Examen du 27 février 2018

2 heures

La correction tiendra grandement compte de la clarté et de la concision de la rédaction.
L'utilisation de calculatrice, de téléphone portable et autre gadget est interdite.

Exercice 1. — Les questions de cet exercice sont indépendantes les unes des autres.

a) Soit $n \geqslant 1$ un entier. Montrer que $\mathbf{Z}/n\mathbf{Z}$ est un corps ssi n est premier.

b) Soient m et n deux entiers premiers entre eux. Pour $a \in \mathbf{Z}$, montrer que a est un carré modulo mn ssi a est un carré modulo m et a est un carré modulo n.

c) Dans l'anneau principal $\mathbf{Z}[\imath]$, trouver un générateur de l'idéal $I = (2, 5 + \imath)$.
Montrer que l'anneau quotient $\mathbf{Z}[\imath]/I$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.

d) Quels sont les éléments irréductibles de $\mathbf{R}[X]$? Justifier votre réponse.

e) Soit P le polynôme $3X^5 + 45X^3 + 15 \in \mathbf{Z}[X]$.
P est-il un élément irréductible de $\mathbf{Z}[X]$? de $\mathbf{Q}[X]$?

f) Soit $\mathcal{E}$ un espace affine. Pour A, B des points de $\mathcal{E}$, soit s_A (resp. s_B) la symétrie centrale de centre A (resp. B). Montrer que $s_A \circ s_B$ est une translation dont on précisera le vecteur.

g) Soit $(\mathcal{E}, E)$ un espace affine et $(\mathcal{F}, F)$ et $(\mathcal{G}, G)$ deux sous-espaces affines non vides de $(\mathcal{E}, E)$.

i) Montrer que $\mathcal{F} \cap \mathcal{G} \neq \emptyset$ ssi pour tous points $M \in \mathcal{F}$ et $N \in \mathcal{G}$, on a $\overrightarrow{MN} \in F + G$.

ii) Montrer que si F et G sont supplémentaires alors $\mathcal{F} \cap \mathcal{G}$ est réduit à un point.

* *
*

Exercice 2. — Soit $q = p^n$ une puissance d'un nombre premier et $\mathbf{F}_q$ un corps à q éléments. Pour tout $\alpha \in \mathbf{F}_q$, on pose $\mathrm{Tr}(\alpha) = \sum_{i=0}^{n-1} \alpha^{p^i}$.

a) Montrer que Tr est une application linéaire à valeur dans le sous-corps $\mathbf{F}_p \subset \mathbf{F}_q$.

b) Montrer qu'il existe $\alpha \in \mathbf{F}_q$ tel que $\mathrm{Tr}(\alpha) \neq 0$.

c) Pour $\alpha \in \mathbf{F}_q$, montrer qu'on a $\mathrm{Tr}(\alpha) = 0$ ss'il existe $\beta \in \mathbf{F}_q$, tel que $\alpha = \beta^p - \beta$.
[**Indication:** Noter que $\mathbf{F}_q \to \mathbf{F}_q$, $\beta \mapsto \beta^p - \beta$ est linéaire. Quelle est la dimension de son image ?]

* *
*

Exercice 3. — Pour $n \geqslant 1$ un entier, on note $\Phi_n = \sum_{k=0}^{\varphi(n)} a_k X^k$ le n-ème polynôme cyclotomique.

a) Montrer que pour $n \geqslant 2$, les coefficients a_k de Φ_n vérifient $a_{\varphi(n)-k} = a_k$.
[**Indication:** Comparer $\Phi_n(X)$ et $\Phi_n(\frac{1}{X})$. Attention au cas $n = 1$.]

b) Quel est le degré de l'extension $\mathbf{Q} \subset \mathbf{Q}[e^{\frac{2i\pi}{n}}]$?

c) Pour $n > 2$, montrer que le degré de l'extension $\mathbf{Q}[\cos(\frac{2\pi}{n})] \subset \mathbf{Q}[e^{\frac{2i\pi}{n}}]$ vaut 2.
[**Indication:** Noter que pour $n > 2$, $e^{\frac{2i\pi}{n}} \notin \mathbf{R}$.]

d) En déduire le degré de l'extension $\mathbf{Q} \subset \mathbf{Q}[\cos(\frac{2\pi}{n})$ lorsque $n > 2$.
En utilisant **a)**, déterminer en fonction de Φ_n le polynôme minimal de $2\cos(\frac{2\pi}{n})$.

e) En notant que le polynôme minimal de $2\cos(\frac{2\pi}{n})$ est unitaire et dans $\mathbf{Z}[X]$, montrer que les seules valeurs entières de n telles que $\cos(\frac{2\pi}{n})$ soit rationnel sont $n = 1, 2, 3, 4$ et 6.