Feuille d'exercices n°15 : Anneaux $\mathbb{Z}/n\mathbb{Z}$, racines de l'unité et cyclotomie

Dans toute cette feuille A est un anneau commutatif, K est un corps et $n \in \mathbb{N}^*$.

À faire

Exercice 1. ***(Propriétés de l'indicatrice d'Euler)***

1. Démontrer les propriétés suivantes sur l'indicatrice d'Euler :
   (a) Si $p \in \mathcal{P}$ et $\alpha \in \mathbb{N}^*$, alors $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.
   (b) Si $a \wedge b = 1$, alors $\varphi(ab) = \varphi(a)\varphi(b)$.
   (c) On a $\varphi(n) = n \prod_{\substack{p \in \mathcal{P} \\ p|n}} \left(1 - \frac{1}{p}\right)$.
   (d) On a $n = \sum_{d|n} \varphi(d)$.
2. En déduire les théorèmes suivants :
   (a) (Théorème d'Euler) Pour tout $a \wedge n = 1$, on a $a^{\varphi(n)} \equiv 1 \mod n$.
   (b) (Théorème de Fermat) Pour tout $p \in \mathcal{P}$ et tout $a \wedge p = 1$, on a $a^{p-1} \equiv 1 \mod p$.
   (c) (Théorème de Wilson) Pour $a \in \mathbb{N}^*$, on a $(a-1)! \equiv -1 \mod a \iff a$ est premier.
   (d) (Théorème RSA) Soient $p, q \in \mathcal{P}$ tels que $p \neq q$ et $n = pq$. Alors pour tous $d, e \in \mathbb{Z}$, on a $de \equiv 1 \mod \varphi(n) \implies \forall m \in \mathbb{Z},\ m^{de} = m \mod n$.

Exercice 2. ***(Valeurs prises par les polynômes cyclotomiques)***

1. Montrer que pour tout $k \in \mathbb{Z}$ et $d, n \in \mathbb{N}^*$, si $d|n$ et $d < n$, alors $\Phi_n(k) | \frac{k^n-1}{k^d-1}$ dans $\mathbb{Z}$.
2. Montrer que pour tout $x \in \mathbb{R}$, si $x \geq 1$ et $n \geq 2$, alors $|\Phi_n(x)| > (x-1)^{\varphi(n)}$.
3. Montrer que pour tout $x \in \mathbb{R}$, si $x \geq 2$ et $n \geq 2$, alors $|\Phi_n(x)| > x - 1$.

Exercice 3. ***(Groupe de Galois d'une extension cyclotomique)***

1. Montrer que le corps de rupture de Φ_n sur $\mathbb{Q}$ est un corps de décomposition de ce polynôme.
2. Montrer que $\mathrm{Aut}_{\mathbb{Q}}\left(\mathbb{Q}[X]/\left(\Phi_n\right)\right)$ est isomorphe à $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$.
   Indication : regarder l'image d'une racine primitive n-ième de l'unité par un tel automorphisme.

Exercice 4. ***(Règles de calcul des polynômes cyclotomiques)***
Soit $n \in \mathbb{N}^*$ et p un nombre premier.

1. Calculer Φ_1 et Φ_p.
2. Montrer que si $p|n$, alors $\Phi_{pn} = \Phi_n(X^p)$.
   Indication : comparer $\mu_n^*(\mathbb{C})$ et $\mu_{pn}^*(\mathbb{C})$.
3. Montrer que $\Phi_2 = -\Phi_1(-X)$ et que si $n \geq 3$ est impair, alors $\Phi_{2n} = \Phi_n(-X)$.
4. Montrer que si $p \neq 2$ et $p \nmid n$, alors $\Phi_n \Phi_{pn} = \Phi_n(X^p)$.
5. **Application :** Calculer Φ_{2592}.

Exercice 5. ***(Des cosinus rationnels)***
Trouver tous les couples d'entiers relatifs (a, b) premiers entre eux, tels que $\cos\left(2\pi\frac{a}{b}\right) \in \mathbb{Q}$.
Indication : on pourra comparer les polynômes $X^2 - 2\cos\left(2\pi\frac{a}{b}\right)X + 1$ et Φ_b.

Exercice 6. ***(Un cas particulier du théorème de progression arithmétique de Dirichlet)***
On suppose que $p = \mathrm{car}(K)$ ne divise pas n.

