Anneaux et corps (MATH-215) — Examen final

23 juin 2023, 15 h 15 – 18 h 15

Nom : Grothendieck

SCIPER : 42

Signature : _____

Numéro

1

Ce dossier d'examen contient 6 exercices, sur 32 pages, pour un total de 100 points. Veuillez utiliser l'espace quadrillé pour vos réponses. N'écrivez **PAS** dans la marge intérieure du livret.

Veuillez rédiger vos solutions sous l'exercice correspondant : sous chaque exercice, il y a l'espace quadrillé prévu à cet effet. Si vous avez besoin de davantage d'espace pour vos solutions, utilisez l'espace restant après la solution d'un autre exercice. Dans ce cas, notez soigneusement où votre solution continue. Si même cela ne suffit pas, demandez aux surveillant(e)s des feuilles additionnelles. Dans ce cas, écrivez vos noms et prénoms ainsi que le numéro de l'exercice que vous résolvez sur le papier additionnel. A la fin de l'examen, sous la surveillance d'un(e) surveillant(e), mettez-les dans le dossier d'examen, indiquez le nombre de pages additionnelles sur la feuille de présence, et signez-là. Vous n'êtes pas autorisés à utiliser vos propres feuilles de brouillon, nous les fournissons. Veuillez ne pas écrire vos solutions au crayon.

Il est interdit de commencer à lire l'examen avant que le signal ne soit explicitement donné. La durée totale de l'épreuve est 180 minutes. Durant les 20 dernières minutes, veuillez rester à votre place, même si vous avez fini. Les copies seront collectées par les surveillant(e)s à la fin de l'examen, et il vous sera alors demandé de rester assis.

La seule feuille de papier autorisée, autre que celles de ce dossier d'examen et les brouillons, est un aide-mémoire manuscrit d'une page A4 (possiblement recto-verso). Tous les documents devront être rendus à la fin de l'examen, y compris les brouillons et l'aide-mémoire. Les livres, notes de cours, et aide-mémoire de plus d'une page ne sont **PAS** autorisés. Aucun matériel électronique n'est autorisé. Veuillez présenter votre CAMIPRO sur le bord de votre table. Aucun sac ou manteau ne doit se trouver à votre place assise.

Vous pouvez résoudre chaque point de chaque exercice séparément. Si vous résolvez un point correctement en admettant les résultats des points précédents, vous recevrez le score maximal. Prenez soin de démontrer tous vos calculs, de justifier et d'expliquer toutes les étapes de votre raisonnement. Nous ne donnons le maximum de points que si la preuve est correcte et présente tous les détails importants.

Vous êtes autorisés à utiliser tous les résultats vus en cours ou en exercices, sauf si la question demande exactement un tel résultat ou un cas particulier évident d'un tel résultat. Lorsque vous utilisez un résultat du cours ou des exercices, vous devez soit le citer par son nom, soit citer la proposition précisément en disant : on a vu dans le cours que "[ici l'énoncé précis du résultat]".

Question:	1	2	3	4	5	6	Total
Points:	16	18	16	18	14	18	100
Score:							

Exercice 1 [**16 pts**]

Considérons la situation suivante :

- L est un corps,
- $G \subseteq \mathrm{Aut}(L)$ est un sous-groupe fini,
- $\alpha \in L$,
- $\alpha_1, \ldots, \alpha_r$ est l'orbite de α par l'action de G, où les α_i sont des éléments distincts de L,
- $f = \prod_{i=1}^{r}(x - \alpha_i) \in L[x]$,
- $K = L^G$.

Dans cette situation :

(1) Démontrez que $f \in K[x]$.

(2) Démontrez que pour chaque $h = \sum_{i=0}^{s} a_i x^i \in K[x]$ et pour chaque $g \in G$ on a l'égalité $g(h(\alpha)) = h(g(\alpha))$.

(3) Démontrez que $m_{\alpha,K} = f$.

