

# TP 5 – CORPS FINIS II

► **PRÉREQUIS** : Chapitre 4 du poly.

## Calculs dans $\mathbb{F}_{244140625}$

- On pose  $P = X^2 - 2 \in \mathbb{F}_5[X]$ . Vérifier que  $P$  est un polynôme irréductible. On note  $K$  son corps de rupture, où on note  $x \in K$  une racine privilégiée du polynôme  $P$ .
- Montrer que  $y \in K^\times$  est un carré dans  $K$  si, et seulement si,  $y^{12} = 1$ .
- Montrer que  $x$  n'est pas un carré dans  $K$ .
- On définit le corps de rupture  $L$  de  $U^2 - x \in K[U]$  sur  $K$ , où  $u$  est la classe de  $U$  dans le quotient  $K[U]/(U^2 - x)$ . Déterminer le polynôme minimal  $Q \in \mathbb{F}_5[U]$ , i.e. le polynôme unitaire  $Q \in \mathbb{F}_5[U]$  de degré moindre tel  $Q(u) = 0$ .  
*Indication : On pourra déterminer  $Q$  directement, ou bien à l'aide de la proposition 4.36 du polycopié.*
- L'élément  $u$  engendre-t-il le groupe  $L^\times$  ?
- Qu'en est-il de  $u + u^2$  ?
- Posons  $R = V^3 + V + 1 \in \mathbb{F}_5[V]$ . Vérifier que  $R$  est irréductible. On note  $M$  son corps de rupture (on note  $v$  la racine privilégiée de  $R$  dans  $M$ ).
- Montrer que  $R$  reste irréductible quand on le voit dans  $L[V]$ .
- On note  $LM = L[V]/(R)$ . Définir un plongement  $M \rightarrow LM$ .
- Quel est le cardinal de  $LM$  ? quels sont ses sous-corps ?
- Développer le polynôme  $S = \prod_{i=0}^{11} (W - (u + v)^{5^i})$  et constater que  $S \in \mathbb{F}_5[W]$ . Comment pouvait-on le démontrer ?
- Faire vérifier à Sage que  $S$  est irréductible dans  $\mathbb{F}_5[W]$ .
- En déduire que  $w = u + v$  engendre le corps  $LM$ .
- Démontrer ce résultat par d'autres méthodes, moins calculatoires.
- Déterminer un générateur du groupe  $LM^\times$ .
- Déterminer le polynôme minimal de  $w$  sur  $\mathbb{F}_5$ ,  $L$ ,  $M$ .
- Déterminer des expressions polynomiales à coefficients dans  $\mathbb{F}_5$  pour  $u$  et  $v$  en fonction de  $w$ .

## Exercice II

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

- Montrer que  $P$  est un polynôme irréductible.

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

- Quel est le cardinal de  $K$  ?
- Combien de racines le polynôme  $P$  admet-il dans  $K$  ? Exprimer ces racines en fonction de  $u$ .
- Soit  $y \in K^\times$ . Montrer que  $y$  est un carré dans  $K$  si, et seulement si,  $y^{171} = 1$ .
- 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  $L$ .

- Déterminer un polynôme  $R \in \mathbb{F}_7[V]$  unitaire de degré 6 tel que  $R(v) = 0$ .
- Montrer que  $R \in \mathbb{F}_7[V]$  est un polynôme irréductible.
- Combien  $L$  possède-t-il de sous-corps ? Préciser le degré sur  $\mathbb{F}_7$  de chacun d'eux, en nommant ceux qui sont déjà apparus.
- Montrer que 3 et  $-1$  ne sont pas des carrés dans  $K$ .
- 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  $w^7 = w$  ?
- 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 ?