Examen du 1er février 2021

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. — Soit p un nombre premier. On suppose $p \not\equiv 1[5]$.

1) Montrer que le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique.
[**Indication:** Soit $d_1|\dots|d_r$ ses facteurs invariants. Considérer les racines du polynôme $X^{d_r}-1 \in \mathbf{Z}/p[X]$.]

Dans la suite, on note $n := p-1$, $E := \{(a,b,c) \in (\mathbf{Z}/p\mathbf{Z})^3,\ a^{10}b^{15}c^{35} = 1\}$ et $F := \{(\alpha,\beta,\gamma) \in (\mathbf{Z}/n\mathbf{Z})^3,\ 2\alpha+3\beta+7\gamma = 0\}$.

2) Montrer que F est de cardinal n^2.
[**Indication:** On pourra introduire la variable $\delta := \alpha+\beta$.]

3) En déduire le cardinal de E.

* *
*

Exercice 2. — Soit k un corps de caractéristique différente de 2 et $P \in k[X]$ un polynôme *unitaire et irréductible*. Le but de cet exercice est d'étudier à quelle condition P s'écrit comme une somme de deux carrés dans $k[X]$. On note $K := k[X]/(P)$.

1) Rappeler la définition de caractéristique d'un corps, ainsi que celle de polynôme irréductible.

2) Montrer que K est un corps.

On propose de montrer l'équivalence suivante :

il existe $A, B \in k[X]$ tels que $P = A^2 + B^2$ $(*)$ ssi -1 est un carré dans K $(**)$.

3) Montrer l'implication $(*) \implies (**)$.

Le reste de l'exercice vise à montrer l'implication $(**) \implies (*)$.
On suppose donc $(**)$ et on note i un élément de K tel que $i^2 = -1$.

4) Traiter le cas où $i \in k$.
[**Indication:** On pourra considérer les polynômes $A_0 = \frac{1+P}{2}$ et $B_0 = \frac{1-P}{2}$.]

Dans toute la suite, on suppose que $i \notin k$. On note $L := k[i]$.

5) Justifier que $L[X]$ est un anneau factoriel.

6) Montrer (rapidement) que l'on a un isomorphisme d'anneaux :

$$L[X]/(P) \cong K[Y]/(Y^2+1).$$

7) En déduire que P n'est pas irréductible dans $L[X]$.

8) Montrer que tout élément de $L[X]$ s'écrit de manière unique $A+iB$, avec $A, B \in k[X]$.

9) On pose $N : L[X] \to k[X],\ A+iB \mapsto A^2+B^2$.
Montrer que N est multiplicative.

10) Soit $Q \in L[X]$ tel que $N(Q)$ soit constant (dans $k[X]$). Montrer que Q est constant.

11) Conclure que P est une somme de deux carrés.

12) **Question subsidiaire (hors barème) :** pour quelles valeurs de n le polynôme cyclotomique $\Phi_n \in \mathbf{Q}[X]$ est-il une somme de deux carrés de $\mathbf{Q}[X]$?