Vous pouvez utiliser sans preuve que le polynôme minimal (unitaire) de α sur K est uniquement déterminé par les propriétés qu'il est un polynôme irréductible sur K, et qu'il s'annule en α.

(4) Démontrez que $K \subseteq L$ est une extension algébrique séparable.

(5) Démontrez que $K \subseteq L$ est une extension simple.

Vous pouvez utiliser sans preuve le théorème d'élément primitif: chaque extension séparable de degré fini est simple.

Solution:

Cet exercice consistait à redémontrer des propositions du cours.

1. Soit $g \in G$. Alors on a

$$gf = \prod_{i=1}^{r}(x - g\alpha_i) = \prod_{i=1}^{r}(x - \alpha_i) = f.$$

Où dans la deuxième égalité on a utilisé que $\alpha_1, \ldots, \alpha_r$ forme une orbite. Dès lors on conclut que les coefficients de f sont invariants par g. Comme $g \in G$ est quelconque, on conclut que les coefficients sont fixés par G, et donc que $f \in K[x]$.

2. La clé est que les éléments de K sont fixés par G. En effet, si $h = \sum_j a_j x^j$, alors

$$g(h(\alpha)) = \sum_j g(a_j)g(\alpha)^j = \sum_j a_j g(\alpha)^j = h(g(\alpha)).$$

3. Grâce à au point précédent, on obtient pour tout α_i que $m_{\alpha,K}(\alpha_i) = 0$. Ainsi on obtient que $f | m_{\alpha,K}$. Comme $f \in K[x]$ a un coefficient dominant égal à 1 on obtient $f = m_\alpha$.

4. Cela suit des derniers points : on a montré que le polynôme minimal de tout α dans L et donné par la formule de l'avant dernier point de la donnée et a donc par définition des racines distinctes.

5. Le point déterminant à démontrer est que le degré de l'extension est fini. On pourra alors conclure par le théorème de l'élément primitif. Notons que pour tout $\alpha \in L$ on obtient que $[K(\alpha) : K]$ est la taille d'une orbite d'un G-ensemble grâce au calcul de $m_{\alpha,K}$, et donc $[K(\alpha) : K]|\text{Card}(G)$. Notons également que par le théorème de l'élément primitif, comme toute sous-extension d'une extension séparable est séparable, que toute sous-extension de degré fini de L est simple. Dès lors, on conclut que toute sous-extension de degré fini de L à un degré qui divise $\text{Card}(G)$. Si on suppose par l'absurde que $[L : K]$ est infini alors par récurence on trouve une sous-extension de degré fini de degré arbitrairement grand. En particulier, on trouve des extensions de degré strictement plus grand que $\text{Card}(G)$, une contradiction.

Barème

1. 3pts
2. 2pts (1 pt pour le calcul, et 1 pt pour dire explicitement que les a_j sont fixés par G).
3. 3pts (1 pt pour utiliser le point précédent pour dire que $m_{\alpha,K}(\alpha_i) = 0$, et 2 pts pour le reste de l'argument)
4. 2pts (1 pt pour l'agrébricité, et 1 pt pour la séparabilité)
5. 6pts : 2 pts pour montrer que les sous-extension simples ont un degré inférieur ou égal à Card(G), 3 pts pour l'argument principal (chaque sous-extension est simple, et conclude par l'absurde que $[L : K] < \infty$), et 1 pt pour conclure

Exercice 2 [**18 pts**]

Considérons la situation suivante :

- A est un anneau factoriel,
- K est le corps des fractions de A,
- f et g sont des polynômes primitifs non-nuls dans $A[x]$,
- $h \in A[x]$ et $c \in K$ des éléments arbitraires.

Dans cette situation :

(1) Démontrez le premier lemme de Gauss: $f \cdot g$ est aussi primitif.

(2) Démontrez le troisième lemme de Gauss: f est irréductible dans $A[x]$ si et seulement si f est irréductible dans $K[x]$.

