CC2 du 19/11/2024 - Algèbre M1 MIC

15h15-16h45 (1h30)
Sans documents ni calculatrices.

Exercise 1

1. ($\simeq$ 1 points) On considère le polynôme $P = X^5 - 4X^2 - 4X + 2$. Montrer que P est irreductible dans $\mathbb{Z}[X]$.

   Solution: On peut lui appliquer le critère d'Eisenstein avec $p = 2$.

2. ($\simeq$ 3 points)
   (a) Montrer que P a une racine multiple dans $\mathbb{F}_5$ et donnez toutes les racines de P dans $\mathbb{F}_5$.

   Solution: Dans $\mathbb{F}_5$, le polynôme devient $P = X^5 + X^2 + X + 2$. Les racines sont 1 et 2 (en vérifiant les cinq éléments un par un). Pour déterminer lesquelles sont multiplies, on dérive le polynôme : $P' = 5X^4 + 2X + 1 = 2X + 1$. Comme $P'(1) = 3 \neq 0$, c'est que 1 est racine simple, mais $P'(2) = 0$ donc 2 est racine multiple.

   (b) On note D_5 le corps de décomposition de P sur $\mathbb{F}_5$. Quelle est la dimension $[D_5 : \mathbb{F}_5]$?

   Solution: D'après ce qui précède, P est divisible par $(X - 1)$ et $(X - 2)^2$. En faisant la division euclidienne, on trouve que

   $$P = (X - 1)(X - 2)^2(X^2 + 2).$$

   Donc le corps D_5 est le corps de rupture de $X^2 + 2$ (qui est irréductible) et est donc de degré $[D_5 : \mathbb{F}_5] = 2$.

3. ($\simeq$ 1 points) Montrer que l'anneau $K_3 = \mathbb{F}_3[X]/(X^2 + 1)$ est un corps et donner son cardinal et sa caractéristique.

   Solution: Le polynôme $X^2 + 1$ n'a pas de racine dans $\mathbb{F}_3$. Comme il est de degré 2, il est donc irréductible, et comme $\mathbb{F}_3[X]$ est principal, il engendre donc un idéal maximal. Ce corps est une extension de degré 2 de $\mathbb{F}_3$ (une base sur $\mathbb{F}_3$ est donnée par $[1], [X]$), il est donc encore de caractéristique 3 et de cardinal $3^2 = 9$.

Dans toute la suite de l'exercice 1, notera i la classe de X dans ce corps.

4. ($\simeq$ 5 points)
   (a) Donner le polynôme minimal de $i + \epsilon$ sur $\mathbb{F}_3$ pour $\epsilon \in \{-1, 1\}$.

   Solution: Quitte à multiplier par une constante on peut chercher un polynôme minimal unitaire. Comme l'extension est de degré 2, ce polynôme minimal est au plus de degré 2. On peut donc le chercher sous la forme $X^2 + aX + b$ avec $a, b \in \mathbb{F}_3$.

— Pour $i+1$: on a $(i+1)^2 + a(i+1) + b = (2+a)i + a + b$. Pour que ça s'annule, on prend $a = -2 = 1$ et $b = -a = 2$, donc le polynôme minimal est $X^2 + X + 2$.
— Pour $i-1$: on a $(i-1)^2 + a(i-1) + b = (-2+a)i - a + b$. Pour que ça s'annule, on prend $a = 2$ et $b = a = 2$, donc le polynôme minimal est $X^2 + 2X + 2$.
Autre méthode : si $\beta = i + \epsilon$, on a $(\beta - \epsilon)^2 = -1$ donc $\beta^2 - 2\beta\epsilon + 1 = -1$ ou encore $\beta^2 + 2\beta\epsilon + 2 = 0$. Le polynôme minimal est donc $X^2 + 2\epsilon X + 2$.