1. Montrer que $\Phi_n(0) \in \{\pm 1\}$.
2. Soit $a \in \mathbb{Z}$. Montrer que $p|\Phi_n(a) \iff a \mod p$ est d'ordre n dans $\mathbb{F}_p^\times$.
3. Montrer que $p \equiv 1 \mod n$ si, et seulement si, il existe un entier $a \in \mathbb{Z}$ tel que p divise $\Phi_n(a)$.
4. En déduire qu'il existe une infinité de nombres premiers p tels que $p \equiv 1 \mod n$.

Exercice 7. ***(Réductibilité du huitième polynôme cyclotomique sur les corps finis)***

1. Calculer $\Phi_8 \in \mathbb{Z}[X]$ et écrire la décomposition de Φ_8 en produit d'irréductibles dans $\mathbb{F}_2[X]$.
2. Soit $p \neq 2$ un nombre premier.
   (a) Donner toutes les manières d'écrire Φ_8 comme produit de deux polynômes dans $\mathbb{C}[X]$.
   (b) Montrer que l'un des éléments $-1, 2, -2$ est un carré dans $\mathbb{F}_p$.
   (c) En déduire que Φ_8 est réductible dans $\mathbb{F}_p[X]$.
3. Soit $p \neq 2$ un nombre premier.
   (a) Montrer que Φ_8 est réductible si, et seulement si, Φ_8 admet une racine dans $\mathbb{F}_{p^2}$.
   (b) Montrer que Φ_8 admet une racine dans $\mathbb{F}_{p^2}$ si, et seulement si, 8 divise $p^2 - 1$.
   (c) En déduire que Φ_8 est réductible dans $\mathbb{F}_p[X]$.

Problèmes

Exercice 8. ***(Théorème de Wedderburn)***
Soit A un anneau intègre unitaire fini (non nécessairement commutatif) et $Z = \{x \in A,\ xy = yx \forall y \in A\}$ appelé le *centre* de A.

1. Montrer que $A \setminus \{0\} = A^*$ est un groupe pour $\cdot$.
2. Montrer que Z est un corps fini. On note q son cardinal.
3. Montrer que A est de cardinal q^n pour un certain $n \in \mathbb{N}^*$.

On considère l'action de A^* sur lui-même par conjugaison et on note $C(x)$ l'orbite de $x \in A^*$.

4. Montrer que $C(x) = \{x\}$ si, et seulement si, $x \in Z$.
5. Montrer que si $x \in A \setminus Z$, alors $C(x)$ est de cardinal $\frac{q^n-1}{q^d-1}$ avec $d|n$ et $0 < d < n$.
6. Montrer que $\Phi_n(q)|q - 1$.
7. En déduire que $A = Z$ est un corps.

Exercice 9. ***(Structure des*** $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ ***)***
Soit p un nombre premier dans $\mathbb{Z}$ et $\alpha \in \mathbb{N}^*$.

1. On suppose que p est impair.
   (a) Montrer que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.
   (b) Montrer que pour tout $\beta \in \mathbb{N}^*$, il existe $m \in \mathbb{Z}$ tel que $m \wedge p = 1$ et $(1+p)^{p^\beta} = 1 + mp^{\beta+1}$.
   (c) En l'ordre de $\overline{p+1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.
   (d) Montrer que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ contient un élément d'ordre $p - 1$.
   Indication : On pourra considérer un antécédent d'un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ *par la surjection canonique* $\psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$.
   (e) En déduire que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.
2. On suppose désormais $p = 2$. Décrire $(\mathbb{Z}/2\mathbb{Z})^\times$ et $(\mathbb{Z}/4\mathbb{Z})^\times$.
3. On suppose $\alpha \geq 3$. Soit $\psi : (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ et $U(\alpha)$ le noyau de ψ.
   (a) Montrer que pour tout $\beta \in \mathbb{N}^*$, il existe $m \in \mathbb{Z}$ impair tel que $5^{2^\beta} = 1 + m2^{\beta+1}$.
   (b) En déduire $U(\alpha)$ est un groupe cyclique d'ordre $2^{\alpha-2}$ engendré par $\overline{5}$.
   (c) Justifier l'isomorphisme de groupes $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/4\mathbb{Z})^\times \times U(\alpha)$.