Vous pouvez utiliser sans preuve le deuxième lemme de Gauss: si $h = cf$, alors $c \in A$, et de plus si h est aussi primitif, alors $c \in A^\times$.

(3) Soit F un corps. Démontrez que $y^3 - x^a \in F[x, y]$ est irréductible pour chaque entier $3 \nmid a > 0$.

Vous pouvez utiliser sans preuve que $F[x]$ est factoriel.

Solution:

Les deux premiers points consistaient à redémontrer des propositions du cours.

1. Par l'absurde, $f \cdot g$ n'est pas primitif et donc il existe $p \in A$ irréductible tel que $fg = 0 \mod p$ Alors f ou g est nul $\mod p$ car comme A est factoriel p et premier, et cela donne une contradiction sur le caractère primitif de f et de g.

   On peut aussi raisonner sur les coefficients. Soit p un premier qui divise tout les coefficients de fg. Soient k et l minimaux pour que p ne divise pas le k-ième coefficient de f et le l-ième coefficient de g qui existent par primitivité. On obtient alors une contradiction avec le coefficient de degré $k + l$ de fg qui n'est alors pas divisible par g.

2. On commence par supposer que f est irréductible dans $K[t]$ et on montrer que f est irréductible dans $A[t]$. Écrivons $f = gh$ pour $g, h \in A[t]$. On peut écrire $g = c_0 g_0$ et $h = d_0 h_0$ pour $c_0, d_0 \in A$ et h_0, g_0 primitifs. Alors par la remarque de l'énoncé on peut supposer pour montrer que f est irréductible que $f = gh$ avec g et h primitifs. En utilisant l'irréductibilité dans $K[t]$, on obtient que f ou g sont des constantes. Une constante primitive étant inversible, on obtient que f est irréductible.

   Ensuite on suppose que f est irréductible dans $A[t]$. Soit $g, h \in K[t]$ avec $f = gh$. Soit $c_0, d_0 \in K$ et $g_0, h_0 \in A[t]$ primitifs tels que $g = c_0 g_0$ et $h = d_0 h_0$. Avec le point 1 de l'exercice, on a que $g_0 h_0$ est primitif. Dès lors avec la remarque dans l'énoncé, on obtient que $c_0 d_0 \in A^\times$. Alors on obtient que g_0 ou f_0 est inversible, donc une constante, ce qui montre que f ou g est inversible dans $K[t]$.

3. En utilisant le point précédent, il suffit de montrer que $y^3 - x^a$ est irréductible dans $K(x)[y]$. Ainsi, comme c'est un polynôme de degré 3, il suffit de montrer que ce polynôme n'as pas de racines dans $K(x)$. Soit par l'absurde $\frac{f(x)}{g(x)}$ une racine. Alors

$$f(x)^3 = x^a g(x)^3.$$

Alors $3\deg(f) = a + 3\deg(g)$, une contradiction en réduisant modulo 3 comme $3 \not| a$.

Barème.

1. 4pts : 1 pour dire explicitement que le minimum est bien défini (car les polynomes sont primitifs), et 3 pour le reste du calcul
2. 4pts pour "irreductible dans $K[x]$ implique irreductible dans $A[x]$ (dont 2 points pour faire remarquer que l'hypothèse de primitivité est importante), et 6pts pour l'autre implication (dont 2 pts pour dire explicitement que $c_0 d_0 \in A$).
3. 4pts (2 pts pour passer au corps des fractions, et 2 pts pour conclure avec les degrés)

Exercice 3 [**16 pts**]

Soit $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(1) Donnez une base $\mathbb{Q}$-linéaire de L qui contient 1, $\sqrt{2}$ et $\sqrt{3}$.

(2) Déterminez le groupe de Galois $G = \mathrm{Gal}(L, \mathbb{Q})$, et donnez l'action de chaque élément de G sur la base de point précédent.

(3) Pour chaque sous-groupe H de G déterminez le corps intermédiaire L^H correspondant à H. Donnez le sous la forme $\mathbb{Q}(\alpha)$.

