Anneaux et corps (MATH-215) — Examen final

20 juin 2024, 15 h 15 – 18 h 15

Ce dossier d'examen contient 5 exercices, sur 3 pages, pour un total de 100 points. Veuillez utiliser l'espace quadrillé de **l'autre livret** pour vos réponses. Informations et instructions importants sur cet autre livret:

- N'écrivez PAS dans la marge intérieure du livret.
- Le livret contient 32 pages. Il **n'est pas possible d'utiliser** plus que ce 32 pages pour votre réponse. Autrement dit, il n'est pas possible d'utiliser des pages additionnelles.
- Veuillez rédiger vos solutions sur le point de l'exercice correspondant. Si l'espace après la question correspondant ne suffit pas, utilisez l'espace restant après la solution d'un autre exercice. Dans ce cas, notez soigneusement où votre solution continue.

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]".

Exercice 1 $\left[\text{ 20 pts }\right]$

Soit A un anneau.

(a). Définissez quand un sous-ensemble $I \subseteq A$ est un idéal bilatère de A.

(b). Soit A un idéal bilatère. Donnez les opérations d'addition et de multiplication sur $A/I = \{\ a + I \mid a \in A\ \}$.

Ici, vous n'avez pas besoin de montrer que ces opérations sont bien définies

(c). Démontrez que la multiplication est bien définie sur A/I.

(d). Soit p un entier premier. Listez les sous-structures suivantes de $\mathbb{F}_{p^2}$, en comptant aussi les cas triviaux (donner un nombre total et une liste complète dans chaque cas):

(i) sous-groupes additifs,

(ii) idéaux (bilatères), et

(iii) sous-anneaux.

Exercice 2 $\left[\text{ 15 pts }\right]$

Calculez la décomposition en facteurs irréductibles des éléments suivants de $\mathbb{Z}\left[i\sqrt{2}\right]$:

(a). $1 + i\sqrt{2}$

(b). $2 - i\sqrt{2}$

(c). $3 + i\sqrt{2}$

(d). $4 + i\sqrt{2}$

Vous pouvez utiliser sans démonstration que $\mathbb{Z}\left[i\sqrt{2}\right]$ *est un anneau factoriel.*

Exercice 3 $\left[\text{ 20 pts }\right]$

Soit $f \in K[x]$ un polynôme, soit L le corps de décomposition de f sur K, et soit $\alpha \in L$ un élément avec polynôme minimal $m_{\alpha,K}$ sur K. Démontrez que $m_{\alpha,K}$ se scinde sur L et que $\mathrm{Gal}(L/K)$ agit transitivement sur les racines de $m_{\alpha,K}$.

Vous pouvez sans autre utiliser les théorèmes suivants:

Theorem *Soit $K \subseteq L = K(\alpha)$ une extension de corps engendrée par $\alpha \in L$, et soit $m_{\alpha,K}$ le polynôme minimal de α sur K. On a alors un isomorphisme $L \cong K[x]\big/(m_{\alpha,K})$ qui envoie α sur la classe de gauche de x et qui fixe K.*

Theorem *Soit $\phi\colon K \to K'$ un isomorphisme de corps, soit $f \in K[x]$ un polynôme, soit f' l'image de f par ϕ, et finalement soient respectivement L et L' les corps de décomposition de f et de f'. Dans ce cas, ϕ s'étend à un isomorphisme $\psi\colon L \to L'$.*

Exercice 4 $\left[\text{ 25 pts }\right]$

Soit $0 < n \in \mathbb{Z}$ un entier strictement positif, et soit $p \in \mathbb{Z}$ un nombre premier.

(a). Montrez que n est irréductible dans $\mathbb{Z}[i]$ si et seulement si n est premier dans $\mathbb{Z}$ et il n'existe pas $a, b \in \mathbb{Z}$ tel que $n = a^2 + b^2$.

(b). Montrez que $\mathbb{Z}[i]\big/(p) \cong \mathbb{F}_p[x]\big/(x^2 + 1)$.

(c). Montrez que p n'est pas premier dans $\mathbb{Z}[i]$ si et seulement si $p = 2$ ou $p \equiv 1 \mod 4$.

Exercice 5 [**20 pts**]

Soit K un corps de caractéristique différente de 2.

Dans votre solution vous pouvez utiliser sans preuve le théorème suivant: si $K \subseteq L$ est une extension de corps de degré 2, alors $L = K(\sqrt{c})$, où $\sqrt{c} \in L$ est un élément dont le carré est $c \in K$.

(a). Soit $K \subseteq L$ une extension de corps $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-galoisienne. Démontrez qu'il existent $c, d \in K$ tels que L est le corps de décomposition de $(x^2 - c)(x^2 - d)$ sur K.

(b). Soit $K \subseteq L$ une extension $S_3 \times \mathbb{Z}/2\mathbb{Z}$-galoisienne. Démontrez qu'il existe $c \in K$ et un polynôme irréductible $g(x) \in K[x]$ de degré 3 tel que L est le corps de décomposition de $g(x)(x^2 - c)$.