Anneaux et corps (MATH-215) — Examen final

20 juin 2022, 15 h 15 – 18 h 15

Nom : Grothendieck Alexander

SCIPER : 42

Signature : _____

Numéro
1

Ce dossier d'examen contient 5 exercices, sur 28 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	Total
Points:	30	18	10	24	18	100
Score:						

Exercice 1 [**30 pts**]

(1) Énoncez et démontrez le critère d'Eisenstein sur l'irréductibilité d'un polynôme $f \in A[x]$, où A est un anneau factoriel.

(2) Démontrez que pour chaque entier (positif) premier p, le polynôme $x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Z}[x]$ est irréductible.

(3) Démontrez que $\left[\mathbb{Q}\left(e^{\frac{2\pi i}{p}}\right) : \mathbb{Q}\right] = p - 1$.

(4) Démontrez que $\mathrm{Gal}\left(\mathbb{Q}\left(e^{\frac{2\pi i}{p}}\right)/\mathbb{Q}\right) \cong \mathbb{F}_p^\times$.

Solution:

1. 10 points **Proposition:** Soit A un anneau factoriel, $p \in A$ un irréductible, et $f = \sum_{i=0}^{n} a_i t^i \in A[t]$ un polynôme primitif de degré n. Si

   (a) $p \nmid a_n$

   (b) pour chaque $0 \leq i < n$ on a $p | a_i$, et

   (c) $p^2 \nmid a_0$,

   alors f est irréductible.

   3 pt **Démonstration:** Prenons une décomposition $f = gh$, et utilisons la notation

   $$g = \sum_{i=0}^{k} b_i t^i \qquad \text{et} \qquad h = \sum_{j=0}^{m} c_j t^j.$$

   où $b_k \neq 0 \neq c_m$. De coup, on a $a_0 = b_0 \cdot c_0$. Par condition item 1b et item 1c, on a $p | b_0$ ou $p | c_0$. Par symétrie on peut supposer que cela soit c_0. Par condition item 1c, on obtient que dans ce cas p ne divise pas b_0 2 pt. De plus comme $a_n = b_k c_m$, par condition item 1a, on obtient que $p \nmid c_m$. Par conséquent le minimum suivant existe

   $$r = \min\left\{ j \in \mathbb{N} \;\middle|\; p \nmid c_j \right\} \quad 2pt.$$

   Observons que

   $$a_r = \underbrace{b_0 \cdot c_r}_{\uparrow} + \sum_{i=1}^{r} \underbrace{b_i \cdot c_{r-i}}_{\uparrow}$$

   $\boxed{p \nmid b_0, p \nmid c_r \implies p \nmid b_0 c_r}$ $\boxed{1 \leq i \leq r \implies p | b_i \implies p | b_i c_{r-i}}$

   n'est pas divisible par p 2 pt. Ainsi, par condition item 1b on obtient que $r = n$. Par **??** cela nous dit que $\deg h = 0$. Puisque f est primitif, cela implique que $h \in A^\times$ 1 pt.

2. 10 points

   On déduite de la **??** que $f = t^{p-1} + \ldots + t + 1 \in \mathbb{Z}[t]$ est irréductible, où $p \in \mathbb{N}$ premier. Pour cela observons que $t^p - 1 = (t-1)f$ 2 pt. Considérons l'homomorphisme $\mathrm{ev}_{y+1} : \mathbb{Z}[t] \to \mathbb{Z}[y]$. C'est un isomorphism, parce que $\mathrm{ev}_{t-1} : \mathbb{Z}[y] \to \mathbb{Z}[t]$ donne l'inverse homomorphisme. Ainsi, puisque être irréductible est préservé par les automorphismes d'anneau, il suffit de démontrer que le polynôme $\mathrm{ev}_{y+1}(f)$ est irréductible 2 pt. Notons

que

$$\sum_{i=1}^{p}\binom{p}{i}y^i = (y+1)^p - 1 = \mathrm{ev}_{y+1}(t^p-1) \underset{\uparrow}{=} \mathrm{ev}_{y+1}(t-1)\cdot\mathrm{ev}_{y+1}(f) = y\cdot\mathrm{ev}_{y+1}(f) \quad 2pt$$

ev_{y+1} est un homomorphisme d'anneau

$$\implies \mathrm{ev}_{y+1}(f) = \sum_{i=0}^{p-1}\binom{p}{i+1}y^i = y^{p-1} + \left(\sum_{i=1}^{p-2}\underbrace{\frac{p!}{(i+1)!(p-i-1)!}}_{\uparrow}y^i\right) + p \quad 2pt$$

$1 \le i \le p-2 \implies p \nmid (i+1)!$, et $p \nmid (p-i-1)! \implies p \left| \frac{p!}{(i+1)!(p-i-1)!} \right.$

On voit que les conditions de **??** sont satisfaites pour $\mathrm{ev}_{y+1}(f)$, et par conséquent $f \in \mathbb{Z}[t]$ est irréductible 2 pt.