Solution:

1. On prétend que $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ est une base. Comme $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$ (ce fait a été vu en exercice) on a $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 2$. Ainsi

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4$$

   De plus comme tout élément de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est de la forme pour $a_{i,j} \in \mathbb{Q}$

$$\sum_{i,j} a_{i,j} \left(\sqrt{2}\right)^i \left(\sqrt{3}\right)^j = \sum_{ij} b_{ij} \left(\sqrt{2}\right)^{\epsilon_i} \left(\sqrt{3}\right)^{\epsilon_j}$$

   avec ϵ_i, ϵ_j égaux à 0 or 1, on voit que la famille est génératrice.

2. Notons que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est Galoisienne sur $\mathbb{Q}$ car séparable (caractéristique zéro) et est le corps de décomposition de $(t^2 - 2)(t^2 - 3)$. Notons aussi que comme

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 2 \quad [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2,$$

   on a des automorphismes s, t de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ qui fixent $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$ respectivement avec $s(\sqrt{2}) = -\sqrt{2}$ et $t(\sqrt{3}) = -\sqrt{3}$, ces actions sont justifiés par la permutation des racines des polynômes minimaux $m_{\sqrt{2},\mathbb{Q}(\sqrt{3})} = t^2 - 2$ et $m_{\sqrt{3},\mathbb{Q}(\sqrt{2})} = t^2 - 3$. Ainsi les 4 éléments du groupe de Galois sont l'identité, s,t et st et l'action sur les éléments de la base non égaux à 1 est, pour les automorphismes non-triviaux est

   (a) $s(\sqrt{2}) = -\sqrt{2}$, $s(\sqrt{3}) = \sqrt{3}$, $s(\sqrt{6}) = -\sqrt{6}$.

   (b) $t(\sqrt{2}) = \sqrt{2}$, $t(\sqrt{3}) = -\sqrt{3}$, $t(\sqrt{6}) = -\sqrt{6}$.

   (c) $st(\sqrt{2}) = -\sqrt{2}$, $st(\sqrt{3}) = -\sqrt{3}$, $st(\sqrt{6}) = \sqrt{6}$.

3. Notons que les éléments x non égaux à 1 de la base sont de degré 2 car $t^2 - x^2$ est leur polynôme minimal sur $\mathbb{Q}$. Notons que $\sqrt{2} + \sqrt{3}$ n'est fixé par aucun automorphisme non trivial donc ne peut pas appartenir à une sous-extension propre. Rappelons aussi que le degré de l'extension correspondant à un sous-groupe est l'indice du sous-groupe. En utilisant ces informations, ainsi que la correspondance de Galois et le point précédent on obtient,

   - $\mathbb{Q}(\sqrt{2}, \sqrt{3})^G = \mathbb{Q}$. *1pts*
   - $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle s \rangle} = \mathbb{Q}(\sqrt{3})$. *1pts*
   - $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle t \rangle} = \mathbb{Q}(\sqrt{2})$. *1pts*
   - $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle st \rangle} = \mathbb{Q}(\sqrt{6})$. *1pts*
   - $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. *1pts*

