Anneaux et corps (MATH-215) — Examen final

23 juin 2023, 15 h 15 – 18 h 15

Nom : Grothendieck Alexander

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.

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.

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 $\mathbb{Q}(\alpha)$.

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

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

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?

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.