mathbf{Q}$.
4. Montrer que si $s \in \mathbf{C}$ est transcendant sur $\mathbf{Q}$, alors $\mathbf{Q}(s)$ est isomorphe à $\mathbf{Q}(\mathrm{X})$.

Exercice 3. Montrer que l'anneau $\mathbf{C}[\mathrm{X}, \mathrm{Y}]/(\mathrm{Y}^2 - \mathrm{X}^3)$ est intègre. Montrer que sa clôture intégrale de A est isomorphe à $\mathbf{C}[\mathrm{T}]$.

Exercice 4. (Anneaux d'entiers des extensions quadratiques)
Soit $\mathrm{K}/\mathbf{Q}$ une extension de degré 2. On note $\mathcal{O}_\mathrm{K}$ l'anneau des entiers de K (c'est-à-dire l'anneau constitué des élements de K entiers sur $\mathbf{Q}$).

1. Montrer qu'il existe un entier $\mathrm{D} \in \mathbf{Z}$ sans facteur carré tel que $\mathrm{K} = \mathbf{Q}(\sqrt{\mathrm{D}})$.
2. Montrer que tout élément de K s'écrit sous la forme $\alpha = \frac{a}{c} + \frac{b}{c}\sqrt{\mathrm{D}}$ avec $a, b, c \in \mathbf{Z}$ et $\mathrm{pgcd}(a, b, c) = 1$. Montrer que α est entier sur $\mathbf{Z}$ si et seulement si $\frac{a^2 - b^2\mathrm{D}}{c^2}$ et $\frac{2a}{c}$ sont dans $\mathbf{Z}$.
3. Montrer que si $\alpha \in \mathcal{O}_\mathrm{K}$, alors $c = 1$ ou $c = 2$.
4. Montrer que $\mathcal{O}_\mathrm{K} = \mathbf{Z}[\sqrt{\mathrm{D}}]$ si $\mathrm{D} \not\equiv 1 \pmod 4$.
5. Montrer que $\mathcal{O}_\mathrm{K} = \mathbf{Z}\left[\frac{1+\sqrt{\mathrm{D}}}{2}\right]$ si $\mathrm{D} \equiv 1 \pmod 4$.

Exercice 5. Soit $n \in \mathbf{N}^*$.

1. Montrer que si $d < n$ divise n, alors $\Phi_n(\mathrm{X})$ divise $\dfrac{\mathrm{X}^n - 1}{\mathrm{X}^d - 1}$ dans $\mathbf{Z}[\mathrm{X}]$.

2. Montrer que si $n > 1$ et $r \in [2, +\infty[$, alors $\Phi_n(r) > r - 1$.
3. Montrer que si n est impair, alors $\Phi_{2n}(\mathrm{X}) = \Phi_n(-\mathrm{X})$. Montrer que si n est pair, alors $\Phi_{2n}(\mathrm{X}) = \Phi_n(\mathrm{X}^2)$.

Exercice 6. (Un cas particulier du théorème de la progression arithmétique)
Soit n un entier supérieur ou égal à 1 et p un nombre premier ne divisant pas n.

1. Montrer que le coefficient constant de $\Phi_n(\mathrm{X})$ vaut 1 ou -1.
2. Soit a un entier relatif ; montrer que p divise $\Phi_n(a)$ si et seulement si la classe de a modulo p est d'ordre n dans $\mathbf{F}_p^\times$.
3. Montrer que p est congru à 1 modulo n si et seulement s'il existe un entier relatif a tel que p divise $\Phi_n(a)$.
4. En déduire qu'il existe une infinité de nombres premiers de la forme $kn+1$ avec k entier.

Exercice 7. (Plongements de $\mathbf{Q}(\zeta_n)$ dans $\mathbf{C}$) Soit $n \geq 1$ et soit ζ_n une racine n-ième primitive de l'unité dans $\mathbf{C}$.

1. Montrer que si $f : \mathbf{Q}(\zeta_n) \to \mathbf{C}$ est un morphisme d'anneaux, alors $f(\zeta_n)$ est une racine n-ième primitive de l'unité et que $\mathrm{im}(f) = \mathbf{Q}(\zeta_n)$. Montrer réciproquement, que si ζ' est un racine n-ième primitive de l'unité, alors $\zeta_n \mapsto \zeta'$ s'étend en un morphisme $\mathbf{Q}(\zeta_n) \to \mathbf{C}$, qui est forcement injectif.
2. Montrer, plus précisement, que $\overline{r} \mapsto (\zeta_n \mapsto \zeta_n^r)$ définit un isomorphisme de groupes $(\mathbf{Z}/n\mathbf{Z})^* \to \mathrm{Aut}(\mathbf{Q}(\zeta_n))$. En déduire que $\mathrm{Aut}(\mathbf{Q}(\zeta_n))$ est cyclique si n est premier.

Exercice 8. (Théorème de Wedderburn)
Le but de cet exercice est de montrer que tout anneau intègre fini A est un corps commutatif.

1. Montrer que tout élément non nul $x \in \mathrm{A}$ est inversible.
2. Soit $\mathrm{K} = \mathrm{Z}(\mathrm{A}) = \{x \in \mathrm{A} | ax = xa, \forall a \in \mathrm{A}\}$. Montrer que c'est un sous-corps fini de A. On note q le cardinal de K. Monter que $|\mathrm{A}| = q^n$ pour un entier $n \geq 1$ (on va montrer que $n = 1$).
3. Montrer que $\mathrm{A}^\times = \mathrm{A}\backslash\{0\}$ agit sur lui-même par automorphismes intérieurs. Montrer que si $x \in \mathrm{A}^\times$, alors $\mathrm{Stab}_x \cup \{0\}$ est un sous-K-espace vectoriel de A.
4. Montrer que les orbites de l'action précédemment décrite sont de cardinal de la forme $\frac{q^n-1}{q^d-1}$ avec $d|n$.
5. Montrer que pour tout $d|n$ avec $d \neq n$, $\Phi_n(q)|\frac{q^n-1}{q^d-1}$.
6. En déduire que $|\Phi_n(q)| \leq q - 1$.
7. En déduire que A est un corps.