

RETOUR TP 5 – CORPS FINIS II

► PRÉREQUIS : Chapitre 4 du poly.

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

1. Le polynôme $P = X^2 - 2 \in \mathbb{F}_5[X]$ est irréductible car de degré 2 sans racine dans $\mathbb{F}_5$ car

$$P(\bar{0}) = -2 \neq 0, \quad P(\bar{1}) = P(\bar{4}) = -1 \neq 0, \quad P(\bar{2}) = P(\bar{3}) = 2 \neq 0,$$

en notant $\bar{n}$ la classe de n dans $\mathbb{Z}/5\mathbb{Z}$.

2. Puisque P est irréductible de degré 2, K est de cardinal $5^2 = 25$ de sorte que $K^\times$ est de cardinal 24. On a donc que si $y \in K^\times$ est un carré, il existe $z \in K^\times$ tel que $y = z^2$ si bien que $y^{12} = z^{24} = 1$. Pour la réciproque, on a au moins deux méthodes.

- (i) Notons ω un générateur du groupe cyclique $K^\times$ et soit $y \in K^\times$ tel que $y^{12} = 1$. Il existe alors par définition $\ell \in \mathbb{Z}$ tel que $y = \omega^\ell$. Ainsi $\omega^{12\ell} = 1$ si bien que $24 \mid 12\ell$ soit $2 \mid \ell$ car ω est d'ordre 24. Posant alors $z = \omega^{\frac{\ell}{2}}$, on a bien $y = z^2$.
- (ii) L'homomorphisme de groupes de $K^\times$ dans lui-même défini par $x \mapsto x^2$ a un noyau de cardinal 2, à savoir $\{-1, 1\}$. Ainsi, le cardinal de son image est de 12. En notant E l'ensemble des $y \in K^\times$ tels que $y^{12} = 1$. On a vu précédemment que E contient cette image. Ainsi E contient au moins 12 éléments mais par ailleurs il en contient au plus 12 car le polynôme $X^{12} - 1$ a au plus 12 racines dans le corps K . Il s'ensuit que E est de cardinal 12 et est égal à l'image, ce qui conclut la preuve.
3. On va bien sûr faire appel à la question précédente. On a clairement $x^2 = 2$ et donc $x^{12} = 2^6 = 4^3 = (-1)^3 = -1 \neq 1$ car on est en caractéristique différente de 2 et où les entiers $-1, 1, 2$ et 4 sont vus dans K et plus précisément dans son sous-corps premier $\mathbb{Z}/5\mathbb{Z}$. On peut aussi bien évidemment faire appel à Sage ici. On conclut donc par la question précédente que x n'est pas un carré dans K .
4. Puisque x n'est pas un carré dans K , le polynôme $U^2 - x$ est de degré 2 et sans racine dans K de sorte qu'il est irréductible sur $K[U]$. Ainsi L est bien défini comme son corps de rupture. Pour déterminer le polynôme minimal Q de u sur $\mathbb{F}_5$, on a là encore deux méthodes.

- (i) On applique la proposition 4.36 du polycopié qui nous indique que le polynôme minimal Q est donné par

$$Q = \prod_{i=0}^{d-1} (X - u^{5^i})$$

où d est le plus petit entier strictement positif tel que $u^{5^d} = u$. On obtient avec Sage que $d = 4$ et que $Q = X^4 - 2$.

- (ii) On peut aussi le calculer directement. En effet, on a $[L : K] = 2$ et $[K : \mathbb{F}_5] = 2$ de sorte que par multiplicativité du degré, $[L : \mathbb{F}_5] = 4$. On sait alors que le polynôme minimal de u sur $\mathbb{F}_5[X]$ est un polynôme unitaire irréductible de degré 4. Or, on a $u^2 = x$ et donc $u^4 = x^2 = 2$ de sorte que $X^4 - 2 \in \mathbb{F}_5[X]$ annule u . Le polynôme minimal de u divise donc $X^4 - 2$ et comme ces deux polynômes sont unitaires et ont même degré, on en déduit que $Q = X^4 - 2$.
5. Puisque L est une extension de degré 4 de $\mathbb{F}_5$, il est de cardinal 5^4 et le groupe $L^\times$ de cardinal $5^4 - 1$. Pour vérifier si x est un générateur, il suffit de vérifier que $x^{\frac{5^4-1}{p}} \neq 1$ pour tout nombre premier $p \mid 5^4 - 1$. On constate que u n'est pas un générateur. On pouvait le voir aisément à la main car $u^4 = 2$ donc $u^{16} = 2^4 = 16 = 1$ donc u n'est pas d'ordre $5^4 - 1 = 624$.
6. En revanche, $u + u^2$ en est un.
7. On vérifie que R est de degré 3 et sans racine dans $\mathbb{F}_5$ car

$$R(\bar{0}) = R(\bar{2}) = R(\bar{3}) = 1, \quad R(\bar{1}) = 3, \quad R(\bar{4}) = 4$$

donc irréductible.