3. 5 points

   Le polynôme $f = \frac{t^p-1}{t-1} = t^{p-1} + \ldots + t + 1 \in \mathbb{Z}[t]$ est irréductible par le point précédent, et il est aussi primitif. Donc par Gauss III, il est irréductible en tant que polynôme sur $\mathbb{Q}$ 2 pt. De plus il s'annnule en $e^{\frac{2\pi i}{p}}$, donc il est le polynôme minimal de $e^{\frac{2\pi i}{p}}$ sur $\mathbb{Q}$ 2 pt, ce qui implique l'affirmation de ce point 1 pt.

4. 5 points Notons $\xi = e^{\frac{2\pi i}{p}}$. Puisque ξ^j est aussi une racie de f pour chaque $1 \le j \le p-1$ 2 pt, on voit que $L = \mathbb{Q}\left(e^{\frac{2\pi i}{p}}\right)$ est le corps de décomposition de f sur $\mathbb{Q}$ 3 pt.

Exercice 2 [**18 pts**]

Soit $K \subseteq L$ une extension de corps.

(1) Définissez quand $K \subseteq L$ est une extension galoisienne. (Vous pouvez utiliser sans la définir la notion de groupe de Galois.)

Supposons pour le reste de l'exercice que $K = L^G$ pour un groupe fini $G \subseteq \mathrm{Aut}(L)$.

(2) Donnez et démontrez l'expression du polynôme minimal sur K d'un élément $\alpha \in L$, en terme de l'orbite de α par l'action de G.

(3) Démontrez que $[L : K] < \infty$.

Solution:

1. 4 points **Définition:**

   Une extension de corps $K \subseteq L$ est *galoisienne* si elle est algébrique 2 pt et $L^{\mathrm{Gal}(L/K)} = K$ 2 pt.

2. 7 points

   Proposition:

   $m_{\alpha,K} = \prod_{i=1}^{r}(x - \alpha_i)$, où $\{\alpha = \alpha_1, \ldots, \alpha_r\}$ est l'orbite de α. 1 pt

   Démonstration:

   Soit $f = \prod_{i=1}^{r}(x - \alpha_i)$. Premièrement on démontre que $f \in K[x]$: Cela découle de la supposition $K = L^G$ par l'argument suivant. Fixons $\sigma \in G$ et soit $\xi : L[x] \to L[x]$ l'homomorphisme induit par $\sigma : L \to L$. Puisque σ permute les α_i, ou autrement dit il envoie α_i sur $\alpha_{\pi(i)}$ pour un $\pi \in S_r$, on obtient que :

   $$\xi(f) = \xi\left(\prod_{i=1}^{r}(x - \alpha_i)\right) \underset{\uparrow}{=} \prod_{i=1}^{r}\xi\left(x - \alpha_i\right) = \prod_{i=1}^{r}(x - \sigma(\alpha_i)) = \prod_{i=1}^{r}(x - \alpha_{\pi(i)}) \underset{\uparrow}{=} f \quad 2pt.$$

   ξ est un homomorphisme

   les $\alpha_{\pi(i)}$ sont les mêmes que les α_i juste ordonnés différémment

   Puisque cela est vrai pour chaque $\sigma \in \mathrm{Gal}(L/K)$ et $L^G = K$, on obtient que $f \in K[x]$. Puisque $f \in K[x]$, et f s'annule en α, on a que $m_{\alpha,K} | f$ 2 pt.

   Dans l'autre direction, chaque α_i doivent être racines de $m_{\alpha,K}$, parce que pour chaque polynôme $g \in K[x]$ on connaît que des éléments de l'orbite galoisienne de chaque racine de g sont aussi racines de g. Cela montre que on a aussi $f | m_{\alpha,K}$ 2 pt.