(b) Donner un isomorphisme d'anneaux explicite entre $\mathbb{F}_3[X]/(X^2+1)$ et $\mathbb{F}_3[X]/(X^2+X-1)$

Solution: Il s'agit de trouver un élément $\alpha \in K_3$ qui vérifie $\alpha^2 + \alpha - 1 = 0$. Coup de chance : c'est le polynôme minimal de $i+1$ trouvé à la question précédente. L'application $\mathbb{F}_3[X] \to K_3$, $X \mapsto i+1$ passe donc au quotient pour définir un morphisme d'anneaux $\mathbb{F}_3[X]/(X^2+X-1) \to K_3$. Comme les deux sont des corps, c'est un morphisme injectif ; et comme ces deux corps sont de dimension 2 sur $\mathbb{F}_3$, c'est un isomorphisme.

(c) Donner un générateur θ du groupe mutiplicatif $(\mathbb{F}_3[i])^\times$.

Solution: Le groupe $K_3^\times$ est cyclique d'ordre $9-1 = 8$. Il nous faut donc trouver un élément $\alpha \in K_3^\times$ d'ordre 8. On connaît déjà un élément d'ordre 4 : l'élément $i \in K_3^\times$ vérifie $i^2 = -1 \neq 1$ mais $i^4 = 1$. Une racine carrée de i fera donc l'affaire.
Supposons que $\alpha = a + ib$, alors $\alpha^2 = a^2 - b^2 + 2abi$. On veut donc résoudre :

$$\begin{cases} a^2 - b^2 = 0 \\ 2ab = 1 \end{cases} \iff \begin{cases} a = \pm b \\ ab = -1 \end{cases}$$

Une solution est par exemple donnée par $\alpha = 1 - i$, qui vérifie bien $\alpha^2 = i$.
PS : Sinon on peut juste tester des valeurs au hasard...

5. ($\simeq 2$ points) Trouvez une racine de P dans $\mathbb{F}_3[i]$ et factorisez P dans $\mathbb{F}_3[X]$.

Solution: On remarque que i est une racine, et donc (pour justifier ce « donc », il faut faire un peu de théorie de Galois !) $-i$ aussi. On en déduit que P est divisible par $(X-i)(X+i) = X^2+1$. La division euclidienne donne $P = (X^2+1)(X^3+2X+2)$. Ce dernier polynôme est irréductible sur $\mathbb{F}_3$ (c'est le polynôme minimal de $i+1$ trouvé plus haut).

6. ($\simeq 5$ points) On note α une racine de $Q = X^3 - X - 1$ dans une extension de $\mathbb{F}_3$.
(a) Montrer que $\alpha^9 \neq \alpha$.

Solution: Comme α est racine de Q, on a $\alpha^3 = \alpha + 1$. Donc $\alpha^9 = (\alpha^3)^3 = (\alpha+1)^3$. Or, en caractéristique 3, $x \mapsto x^3$ est un morphisme de corps, donc $(\alpha+1)^3 = \alpha^3 + 1^3 = \alpha + 2$. Comme $2 \neq 0$, on a bien $\alpha^9 \neq \alpha$.

(b) Montrer que $\mathbb{F}_3[\alpha]$ est le corps de décomposition de Q.

Solution: L'élément α est une racine de Q, c'est-à-dire que $\alpha^3-\alpha-1$ ou encore $\alpha^3=\alpha+1$. L'automorphisme de Frobenius $x\mapsto x^3$ envoie donc α sur $\alpha+1$. Or, si $Q(\alpha)=0$, alors $\mathrm{Frob}(Q(\alpha))=0$, et comme Q est à coefficients dans $\mathbb{F}_3$, on a donc $Q(\mathrm{Frob}(\alpha))=0$, c'est-à-dire $Q(\alpha+1)=0$. Comme $\alpha+1\neq\alpha$, on en déduit que Q a au moins deux racines distinctes dans $\mathbb{F}_3[\alpha]$, et comme il est de degré 3, on en déduit qu'il est scindé. Comme $\mathbb{F}_3[\alpha]$ est engendré par une racine de P et que P y est scindé, c'est par définition le corps de décomposition de P.

(c) Quel est le cardinal du corps de décomposition D_3 de P sur $\mathbb{F}_3$?

