

**Arithmétique et applications, combinatoire et graphes**  
**Devoir préparatoire No. 1, février 2019, corps finis**  
**Aucun document n'est autorisé, usage de calculatrices interdit**

1. Factoriser le polynôme  $x^5 + x + 1$  en polynômes irréductibles sur  $\mathbb{F}_2 = \mathbf{Z}/2\mathbf{Z}$ .
2. Montrer que le polynôme  $x^5 + x^2 + 1$  est irréductible sur  $\mathbb{F}_2$ .

Soit  $\mathbb{K}$  le corps  $\mathbb{K} = \frac{\mathbb{F}_2[x]}{(x^5 + x^2 + 1)}$ .

3. Combien d'éléments y a-t-il dans  $\mathbb{K}$  ?
4. Calculer l'inverse multiplicative de  $x^3 + 1$  dans  $\mathbb{K}$ .
5. Est-ce que le polynôme  $x^5 + x^2 + 1$  est primitif, vu comme un polynôme sur  $\mathbb{F}_2$  ?
6. Soit  $a = \bar{x} = x + (x^5 + x^2 + 1) \in \mathbb{K}$  et soit  $f(x) = x^7 + x^4 + x^2 + 1$ . Calculer  $f(a^4)$ .
7. Quel est le polynôme minimal de  $a$ , de  $a^2$ , de  $a^4$  ?
8. (question optionnelle plus difficile) Trouver le polynôme minimal de  $a^3$ .

FIN