Licence de mathématiques
L3, parcours « enseignement » – arithmétique et groupes
contrôle partiel n° 2 du jeudi 23 novembre
**durée 1h30**

*Ni documents, ni calculatrices, ni téléphones, ni ordinateurs ne sont autorisés.*

2 **Exercice 1** a) Soit $c \in \mathbb{R}$. Exprimer en fonction de $c$ le reste de la division euclidienne de $X^4 - X^3 + X^2 - X + 1$ par $X^2 - cX + 1$ dans $\mathbb{R}[X]$ et déterminer les $c \in \mathbb{R}$ pour lesquels le reste est nul.

2 b) En déduire la factorisation du polynôme $X^4 - X^3 + X^2 - X + 1$ dans $\mathbb{R}[X]$.

2 c) Exprimer les racines complexes de $X^4 - X^3 + X^2 - X + 1$.

3 **Exercice 2** Trouver deux polynômes à coefficients rationnels $U(X), V(X)$ tels que

$$U(X)(X^5 + 1) + V(X)(X^4 + 1) = 1$$

dans $\mathbb{Q}[X]$.

1 **Exercice 3** a) Quel est l'ordre de 5 dans le groupe $(\mathbb{Z}/64\mathbb{Z}, +)$ ?

2 ~~3~~ b) Quel est l'ordre du groupe $((\mathbb{Z}/64\mathbb{Z})^*, \cdot)$ ? Quel est l'ordre de 5 dans $((\mathbb{Z}/64\mathbb{Z})^*, \cdot)$ ?

1 c) Montrer que pour tout $k \in \mathbb{Z}$, $5^k \neq -1 \bmod 64$. *Indication. Raisonner modulo 4.*

2 d) En déduire que l'application

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \to (\mathbb{Z}/64\mathbb{Z})^*,\ (\epsilon, k) \mapsto (-1)^\epsilon 5^k$$

est un isomorphisme de groupes.

2 e) Le groupe $((\mathbb{Z}/64\mathbb{Z})^*, \cdot)$ est-il cyclique ? *Justifier votre réponse.*

1 **Exercice 4** a) Rappeler la définition de la signature d'une permutation $\sigma \in \mathfrak{S}_n$.

4 b) Pour tout diviseur de $d$ de 24, déterminer le nombre d'éléments d'ordre $d$ dans $\mathfrak{S}_4$.

2 c) Soit $G = \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. Quel est l'ordre de $G$ ?

2 d) Montrer que le morphisme dét : $G \to (\mathbb{Z}/3\mathbb{Z})^*$ est surjectif.
En déduire l'ordre du groupe $S = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) = \{g \in G \ :\ \mathrm{dét} g = 1\}$.

3

e) Déterminer l'ordre de la matrice $A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \in S$. Les groupes $S$ et $\mathfrak{S}_4$ sont-ils isomorphes ? *Justifier.*