Solution: Le corps D_3 est engendré par α et i (les racines de $Q=X^2-X-1$ et X^2+1). Comme $\mathbb{F}_3[i]$ est de degré 2, tous ses éléments vérifient $x^{3^2}=x$. Comme ce n'est pas le cas de α, c'est que $\alpha\notin\mathbb{F}_3[i]$. On en déduit que $[D_3:\mathbb{F}_3]=[\mathbb{F}_3[\alpha,i]:\mathbb{F}_3[i]]\times[\mathbb{F}_3[i]:\mathbb{F}_3]=3\times 2=6$.

Exercise 2

On considère le polynôme $T=X^6-2$ de $\mathbb{Q}[X]$.

1. ($\simeq 2.5$ points) Donnez les racines réelles de T et factorisez T dans $\mathbb{R}[X]$.

Solution: Notons $\alpha=\sqrt[6]{2}$. Ce polynôme admet six racines complexes : $\alpha, e^{2i\pi/6}\alpha,\dots,e^{10i\pi/6}\alpha$. Parmi celles-ci, seules deux sont réelles, à savoir α et $-\alpha$. Le polynôme est donc divisible par $(X-\alpha)(X+\alpha)$.
De plus, pour $z\in\mathbb{C}$, on a $(X-z)(X-\bar{z})=X^2-2\Re(z)X+|z|^2$ est à coefficients réels, donc on peut apparier les racines complexes deux par deux pour en déduire que le polynôme est divisible par :

$$(X-e^{2i\pi/6}\alpha)(X-e^{-2i\pi/6}\alpha)=X^2-\alpha X+\alpha^2,$$
$$(X-e^{4i\pi/6}\alpha)(X+e^{-4i\pi/6}\alpha)=X^2+\alpha X+\alpha^2.$$

On en déduit que :

$$T=(X-\alpha)(X+\alpha)(X^2-\alpha X+\alpha^2)(X^2+\alpha X+\alpha^2).$$

2. ($\simeq 2.5$ points) On note D_T le corps de décomposition de T.
   (a) Montrer que T est irréductible sur $\mathbb{Q}$ et que son corps de rupture n'est pas isomorphe à D_T.

Solution: Le critère d'Eisenstein ($p=2$) montre que T est irréductible sur $\mathbb{Q}$. D'après ce qui précède, $\mathbb{Q}[\alpha]$ est le corps de rupture de T, mais P n'y est pas scindé, donc le corps de rupture n'est pas isomorphe au corps de décomposition.

   (b) Montrer que $D_T=\mathbb{Q}[\sqrt[6]{2},i\sqrt{3}]$ et donner la valeur de $[D_T:\mathbb{Q}]$.

Solution: Comme $e^{2i\pi/6} = \frac{1+i\sqrt{3}}{2}$, on remarque que toute les racines de T sont dans $\mathbb{Q}[\alpha, i\sqrt{3}]$, donc ce corps contient le corps de décomposition de T dans $\mathbb{C}$, i.e., $D_T \subset \mathbb{Q}[\alpha, i\sqrt{3}]$.
De plus, $(i\sqrt{3})^2 = -3 \in \mathbb{Q}$, donc $[\mathbb{Q}[i\sqrt{3}] : \mathbb{Q}] = 2$. Par multiplicativité des degrés et que $i\sqrt{3} \notin \mathbb{Q}[\alpha]$, on en déduit que :

$$[\mathbb{Q}[\alpha, i\sqrt{3}] : \mathbb{Q}[\alpha]] = 2.$$

Comme D_T contient toutes les racines de P, il doit contenir $\mathbb{Q}[\alpha]$, i.e., on a :

$$\mathbb{Q}[\alpha] \subset D_T \subset \mathbb{Q}[\alpha, i\sqrt{3}].$$

Comme $\mathbb{Q}[\alpha]$ n'est pas le corps de décomposition, il est strictement inclus dans D_T, donc $[D_T : \mathbb{Q}[\alpha]]$ est au moins égal à 2. On en déduit donc que $[\mathbb{Q}[\alpha, i\sqrt{3}] : D_T] \leq 1$, et donc $D_T = \mathbb{Q}[\alpha, i\sqrt{3}]$.
Par multiplicativité du degré, on obtient $[D_T : \mathbb{Q}] = [D_T : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}] = 2 \cdot 6 = 12$.