8. On peut vérifier avec Sage que R reste irréductible quand on le voit dans $L[V]$ avec la commande `factor` ou en vérifiant que R n'a pas de racine dans L .
9. Le plongement de $\mathbb{F}_5 \rightarrow L$ fournit un morphisme $\mathbb{F}_5[X] \rightarrow L[X]$ qui, composé avec la surjection canonique, fournit un morphisme $\mathbb{F}_5[X] \rightarrow L[X]/(R)$. Ce dernier passe immédiatement au quotient modulo l'idéal engendré par R et fournit un plongement $\mathbb{F}_5[X]/(R) \rightarrow L[V]/(R)$, soit un plongement $M \rightarrow LM$.

1. Où l'on a bien $1 \neq -1$ car on est en caractéristique $5 \neq 2$.
2. En effet, L contient le corps de rupture de u et ce dernier n'est pas de degré 2 donc ce corps de rupture est nécessairement égal à L . S'il était de degré 2, on aurait un polynôme unitaire de degré 2 annihilant u et en remplaçant u^2 par x , on aurait que $x \in \mathbb{F}_5$ ou que $u \in K$, ce qui est absurde.
3. Je rappelle que tout morphisme de corps est injectif!

- 10.** Puisque LM est une extension de L de degré 3 car R est irréductible de degré 3, le cardinal de LM est celui de L au cube, soit $625^3 = 244140625 = 5^{12}$, ce qu'on retrouve avec Sage. Pour chaque $d \in \{1, 2, 3, 4, 6, 12\}$, on sait d'après le cours que LM admet un unique sous-corps de cardinal 5^d . Il s'agit dans l'ordre de $\mathbf{F}_5, K, M, L, K[V]/(R)$ et LM . Pour $K[V]/(R)$, puisque K se plonge dans L , R reste irréductible sur K et $K[V]/(R)$ se plonge dans LM comme en question 9. avec le plongement de K dans L .
- 11.** En développant le polynôme⁴ $S = \prod_{i=0}^{11} (W - (u+v)^{5^i})$ avec Sage, on constate que $S \in \mathbf{F}_5[W]$. On pouvait l'établir de la façon suivante. Puisque $u+v \in LM$ et que $[LM : \mathbf{F}_5] = 12$, on a $(u+v)^{5^{12}} = u+v$ donc l'ensemble des racines de S est stable par le morphisme de Frobenius $x \mapsto x^5$. Comme les coefficients de S sont des polynômes symétriques en ses racines, ils sont eux aussi invariants par ce morphisme de Frobenius et par conséquent dans $\mathbf{F}_5$.
- 12.** On fait vérifier à Sage que S est irréductible dans $\mathbf{F}_5[W]$.
- 13.** Comme S est irréductible unitaire et annulant $u+v$, on en déduit que S est le polynôme minimal de $u+v$ sur $\mathbf{F}_5[X]$. Ainsi $\mathbf{F}_5(u+v)$ est une extension de $\mathbf{F}_5$ de degré 12 incluse dans LM qui est aussi de degré 12. On peut donc en conclure que $LM = \mathbf{F}_5(u+v)$ et $u+v$ engendre bien LM .
- 14.** On peut retrouver ce résultat en utilisant le fait que $\mathbf{F}_5(w)$ est un sous-corps de LM et que ce dernier est égal à LM si, et seulement si, $(u+v)^{5^d} \neq u+v$ pour $d \in \{1, 2, 3, 4, 6\}$, ce que l'on peut vérifier avec Sage. Mais cela reste calculatoire et on peut encore s'épargner des calculs. En effet, $u+v \notin \mathbf{F}_5(u)$ et $u+v \notin \mathbf{F}_5(v)$ car sinon on aurait respectivement $\mathbf{F}_5(v) \subseteq \mathbf{F}_5(u)$ ou $\mathbf{F}_5(v) \subseteq \mathbf{F}_5(u)$, ce qui est impossible pour des raisons de degré⁵. En particulier, $\mathbf{F}_5(w) \neq \mathbf{F}_5, M, L$. De même, $\mathbf{F}_5(w) \neq K$ car sinon $v \in \mathbf{F}_5(u)$ car $x = u^2$ et $K = \mathbf{F}_5(x)$ ce qui est de même impossible pour des raisons de degré. Finalement $\mathbf{F}_5(w)$ est une sous-extension de LM de degré 6 ou 12. Il suffit alors par exemple de vérifier que $w^{5^6} \neq w$, ce que l'on peut faire avec Sage. Mais on peut aussi s'en sortir sans calcul puisque une sous-extension de degré 6 ou 12 contient une unique sous-extension de degré 3. Ici on n'a pas le choix, cela implique que $\mathbf{F}_5(w)$ contient $M = \mathbf{F}_5(v)$ de sorte que $\mathbf{F}_5(w)$ contient nécessairement aussi $\mathbf{F}_5(v)$. Puisque $\mathbf{F}_5(w)$ contient une sous-extension de degré 3 et une de degré 4, par multiplicativité des degrés, son degré est multiple du ppcm de 3 et 4, à savoir de 12 et par conséquent, $\mathbf{F}_5(w) = LM$.
- 15.** On obtient avec Sage un générateur en appliquant l'algorithme du cours ou décrit en question 5.
- 16.** On a vu que le polynôme minimal de w sur $\mathbf{F}_5$ est donné par S , que l'on a simplifié avec Sage. Pour L et M on applique la proposition 4.36 du cours, le polynôme minimal sur L , respectivement M est donné par