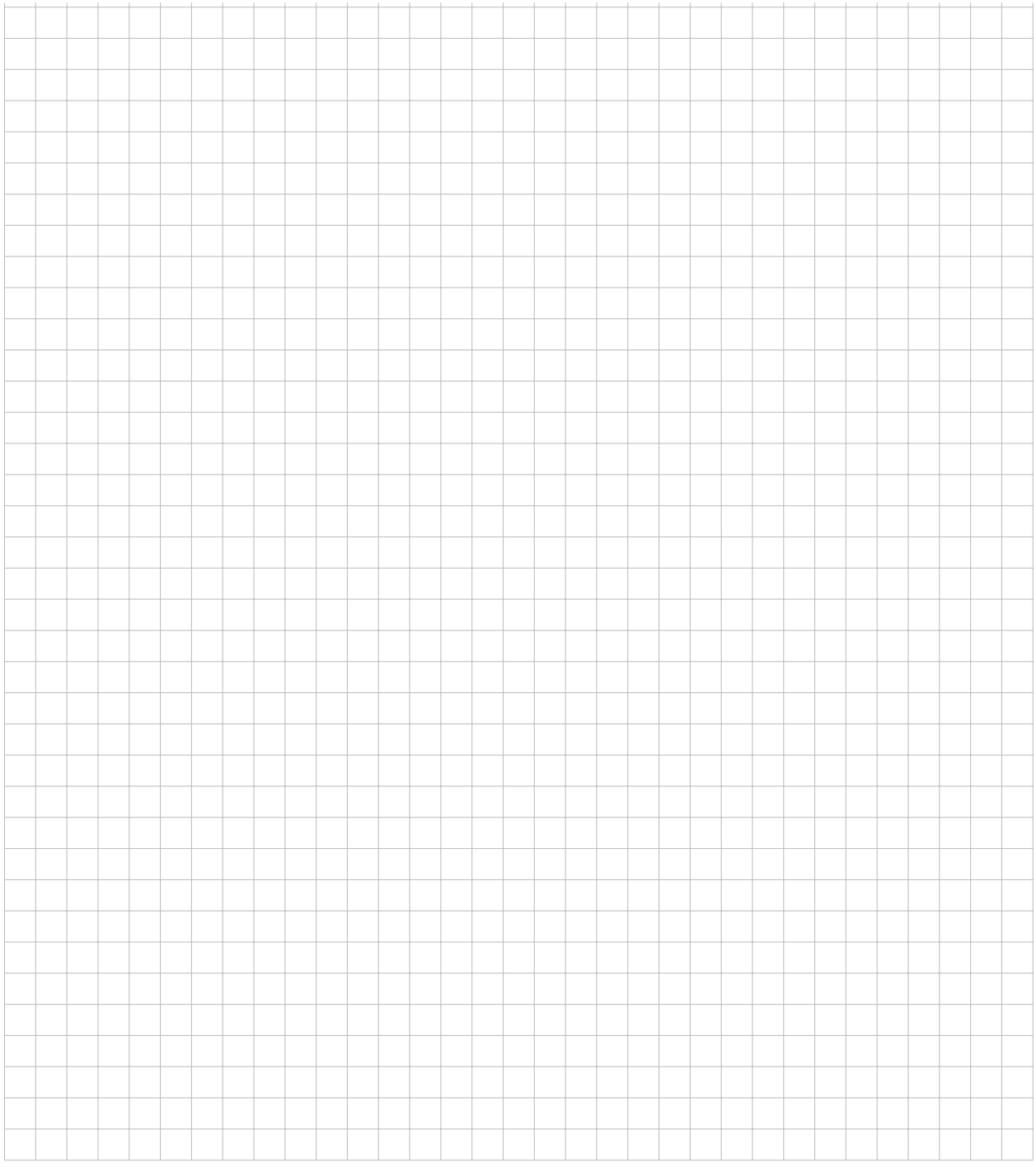
Barème.

1. 5pts : 2pts pour une base correcte, 3pts pour la justification que c'est une base.

2. 6pts : 2pts pour justifier que l'extension est Galoisienne. 2pts pour une construction correcte de s et t. 2pts pour une expression correcte de l'action des automorphismes sur la base.

3. 5pts. Voir détail ci-dessus. Il ne suffit pas d'écrire ces égalités, il faut aussi argumenter correctement pour les justifier.

   À noter que peu importe la manière de procéder, il faut justifier le degré des extensions propres et le degré des éléments pour par exemple montrer que l'inclusion évidente $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3},\sqrt{2})^{\langle s \rangle}$ *est une égalité. (Ou autre argument). Il faut aussi un argument pour justifier* $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.



Exercice 4 [**18 pts**]

Soit $p > 2$ un entier premier.