3. 7 points

   Par la point précédent, $K \subseteq L$ est algébrique et séparable 2 pt. On démontre premièrement que elle est aussi une extension simple. Prenons

   $$K \subsetneq K_1 = K(\alpha_1) \subsetneq \cdots \subsetneq K_n = K(\alpha_1, \ldots, \alpha_n) \subsetneq \ldots \quad 1pt \tag{1}$$

   On démontre que cette chaine stabilise. Par le théorème de l'élément primitif, $K \subseteq K_i$ est un extension simple pour chaque entier $i \geq 1$. Notons que ici on utilise la séparabilité de $K \subseteq L$ donnée par le point précédent. Avoir démontré la simplicité de $K \subseteq K_i$, le point précédent implique $[K_i : K] \big| |G|$, dont on en déduit que Equation 1 stabilise. Cela veut dire que l'on a $L = K_m$ 2 pt. Puisque on a déjà démontré que $[K_m : K] \big| |G|$ on obtient que $[L : K]$ est fini 2 pt.

Exercice 3 [**10 pts**]

Notons $\mathcal{C} := C^0([0,1];\mathbb{R})$ l'anneau des fonctions réelles continues sur l'intervalle $[0,1]$ (muni des opérations d'addition et de multiplication de fonctions). Pour chaque $x \in [0,1]$ définissons

$$I_x := \{\ f \in \mathcal{C} \mid f(x) = 0\ \}.$$

Vous pouvez utiliser sans preuve que I_x est un idéal maximal de $\mathcal{C}$.

(1) Soit $I \subset \mathcal{C}$ un idéal tel que I n'est contenu dans aucun des I_x. Montrez que $I = \mathcal{C}$.
Vous pouvez utiliser que $[0,1]$ *est compact, c'est-à-dire que chaque recouvrement ouvert de* $[0,1]$ *contient un recouvrement fini.*

(2) Montrez que tout idéal maximal de $\mathcal{C}$ est égal à I_x pour un certain $x \in [0,1]$.

Solution:

1. 7 points Pour chaque $x \in [0,1]$, par hypothèse il existe $0 \neq f_x \in I$ tel que $f_x(x) \neq 0$. 1 point Puisque f_x est continue, l'ensemble $\mathcal{U}_x := \{y \in [0,1] \mid f_x(y) \neq 0\}$ est ouvert (dans la topologie euclidienne de $[0,1]$) et contient x. 1 point Ainsi

$$[0,1] = \bigcup_{x\in[0,1]} \mathcal{U}_x. \quad 1point$$

Puisque la topologie euclidienne fait de $[0,1]$ un espace compact, la propriété de Heine–Borel implique qu'il existe $x_1, \ldots, x_n \in [0,1]$ tels que

$$[0,1] = \bigcup_{i=1}^{n} \mathcal{U}_{x_i} \quad 1point.$$

Considérons maintenant la fonction continue

$$F := \sum_{i=1}^{n} f_{x_i}^2 \quad 1point.$$

Alors $F \in I$ et par construction F est strictement positive sur $[0,1]$ 1 point. Ainsi $1/F \in \mathcal{C}$, et $1 = F \cdot 1/F \in I$. Donc $I = \mathcal{C}$ 1 point.

2. 3 point Soit $I \subset \mathcal{C}$ un idéal maximal. En vertu du point précédent, puisque $I \neq \mathcal{C}$ il existe un I_x tel que $I \subseteq I_x$ 2 point. Puisque I est maximal, on en déduit que $I = I_x$ 1 point.

Exercice 4 [**24 pts**]

Considérons $K = \mathbb{Q}$ et $L = \mathbb{Q}\big[i, \sqrt{2}\big]$. Un élément $\alpha \in L$ s'écrit de manière unique

$$\alpha = a + bi + c\sqrt{2} + di\sqrt{2}$$

avec $a, b, c, d \in \mathbb{Q}$ (vous pouvez utiliser cette affirmation sans preuve). Fixons un élément $\alpha \in L$.

(1) Démontrez que $\deg m_{\alpha,K} \in \{1, 2, 4\}$.

(2) Démontrez que pour $G = \mathrm{Gal}(L/K)$ on a $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(3) Donnez des conditions nécessaires et suffisantes sur les coefficients a, b, c et d pour que $\deg m_{\alpha,K} = 1$, respectivement $\deg m_{\alpha,K} = 2$, respectivement $\deg m_{\alpha,K} = 4$. Démontrez votre réponse (comme toujours) .

