Université de Bretagne Occidentale
UFR Sciences et Techniques
L3 DE MATHEMATIQUES

ARITHMÉTIQUE ET APPLICATIONS

Contrôle continu, le 22 mars 2022, 8h00-8h30

Documents et calculatrices interdits.

Exercice 1. Le but de cet exercice est de déterminer un générateur du groupe multiplicatif $\mathbb{F}_{25}^\star$ du corps $\mathbb{F}_{25}$ à 25 éléments.

a. Déterminer un générateur du groupe multiplicatif $\mathbb{F}_5^\star$ du corps $\mathbb{F}_5$ à 5 éléments.

Soit $P = X^2 - \bar{2} \in \mathbb{F}_5[X]$.

b. Montrer que P est irréductible dans $\mathbb{F}_5[X]$.

c. En déduire que $\mathbb{F}_5[X]/(P)$ est un corps à 25 éléments.

On le notera $\mathbb{F}_{25}$ dans la suite, et on notera δ la classe $\bar{X}$ de X dans $\mathbb{F}_{25}$ de sorte que $\delta^2 = \bar{2}$. On remarquera que $\mathbb{F}_{25}$ contient $\mathbb{F}_5$ comme sous-anneau.

d. Montrer que δ est d'ordre 8 dans $\mathbb{F}_{25}^\star$.

Soit $Q = X^3 - \bar{1} = (X - \bar{1})(X^2 + X + \bar{1}) \in \mathbb{F}_5[X]$.

e. Montrer que Q a 3 racines distinctes dans $\mathbb{F}_{25}$. (Indication : le discriminant Δ de $X^2 + X + \bar{1}$ est égal à $-\bar{3} = \bar{2} = \delta^2$.)

Notons ε l'une des racines de Q dans $\mathbb{F}_{25}$ différentes de $\bar{1}$.

f. Montrer que ε est d'ordre 3 dans $\mathbb{F}_{25}^\star$.

g. Montrer que $\delta\varepsilon$ est un générateur de $\mathbb{F}_{25}^\star$.

Barème sur 20 points :

Exercice 1a	3 pts
Exercice 1b	3 pts
Exercice 1c	3 pts
Exercice 1d	3 pts
Exercice 1e	3 pts
Exercice 1f	2 pts
Exercice 1g	3 pts