$$\prod_{i=0}^{d_L-1} (X - w^{5^{4i}}), \quad \text{respectivement} \quad \prod_{i=0}^{d_M-1} (X - w^{5^{3i}})$$

où d_L est le plus petit entier strictement positif tel que $w^{5^{4d_L}} = w$ et d_M est le plus petit entier strictement positif tel que $w^{5^{3d_M}} = w$. On effectue alors les calculs avec Sage.

- 17.** Il est clair que $W = (1, w, w^2, \dots, w^{11})$ forme une base du $\mathbf{F}_5$ -espace vectoriel LM et que

$$B = (1, u, u^2, u^3, v, vu, vu^2, vu^3, v^2, v^2u, v^2u^2, v^2u^3)$$

également. En faisant développer les w^i pour $i \in \{1, \dots, 11\}$ à Sage et en récoltant les coefficients de w^i dans la base B , on obtient une matrice $M \in \mathcal{M}_{12}(\mathbf{F}_5)$ telle que ${}^tW = M^tB$. Autrement dit ${}^tB = M^{-1} \times {}^tW$ et le deuxième et le quatrième coefficient du vecteur $M^{-1} \times {}^tW$ fournissent les expressions polynomiales de u et v en fonction de w voulues.

Attention que la fonction Sage `x.minpoly()` donne le polynôme minimal de x sur k si x vit dans $k[X]/(P)$. Mais par exemple, en question 4., la commande renvoyait pour u le polynôme $X^2 - x$ puisque pour Sage, u vit dans $K[X]/(X^2 - x)$.

Exercice II

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

- 1.** On vérifie que P est un polynôme de degré 3 sans racine modulo 7 et par conséquent irréductible.

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

- 2.** Le polynôme P étant irréductible de degré 3, le cardinal de K est de $7^3 = 343$.
- 3.** Sur un corps fini, tout corps de rupture étant corps de décomposition, le polynôme P admet donc 3 racines dans K . Ces racines sont u , $u^7 = -5u^2 - 1$ et $u^{7^2} = u^{49} = -2u^2 - u - 6$. On peut par exemple l'obtenir à l'aide de Sage ou de la proposition 4.36 du polycopié de cours.

4. Je vous renvoie à la Proposition 5.46 pour expliquer d'où sort ce polynôme S .

5. Une extension de $\mathbf{F}_5$ de degré 4 ne peut pas contenir une sous-extension de degré 3 et inversement.

4. On raisonne exactement comme en question 2. de la section précédente.

5. Le polynôme $Q = X^2 + 1 + u \in K[X]$ est un polynôme de degré 2 sans racine dans K et par conséquent irréductible. On peut vérifier qu'il n'a pas de racine dans K avec Sage par exemple. On peut aussi noter que, pour faire moins de calculs, on peut avoir recours à la question précédente. En effet, Q est irréductible si, et seulement si, $-1 - u$ n'est pas un carré⁶ dans $K^\times$. Or, on vérifie avec Sage que $(-1 - u)^{171} = -1 \neq 1$ et par conséquent $-1 - u$ n'est pas un carré et Q est irréductible sur $K[X]$.