Solution :

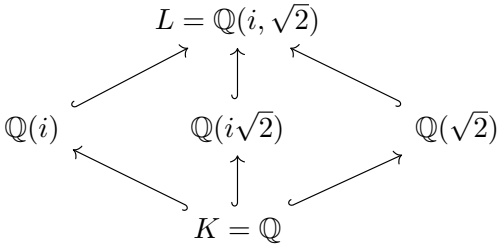
1. 3 points. – Par la donnée, on a $\dim_K L = [L : K] = 4$ (1 point). On sait aussi que $\deg m_{\alpha,K} = [K(\alpha) : K]$ (1 point). Puisque $K \subset K(\alpha) \subset L$ on voit par la multiplicativité des degrés que $[K(\alpha) : K]$ divise $[L : K] = 4$ (1 point). D'où $\deg m_{\alpha,K} \in \{1, 2, 4\}$.

2. 6 points. – On a $m_{i,K} = x^2 + 1$ et $m_{\sqrt{2},K} = x^2 - 2$. Donc on obtient un morphisme de groupes
$$\varphi\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Bij}(\{i, -i\}) \times \mathrm{Bij}(\{\sqrt{2}, -\sqrt{2}\})$$
qui est injectif puisque $L = K(i, \sqrt{2})$. 2 points (l'injection n'a pas besoin d'être explicite : il suffit d'expliquer qu'il y a au plus 4 automorphismes).

   Puisque L contient toutes les racines de $(x^2 + 1)(x^2 - 2) \in K[x]$, c'est un corps de décomposition d'un polynôme sur K. De plus toutes les racines sont distinctes. Ainsi L/K est une extension de Galois (2 points), et il s'ensuit que
$$|\mathrm{Gal}(L/K)| = [L : K] = 4.$$
   Puisque $\mathrm{Bij}(\{i, -i\}) \times \mathrm{Bij}(\{\sqrt{2}, -\sqrt{2}\})$ est d'ordre 4, on obtient que φ est une bijection, et donc un isomorphisme de groupes. Puisque $\mathrm{Bij}(\{i, -i\}) \times \mathrm{Bij}(\{\sqrt{2}, -\sqrt{2}\}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (2 points), on conclut.

   Alternative : On peut écrire explicitement 4 automorphismes de L/K, ce qui conclut directement. Dans ce cas : 4 points pour identifier les automorphismes (seulement 3 s'il n'est pas justifié que ce sont bien des morphismes), et 2 points pour la structure de groupe.

3. 15 points. – Commençons par donner le treillis d'extensions intermédiaires de L/K. Par le théorème fondamental de la théorie Galois, ce treillis correspond au treillis des sous-groupes de $\mathrm{Gal}(L/K)$. Par le point précédent, il y a seulement trois sous-groupes non-triviaux (les deux facteurs et la diagonale), qui correspondent à $\mathrm{Stab}_{\mathrm{Gal}(L/K)}(i)$, à $\mathrm{Stab}_{\mathrm{Gal}(L/K)}(\sqrt{2})$ et à $\mathrm{Stab}_{\mathrm{Gal}(L/K)}(i\sqrt{2})$. Ainsi le treillis de sous-corps est



et chaque flèche est une extension de degré 2.

Fixons $\alpha \in L$. Puisque $\deg m_{\alpha,K} = [K(\alpha) : K]$, on a :

- $\deg m_{\alpha,K} = 1$ si et seulement si $\mathbb{Q}(\alpha) = \mathbb{Q}$.
- $\deg m_{\alpha,K} = 2$ si et seulement si : $\mathbb{Q}(\alpha) = \mathbb{Q}(i)$ ou $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2})$ ou $\mathbb{Q}(\alpha) = \mathbb{Q}(i\sqrt{2})$.
- $\deg m_{\alpha,K} = 4$ si et seulement si $\mathbb{Q}(\alpha) = \mathbb{Q}(i, \sqrt{2})$.

Ecrivons $\alpha = a + bi + c\sqrt{2} + di\sqrt{2}$ avec $a, b, c, d \in \mathbb{Q}$. On interprète les conditions précédentes en fonction des coefficients rationnels.