(1) Démontrez que $\mathbb{Z}[i]\Big/(p) \cong \mathbb{F}_p[t]\Big/(t^2+1)$.

(2) Démontrez que $t^2+1 \in \mathbb{F}_p[t]$ est irréductible si et seulement si $p \not\equiv 1 \mod 4$.

(3) Démontrez que

$$\mathbb{Z}[i]\Big/(p) \cong \begin{cases} \mathbb{F}_{p^2} & \text{, si } p \not\equiv 1 \mod 4 \\ \mathbb{F}_p \times \mathbb{F}_p & \text{, si } p \equiv 1 \mod 4 \end{cases}$$

Solution:

1. *On peut assumer que*

$$\mathbb{Z}[t]/(t^2+1) \cong \mathbb{Z}[i]$$

qui a été vu en cours dans un exemple. On peut ensuite le "théorème du quotient en deux temps" pour conclure.

2. On procède par suite d'équivalences. (On rappelle que $p > 2$).

$t^2+1 \in \mathbb{F}_p[t]$ est irréductible
$\overset{1pt}{\iff}$ t^2+1 n'a pas de racines dans $\mathbb{F}_p$
$\overset{1pt}{\iff}$ Il n'existe pas de $\alpha \in \mathbb{F}_p$ tel que $\alpha^2 = -1$
$\overset{2pts}{\iff}$ Il n'existe pas d'élément de $\mathbb{F}_p^\times$ d'ordre 4. (l'équivalence ci-dessus utilise $p > 2$)
$\overset{1pt}{\iff}$ Il n'existe pas d'élément de $\mathbb{Z}/(p-1)\mathbb{Z}$ d'ordre 4
$\overset{1pt}{\iff}$ $4 \not| p-1$
$\iff$ $p \not\equiv 1 \mod 4$.

3. Si $p \not\equiv 1 \mod 4$, par le point précédent, t^2+1 est irréductible. Alors avec le point (1), on obtient que $\mathbb{Z}[i]/(p)$ est isomorphe à $\mathbb{F}_{p^2}$ en utilisant qu'alors $\mathbb{F}_p[t]/(t^2+1)$ est un corps et un $\mathbb{F}_p$-espace vectoriel de dimension 2, donc de taille p^2 et le théorème de classification des corps finis.

   Donc l'autre cas, on a qu'il existe un $\alpha \in \mathbb{F}_p$ avec $t^2+1 = (t-\alpha)(t+\alpha)$. Ainsi, en utilisant le théorème des restes chinois et l'évaluation en α et $-\alpha$, on conclut.

Barème.

1. 4pts
2. 6pts (Voir détail au-dessus)
3. 8pts : 4pts pour chaque direction

Exercice 5 [**14 pts**]

Fixons un entier premier $p > 0$ et considérons le sous-anneau suivant de l'anneau de matrices 2×2 sur $\mathbb{F}_p$:

$$A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{F}_p \right\}$$

Rappelons que la loi de la multiplication est:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} e & f \\ 0 & g \end{pmatrix} = \begin{pmatrix} ae & af + bg \\ 0 & cg \end{pmatrix}$$

(1) Combien d'éléments idempotents A contient-il?

Rappelons que $d \in A$ est idempotent par définition si et seulement si $d^2 = d$.

(2) Est-ce que l'on peut écrire $A \cong B \times C$ pour des anneaux B et C non-nuls?

Solution:

1. Notons tout d'abord qu'un élément est idempotent si et seulement si $a = a^2$ et $c = c^2$ et $b = ab + bc = b(a + c)$.

   - Si $b = 0$ alors $a, c = 1, 0$ sont possibles donc il y a 4 possibilités dans ce cas.
   - Si $b \neq 0$ alors $a = 1 - c$. On a donc 2 possibilités pour a et c et n'importe quel $b \neq 0$ est possible. Alors on a $2(p - 1)$ possibilités.