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

6. En appliquant la proposition 4.36, il suffit de poser

$$R(V) = \prod_{i=0}^6 (V - v^{7^i}) \in \mathbf{F}_7[X]$$

car $v^{7^6} = v$ car par multiplicativité des degrés, $[L : \mathbf{F}_7] = [L : K][K : \mathbf{F}_7] = 6$. Sage fournit que

$$R(V) = V^6 + 3V^4 + 4V^2 + 1.$$

7. On a $u = -1 - v^2 \in \mathbf{F}_7(v)$ de sorte que $L = K(v) = \mathbf{F}_7(u, v) \subseteq \mathbf{F}_7(v)$ et l'inclusion réciproque étant évidente, on a $L = \mathbf{F}_7(v)$ et par conséquent $[\mathbf{F}_7(v) : \mathbf{F}_7] = 6$. Le polynôme minimal de v sur $\mathbf{F}_7[X]$ est donc irréductible unitaire de degré 6. Par ailleurs, il divise R qui est unitaire et de degré 6 car $R(v) = 0$ et $R \in \mathbf{F}_7[X]$. Il s'ensuit que le polynôme minimal de v est R et ainsi R est irréductible sur $\mathbf{F}_7[X]$. Une autre méthode plus laborieuse est d'écrire tous les polynômes irréductibles de $\mathbf{F}_7$ de degré 2, 3 et 4 et de vérifier que R n'est pas produit de tels polynômes. Cette version (bien sûr beaucoup plus longue) est aussi implémentée dans le Notebook Jupyter.

8. On a $[L : \mathbf{F}_7] = 6$ et les sous-corps de L sont en bijection avec les diviseurs de 6. Ce sont donc $\mathbf{F}_7$, K , L ainsi qu'un sous-corps de degré 2.

9. On constate avec Sage que $3^{171} = (-1)^{171} = -1$ et on conclut avec la question 4. On peut ici faire le calcul à la main dans le sous-corps premier $\mathbf{F}_7$ en constatant par exemple que $3^3 \equiv -1 \pmod{7}$ et que $171 = 3 \times 57$.

10. On a $w^{7^2} = v^{7^2+7^4+7^6} = w$ car $v^{7^6} = v$ comme on l'a vu en question 6. On constate avec Sage que

$$(X - w)(X - w^7) = X^2 + 1$$

qui est à coefficients dans $\mathbf{F}_7$. Si l'on note L' le sous-corps de L de degré 2 de la question 8, on a un corps de cardinal $7^2 = 49$. Le morphisme de Frobenius F associé à L' est donc donné par $F(x) = x^{49}$. Comme $[L : L'] = 3$ et $v \in L$, on a $F^3(v) = F \circ F \circ F(v) = v$ (ce qui ne traduit rien d'autre que le fait que $v^{7^6} = v$). Or, on a vu que $F(w) = w$ ce qui implique que $w \in L'$ et $\mathbf{F}_7(w) \subseteq L'$ avec $[L' : \mathbf{F}_7] = 2$. On vérifie alors avec Sage que $w^7 \neq w$ ce qui implique que $\mathbf{F}_7(w) \neq \mathbf{F}_7$ et $\mathbf{F}_7(w) = L'$.

11. D'après la question précédente, $w^6 \neq 1$ et puisque $w \in L'^\times$ et $w^{49} = w$, alors $w^{48} = 1$. Or, $48 = 6 \times 2^3$. On détermine avec Sage l'unique entier $i \in \{1, 2, 3\}$ tel que $w^{6 \times 2^i} = 1$ et $w^{6 \times 2^{i-1}} \neq 1$. On obtient $i = 1$ et on a alors $w^6 = -1$ si bien que $w'^2 = -1$ avec $w' = w^3$. Les deux racines de -1 dans L sont donc $\pm w^3$. Par ailleurs, -3 est un carré dans $\mathbf{F}_7$, en tant que produit de deux non carrés⁷ et on obtient facilement que $-3 = 2^2$ modulo 7. Ainsi $\pm 2w' = \pm 2w^3$ sont les deux racines carrées de 3 dans L . Le sous-corps L' de degré 2 de la question 8 est donc donné par $L' = \mathbf{F}_7(w) = \mathbf{F}_7(w')$.

On pouvait aussi utiliser le fait que

$$(X - w)(X - w^7) = X^2 + 1.$$

Ainsi, w et w^7 sont les deux racines carrées de -1 dans L . On retrouve le résultat précédent car $w^2 = -1$ donc $w^3 = -w$ et ainsi $w^7 = w^3$.

6. On a évidemment $-1 - u \neq 0$.

7. Penser par exemple au symbole de Legendre.