- $\mathbb{Q}(\alpha) = \mathbb{Q}$ si et seulement si $b = c = d = 0$.
- $\mathbb{Q}(\alpha) = \mathbb{Q}(i)$ si et seulement si $(c = d = 0, b \neq 0)$; $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2})$ si et seulement si $(b = d = 0, c \neq 0)$; $\mathbb{Q}(\alpha) = \mathbb{Q}(i\sqrt{2})$ si et seulement si $(b = c = 0, d \neq 0)$.
- En utilisant le tiers exclu, tous les autres cas correspondent à $\mathbb{Q}(\alpha) = \mathbb{Q}(i, \sqrt{2})$.

3 points pour chaque corps. S'il manque une condition $\neq 0$, enlever un point.

Exercice 5 [**18 pts**]

Considérons deux anneaux A et B (possiblement non-commutatifs), un idéal bilatère $I \subseteq A \times B$ et définissons

$$I_A = \{\, x \in A \mid (x,0) \in I \,\}, \qquad \text{et} \qquad I_B = \{\, y \in B \mid (0,y) \in I \,\}.$$

(1) Démontrez que I_A et I_B sont des idéaux bilatères dans A et B, respectivement.

(2) Démontrez que $I = I_A \times I_B$.

(3) Soit p un nombre entier (positif) premier. Listez tous les idéaux bilatères de $M_2(\mathbb{F}_p) \times \mathbb{F}_p$, où $M_2(\mathbb{F}_p)$ est l'anneau des matrices 2×2 à coefficients dans $\mathbb{F}_p$.

Solution :

1. Nous allons montrer que I_A est un idéal bilatère, la preuve pour I_B étant identique. Il faut montrer que I_A est stable par addition, et stable par multiplication avec un élément quelconque de A.

   - 3 points. Soient $x, y \in I_A$. Alors $(x,0),(y,0) \in I$ et puisque I est un idéal, on a $(x+y,0) = (x,0)+(y,0) \in I$ et donc $x+y \in I_A$.
   - 3 points. Soient $x \in I_A$ et $a \in A$. Alors

     $$(ax,0) = (a,0)(x,0) \in I, \quad (xa,0) = (x,0)(a,0) \in I$$

     puisque I est un idéal bilatère. Donc $ax, xa \in I_A$.

2. Montrons que $I = I_A \times I_B$ (en tant que sous-ensembles de $A \times B$) par double-inclusion.

   - 3 points. Prenons $x \in I_A$ et $y \in I_B$. Par définition $(x,0) \in I$ et $(0,y) \in I$. Puisque I est un idéal, on a $(x,y) = (x,0)+(0,y) \in I$. Cela montre que $I_A \times I_B \subseteq I$.
   - 3 points. Prenons $(a,b) \in I$. Alors

     $$(a,0) = (a,b)(1,0) \in I, \quad (0,b) = (a,b)(0,1) \in I$$

     puisque I est un idéal. Ainsi $a \in I_A$ et $b \in I_B$, ce qui implique que $(a,b) \in I_A \times I_B$. Il s'ensuit que $I \subseteq I_A \times I_B$.

3. Par les deux points précédents, si I est un idéal bilatère de $M_2(\mathbb{F}_p) \times \mathbb{F}_p$ alors il est de la forme $I' \times I''$, où I' est un idéal bilatère de $M_2(\mathbb{F}_p)$ et I'' est un idéal bilatère de $\mathbb{F}_p$.

   Inversément, il est immédiat qu'un tel produit $I' \times I'' \subseteq M_2(\mathbb{F}_p) \times \mathbb{F}_p$ est un idéal bilatère. Pas nécessaire d'être explicite dans la solution.

   Puisque $\mathbb{F}_p$ est un corps, ses seuls idéaux bilatères sont triviaux (3 points). On a vu en série d'exercices qu'il en est de même pour les anneaux $M_n(k)$ de matrices $n \times n$ à coefficients dans un corps k, donc en particulier pour $M_2(\mathbb{F}_p)$ (3 points).

   Ainsi, les idéaux bilatères de $M_2(\mathbb{F}_p) \times \mathbb{F}_p$ sont

   $$M_2(\mathbb{F}_p) \times \mathbb{F}_p, \quad M_2(\mathbb{F}_p) \times \{0\}, \quad \{0\} \times \mathbb{F}_p, \quad \{0\} \times \{0\}.$$