   Ainsi on compte $4 + 2(p - 1) = 2 + 2p$ idempotents.

2. On commence par utiliser le théorème qui affirme qu'un anneau est un produit d'anneaux non-nuls si et seulement s'il existe des idempotents centraux non-nuls e, f tels que $e+f = 1$ et $ef = 0$.

   En particulier, si A est un produit d'anneaux non-nuls il doit y exister deux idempotents centraux non-nuls. Soit $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in A$ central. Comme,

   $$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},$$

   on voit que nécessairement $b = 0$. Notons également que comme[1]

   $$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

   ainsi que,

   $$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

   on peut conclure qu'il existe un unique idempotent central non-nul, l'identité. Ainsi, A n'est pas le produit de deux anneaux non-nuls.

Barème.

1. 6pts. 3+3 pour chacun des cas comme traités ici.

[1] Ce calcul permet déjà de conclure sans même affirmer que $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ n'est également pas central car les deux seules possibilités restantes ont un produit non-nul (et ne somment pas à l'identité).

2. 3 pts pour faire appel au théorème qui caractérise les produits avec des idempotents centraux. 5 pts pour argumenter qu'il n'y en pas assez ou tout autre méthode correcte qui amène au résultat. Il y a ici certainement de nombreuses méthodes pour s'en sortir.

Exercice 6 [**18 pts**]

Soit $7 \neq p > 0$ un entier premier.

(1) Démontrez que pour un entier $n > 0$ quelconque $\mathbb{F}_{p^n}$ contient une racine primitive 7-ième d'unité, c'est à dire un élément α tel que $\alpha^7 = 1$ et $\alpha \neq 1$, si et seulement si $p^n \equiv 1 \mod 7$.

Démontrez de plus, que dans ce cas $\mathbb{F}_{p^n}$ contient exactement 6 tels éléments.

(2) Supposons que $p + 7\mathbb{Z} \in \left(\mathbb{Z}/7\mathbb{Z}\right)^\times$ est un générateur du groupe $\left(\mathbb{Z}/7\mathbb{Z}\right)^\times$. Par exemple, $p = 3$ ou $p = 5$. Démontrez que

$$\mathbb{F}_{p^6} \cong {}^{\mathbb{F}_p[x]}\Big/(1 + x + x^2 + x^3 + x^4 + x^5 + x^6).$$

(3) Supposons maintenant que $p+7\mathbb{Z} \in \left(\mathbb{Z}/7\mathbb{Z}\right)^\times$ n'est pas un générateur du groupe $\left(\mathbb{Z}/7\mathbb{Z}\right)^\times$. Par exemple, $p = 13$ ou $p = 23$. Démontrez que

$$\mathbb{F}_p[x]\Big/(1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$$

n'est pas intègre en tant qu'anneau.

Solution:

1. Comme $\mathbb{F}_{p^n}^\times \cong \mathbb{Z}/(p^n - 1)\mathbb{Z}$ et que dans un groupe cyclique fini A il existe un élément non-trivial $a \in A$ tel que $a^7 = 1$ si et seulement si $7|\mathrm{Card}(A)$, on obtient qu'il existe $\alpha \neq 1$ avec $\alpha^7 = 1$ dans $\mathbb{F}_{p^n}$ si et seulement si $7|p^n - 1$ donc si et seulement si $p^n \equiv 1 \mod 7$. Dans ce cas, comme on sait qu'il existe un unique sous-groupe de cardinal 7 avec 6 éléments non-triviaux dans un groupe cyclique fini dont 7 divise le cardinal, on conclut qu'il y a exactement 6 éléments qui satisfont à la propriété demandée.

   On peut aussi voir que comme $p \neq 7$ le polynôme $x^7 - 1$ a des racines distinctes dans son corps de décomposition. On voit cela en dérivant le polynôme.

2. Notons $\alpha = \alpha_1, \ldots, \alpha_6$ les racines 7-ièmes non égales à 1 dans le corps de décomposition L de $x^7 - 1$ sur $\mathbb{F}_p$.

