TP 6 : Corps finis III

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

Exercice I

On considère $P = X^3 + X + 1 \in \mathbf{F}_7[X]$.

1. Montrer que P est un polynôme irréductible.

On note K le corps de rupture de P sur $\mathbf{F}_7$ et $u \in K$ la racine privilégiée de P.

2. Quel est le cardinal de K ?

3. Combien de racines le polynôme P admet-il dans K ? Exprimer ces racines en fonction de u.

4. Soit $y \in K^\times$. Montrer que y est un carré dans K si, et seulement si, $y^{171} = 1$.

5. Vérifier que $Q = X^2 + 1 + u \in K[X]$ est un polynôme irréductible.

On note L le corps de rupture de Q et $v \in L$ la racine privilégiée de Q dans L.

6. Déterminer un polynôme $R \in \mathbf{F}_7[V]$ unitaire de degré 6 tel que $R(v) = 0$.

7. Montrer que $R \in \mathbf{F}_7[V]$ est un polynôme irréductible.

8. Combien L possède-t-il de sous-corps ? Préciser le degré sur $\mathbf{F}_7$ de chacun d'eux, en nommant ceux qui sont déjà apparus.

9. Montrer que 3 et -1 ne sont pas des carrés dans K.

10. On note $w = v^{1+7^2+7^4}$. Montrer que $w^{7^2} = w$. Déterminer les coefficients du polynôme $(X - w)(X - w^7)$. Que constate-t-on ? A-t-on $w^7 = w$?

11. En déduire l'expression explicite (faisant intervenir u et v) d'une racine carrée de -1 et de 3 dans L. En quoi ceci permet-il de préciser la réponse à la question **8.** ?

Exercice II

Pour l'algorithme de Berlekamp (chapitre 5 du poly), nous aurons besoin de considérer des quotients $k[X]/(P)$ pour k un corps fini et $P \in k[X]$ un polynôme qui ne sera pas forcément irréductible (l'anneau $k[X]/(P)$ ne sera peut-être pas un corps, et donc pas un corps de rupture puisque cette notion suppose que P soit irréductible).

1. Définir l'anneau des polynômes $A := \mathbf{F}_5[X]$.

2. Étudier l'aide associée à `A.quotient` et définir l'anneau quotient $B := A/(P)$ où $P := X^{10} + X + 2 \in A$. Notons x la classe de X dans B.

3. Déterminer une base de B comme $\mathbf{F}_5$-espace vectoriel.

4. Calculer la classe de $X^{1000000}$ dans B.

5. Déterminer le plus petit entier $n \geqslant 1$ tel que $x^{5^n} = x$ dans B. En déduire que P n'est pas un polynôme irréductible.

6. Déterminer un représentant $Q \in A$ de degré < 10 de $x^{5^3} - x \in B$.

7. Calculer le pgcd de P et Q.