Examen du 29 janvier 2019

1 heure 30

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 entre elles.

1) Soient A un anneau et $I \subsetneq A$ un idéal strict.
Montrer que I est maximal ssi l'anneau A/I est un corps.

2) On note $N : \mathbf{Z}[i] \to \mathbf{N}$ l'application $a + ib \mapsto a^2 + b^2$.

i) Soient $\alpha, \beta \in \mathbf{Z}[i]$ deux éléments tels que les entiers $N(\alpha)$ et $N(\beta)$ soient premiers entre eux. Montrer que α et β sont premiers entre eux (dans $\mathbf{Z}[i]$).

ii) Réciproquement, si α et β sont premiers entre eux, a-t-on nécessairement $N(\alpha)$ et $N(\beta)$ premiers entre eux ?

3) On rappelle la loi de réciprocité quadratique : pour p, q des nombres premiers impairs

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right) \qquad \text{et} \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

i) 22 est-il un carré dans $\mathbf{Z}/43\mathbf{Z}$?

ii) 17 est-il un carré dans $\mathbf{Z}/33\mathbf{Z}$?

* *
*

Exercice 2. — Soit p un nombre premier fixé. On note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$. Le but de cet exercice est d'étudier certains quotients d'anneaux de polynômes à coefficients dans $\mathbf{F}_p$. On note $A := \mathbf{F}_p[X]$. Pour tout $Q \in A$ *non nul*, on note (Q) l'idéal de A engendré par Q et $|Q| := p^{\deg(Q)}$.

1) Montrer que l'anneau quotient $A/(Q)$ est fini de cardinal $|Q|$.

2) Pour $Q \in$ de degré $\geqslant 1$, montrer que les assertions suivantes sont équivalentes :

i) $A/(Q)$ est un corps

ii) Q est irréductible dans A

Dans toute la suite, on note $\Phi(Q)$ le cardinal du groupe des éléments inversibles $(A/(Q))^\times$.

3) Si Q est irréductible et $\alpha \geqslant 1$, montrer que l'on a

$$\Phi(Q^\alpha) = |Q^{\alpha-1}|(|Q| - 1).$$

4) Montrer que si Q_1 et Q_2 sont premiers entre eux, alors on a

$$\Phi(Q_1 \cdot Q_2) = \Phi(Q_1) \cdot \Phi(Q_2).$$

5) Quelle formule en déduit-on pour $\Phi(Q)$ dans le cas général ?

Dans la suite, on suppose Q irréductible et $\alpha \geqslant 1$. On étudie la structure du groupe des inversibles $(A/(Q^\alpha))^\times$.

6) Montrer que si $\alpha = 1$ alors le groupe $(A/(Q))^\times$ est cyclique.
[**Indication:** Imiter la preuve que $\mathbf{F}_p^*$ est cyclique].

7) Déduire de **6)** le nombre de cubes dans $(A/(Q))^\times$.

8) Pour $\alpha > 1$, construire un morphisme de groupes *surjectif*

$$\rho : (A/(Q^\alpha))^\times \to (A/(Q))^\times.$$

En déduire l'existence d'un élément d'ordre $|Q| - 1$ dans $(A/(Q^\alpha))^\times$.

9) Soit Γ le noyau de ρ. Montrer qu'on a un isomorphisme de groupes

$$(A/(Q^\alpha))^\times \cong \Gamma \times \mathbf{Z}/(|Q| - 1)\mathbf{Z}.$$

10) Soit f est le plus petit entier tel que $p^f \geqslant \alpha$, montrer que tous les éléments de Γ sont d'ordre $\leqslant p^f$.

11) Montrer que le groupe $(A/(Q^\alpha))^\times$ est cyclique ssi ($\alpha = 1$) ou ($\alpha = 2$ et $\deg(Q) = 1$) ou ($\alpha = 3$, $d = 1$ lorsque $p = 2$).