

TP 4

Exercice 1.

On se place en caractéristique $p = 3$.

1. On considère le polynôme $P = X^5 + X^4 + X^2 + 1 \in \mathbb{F}_p[X]$. ($m = \deg(P)$).
On pose $K = \mathbb{F}_p[X]/\langle P \rangle$ et $\alpha = \overline{X} \in K$.
2. Déterminer $\text{Card}(K)$ et l'ordre n de α dans K^* .
3. Ecrire la table de correspondance entre les représentations additive et multiplicative dans K (on utilise un tableau $T = (T_i)_{0 \leq i \leq n-1}$ dans lequel $T_i = f(\alpha)$ où $f(\alpha)$ est l'écriture additive de α^i et une fonction PYTHON ou une procédure MAPLE permettant de calculer le logarithme discret d'un élément x de K^*).
4. Ecrire une fonction PYTHON ou une procédure MAPLE *Orb* permettant de déterminer le cycle d'un entier $i \in \{0, \dots, n-1\}$ pour l'application $F : i \rightarrow pi \bmod n$.
5. On considère le code BCH C de distance apparente $\delta = 8$:
 - (a) Déterminer le plus petit ensemble $J \subset \{0, \dots, n-1\}$ stable par $F : i \rightarrow pi \bmod n$ et contenant $\{1, \dots, \delta-1\}$.
 - (b) Calculer les racines de C .
 - (c) Calculer le polynôme générateur g de C .
 - (d) Combien de mots le code C contient-il ?
 - (e) Quelle est la taille de sa matrice génératrice G ?