   Comme $x^7 - 1 = (x-1)(x^6 + x^5 + \cdots + 1)^2$ On obtient que $\alpha = \alpha_1, \ldots, \alpha_6$ sont les racines de $x^6 + x^5 \cdots + 1$. Rappelons que le groupe de Galois de L sur $\mathbb{F}_p$ est généré par la morphisme "mettre à la puissance p", qu'on notera F. Dès lors, F agit sur le sous-groupe cyclique multiplicatif généré par α dans $L^\times$ comme la multiplication par p si on identifie $(\langle\alpha\rangle, \cdot)$ à $(\mathbb{Z}/7\mathbb{Z}, +)$. Si on suppose comme on le fait dans ce point que la multiplication par p est un générateur des automorphismes de $\mathbb{Z}/7\mathbb{Z}$, on obtient que les 6 automorphismes de $(\langle\alpha\rangle, \cdot)$, qui sont caractérisés par $\alpha \mapsto \alpha_i$ pour $i = 1, \ldots 6$, peuvent s'obtenir comme F^j pour un certain entier j. Dès lors, on voit que $\{\alpha_1, \ldots, \alpha_6\}$ est l'orbite de α par F. Dès lors, il suit que $x^6 + x^5 + \cdots + 1$ est le polynôme minimal de α sur $\mathbb{F}_p$. Alors, étant irréductible de degré 6 dans $\mathbb{F}_p[t]$, on conclut à l'isomorphisme de l'énoncé en invoquant la classification des corps finis.

   On peut aussi argumenter avec l'idée suivante : comme 6 est le plus petit entier tel que $p^6 \equiv 1 \mod 7$, alors si α racine primitive 7-ième de l'unité on a par le point 1, $\alpha \in \mathbb{F}_{p^6}$ mais dans aucun sous-corps. Ainsi le degré de α est 6, ce qui donne 'irréductibilité du polynôme voulu.

[2] Cette division euclidienne a été vue en cours et en exercice et ne pas la justifier est accepté.

3. Par l'argument précédent, on voit que l'ordre de $p + 7\mathbb{Z}$ dans $(\mathbb{Z}/7\mathbb{Z})^\times$ correspond à la taille de l'orbite de α par F, c'est à dire au degré de son polynôme minimal sur $\mathbb{F}_p$. Si celui-ci est strictement inférieur à 6, comme on le suppose dans ce point, on a lors une décomposition
$$x^6 + x^5 + \cdots + 1 = m_{\alpha,\mathbb{F}_p} g$$
pour g un polynôme non-constant premier avec $m_{\alpha,\mathbb{F}_p}$. Ainsi, l'idéal $(x^6 + \cdots + 1)$ n'est pas premier, ce qui conclut.

   On peut aussi argumenter qu'il existe dès lors que pour un $n < 6$ on a $p^n \equiv 1 \mod 7$ et donc que par le point 1, on peut conclure que le degré de α sur $\mathbb{F}_p$ est strictement plus petit que 6 ce qui démontre que le polynôme en question n'est pas irréductible.

Barème.

1. 2 points par implication, 1 point pour montrer qu'il y en a exactement 6.
2. 2 points pour comprendre que $x^6 + \cdots + x + 1$ annule une racine primitive 7-ième, ou mentionner $(x-1)(x^6 + x^5 + \cdots + x + 1)$, ce qui montre que le lien entre ce polynôme et les racines de l'unité est compris. 4 points pour utiliser correctement l'hypothèse $p + 7\mathbb{Z}$ générateur. 2 points pour invoquer la classification des corps finis, plus précisément pour dire que $\mathbb{F}_p[x]/(f)$ pour f irréductible de degré 6 est isomorphe à $\mathbb{F}_{p^6}$.
3. 2 points pour comprendre qu'il faut montrer que le polynôme n'est pas irréductible. 3 points pour utiliser correctement l'hypothèse et conclure.