TP 5 : Corps finis II

►**Prérequis** : *Chapitre 4 du poly.*

Calculs dans $\mathbf{F}_{244140625}$

1. On pose $P = X^2 - 2 \in \mathbf{F}_5[X]$. Vérifier que P est un polynôme irréductible. On note K son corps de rupture, et $x \in K$ une racine privilégiée du polynôme P.
2. Montrer que $y \in K^\times$ est un carré dans K si, et seulement si, $y^{12} = 1$.
3. Montrer que x n'est pas un carré dans K.
4. On définit le corps de rupture L de $U^2 - x \in K[U]$ sur K, et on note u la classe de U dans le quotient $K[U]/(U^2 - x)$. Rappeler pourquoi L existe, et déterminer le polynôme minimal Q de u sur $\mathbf{F}_5$, *i.e.* le polynôme unitaire $Q \in \mathbf{F}_5[U]$ de degré moindre tel $Q(u) = 0$.
   Indication : On pourra déterminer Q directement, ou bien à l'aide de la proposition 4.36 du poly.
5. L'élément u engendre-t-il le groupe $L^\times$? On rappelle que l'ordre d'un élément d'un groupe fini divise l'ordre de ce groupe. On pourra notamment implémenter une fonction qui prend en entrée un corps fini k et un élément $x \in k$ et qui teste si x est un générateur de $k^\times$ ou non.
6. Qu'en est-t-il de $u + u^2$?
7. Posons $R = V^3 + V + 1 \in \mathbf{F}_5[V]$. Vérifier que R est irréductible. On note M son corps de rupture et v la racine privilégiée de R dans M.
8. Montrer que R reste irréductible quand on le voit dans $L[V]$.
9. On note $LM = L[V]/(R)$. Définir un plongement $M \to LM$.
10. Quel est le cardinal de LM ? Quels sont ses sous-corps ?
11. Développer le polynôme $S = \prod_{i=0}^{11} \left(W - (u+v)^{5^i}\right)$ et constater que $S \in \mathbf{F}_5[W]$. Comment pouvait-on le démontrer ?
12. Faire vérifier à `Sage` que S est irréductible dans $\mathbf{F}_5[W]$.
13. En déduire que $w = u + v$ engendre le corps LM.
14. Démontrer ce résultat par d'autres méthodes, moins calculatoires.
15. Déterminer un générateur du groupe $LM^\times$.
16. Déterminer le polynôme minimal de w sur $\mathbf{F}_5$, L, M.
17. Déterminer des expressions polynomiales à coefficients dans $\mathbf{F}_5$ pour u et v en fonction de w.