Anneaux et corps (MATH-215) — Examen final

20 juin 2024, 15 h 15 – 18 h 15

Ce dossier d'examen contient 5 exercices, sur 9 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 [**20 pts**]

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.

Solution:

(a). **3 points total** Un sous-ensemble $I \subseteq A$ est un idéal si par définition c'est un sous-groupe additif, et pour tous $a \in A$ et $i \in I$, on a $ai \in I$ et $ia \in I$.

(b). **2 points total** Soient $a + I, b + I \in A/I$. On définit alors

$$(a + I) + (b + I) \coloneqq (a + b) + I$$

et

$$(a + I) \cdot (b + I) \coloneqq (a \cdot b) + I.$$

(c). **3 points total** Soient $a, a', b, b' \in A$ tels que $a + I = a' + I$ et $b + I = b' + I$. Nous devons montrer que les éléments $ab + I$ et $a'b' + I$ sont égaux.

En d'autres termes, il faut montrer que si $a - a' \in I$ et $b - b' \in I$, alors $ab - a'b' \in I$. Or, on a

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b'.$$

Comme $b - b' \in I$ et que I est un idéal bilatère, alors $a(b - b') \in I$. De manière similaire, $(a - a')b \in I$ et donc leur somme est aussi dans I, i.e. $ab - a'b' \in I$.

(d). **12 points total**

(i) Premièrement, comprenons mieux la classe d'isomorphisme de $(\mathbb{F}_{p^2}, +)$.

Preuve 1 pour la classe d'isomorphisme: Vu que $\mathbb{F}_p \subseteq \mathbb{F}_{p^2}$ est une extension de degré 2, on a par définition que $\mathbb{F}_{p^2}$ est un $\mathbb{F}_p$-espace vectoriel de dimension 2. Autrement dit,

$$\mathbb{F}_{p^2} \cong \mathbb{F}_p \times \mathbb{F}_p.$$

Preuve 2 pour la classe d'isomorphisme: Notez tout d'abord que pour tout $a \in \mathbb{F}_{p^2}$, on a $p \cdot a = 0$. Autrement dit, tout élément de $\mathbb{F}_{p^2}$ est p-torsion. On sait par le théorème de classification des groupes abéliens que soit $(\mathbb{F}_{p^2}, +) \cong \mathbb{Z}/p^2\mathbb{Z}$, soit $(\mathbb{F}_{p^2}, +) \cong \mathbb{F}_p \times \mathbb{F}_p$. Or, vu que tout élément est de p-torsion, on exclut nécessairement le premier cas, et donc $\mathbb{F}_{p^2} \cong \mathbb{F}_p \times \mathbb{F}_p$.

On a donc montré qu'il faut comprendre les sous-groupes additifs de $\mathbb{F}_p \times \mathbb{F}_p$. Supposons que ce sous-groupe est non-trivial. Alors vu que son ordre divise p^2 mais n'est ni 1 ni p^2, il est forcément d'ordre p et donc cyclique (isomorphe à $\mathbb{Z}/p\mathbb{Z}$). Il suffit de lister les sous-groupes $\langle v \rangle$ avec $0 \neq v \in \mathbb{F}_p \times \mathbb{F}_p$.

Ecrivons $v = (v_1, v_2)$ (rappelons que $v_1 \neq 0$ ou $v_2 \neq 0$). Si $v_1 \neq 0$, alors il existe $a \in \mathbb{F}_p^\times$ tel que $av_1 = 1$, et donc

$$\langle v \rangle = \langle av \rangle = \langle (1, av_2) \rangle.$$

Montrons que si $x \neq y \in \mathbb{F}_p$, alors $\langle (1, x) \rangle \neq \langle (1, y) \rangle$.

Si $\langle (1, x) \rangle = \langle (1, y) \rangle$, alors il existe $b \in \mathbb{F}_p$ tel que

$$b(1, x) = (1, y).$$

Or, $b(1, x) = (b, bx)$ et donc cela impose $b = 1$, contredisant que $x = y$.

Ainsi, la liste des $\langle (v_1, v_2) \rangle$ avec $v_1 \neq 0$ est exactement

$$\{\langle (1, b) \rangle\}_{b \in \mathbb{F}_p}$$

Finalement, si $v_1 = 0$, alors $v_2 \neq 0$ et

$$\langle (v_1, v_2) \rangle = \langle (0, 1) \rangle.$$

On a donc une liste complète de nous sous-groupes (à travers l'isomorphisme de groupes additifs $\mathbb{F}_{p^2} \cong \mathbb{F}_p \times \mathbb{F}_p$):

- $\mathbb{F}_p \times \mathbb{F}_p$;
- $\{0\}$;
- les $\langle (1, b) \rangle$, avec $b \in \mathbb{F}_p$;
- $\langle (0, 1) \rangle$.

En particulier, cela fait $p + 3$ sous-groupes.

Preuve alternative. On sait qu'on a déjà 3 sous-groupes $0, \mathbb{F}_p, \mathbb{F}_{p^2}$. comme chaque élément non-nul du corps est d'ordre p, on a pour chaque $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ un sous groupe d'ordre p le sous-groupe additif généré par $\langle \alpha \rangle$. Comme deux sous-groupes distincts d'ordre p s'intersectent uniquement en zéro, et que $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ est de taille $p^2 - p = p(p-1)$ on voit donc qu'il y a p sous-groupes de cette forme. On déduit donc qu'il y a $p + 3$ sous-groupes.

Barème. On accorde 3 points pour lister les sous-groupes nul, total et $\mathbb{F}_p$. On accorde 4 points pour lister correctement les autres comme ci-dessus, cette étape étant le cœur de l'exercice.

(ii) Comme $\mathbb{F}_{p^2}$ est un corps, on sait par le cours que ses seuls idéaux sont (0) et $\mathbb{F}_{p^2}$. **Barème.** 2 points.

(iii) Si $A \subseteq \mathbb{F}_{p^2}$ est un sous-anneau, alors par définition A contient 1. Ainsi, il contient forcément $2, 3, \ldots, p-1$ et donc $\mathbb{F}_p \subseteq A$. Un sous-anneau est forcément un sous-groupe additif et donc de taille 1, p ou p^2. L'argument ci-dessus permet donc de conclure que $\mathbb{F}_p$ et $\mathbb{F}_{p^2}$ sont les deux sous-anneaux. On peut aussi argumenter que comme un sous-anneau sera intègre fini, il sera un corps. On peut alors faire appel au cours pour lister les sous-corps.

Encore une autre preuve avec de la théorie des corps, après avoir dit qu'un sous-anneau doit contenir $\mathbb{F}_p$ sans faire appel à l'ordre, on peut dire que s'il contient un élément hors de $\mathbb{F}_p$ celui-ci est de degré 2 et donc va engendré $\mathbb{F}_{p^2}$.

Barème. 3 points. On enlèvera un point pour l'erreur de considérer $\{0\} \subset A$ comme un sous-anneau, il ne contient pas l'unité multiplicative. Si on invoque le cours pour lister les sous-corps, sans expliquer pourquoi dans ce cas tout les sous-anneaux sont des corps (ou en expliquant faussement que tout sous-anneau d'un corps est un corps) 2/3. Si on invoque une liste erronée de sous-groupes pour conclure à une exhaustivité on impliquera un point de pénalité car c'est une erreur qui simplifie le problème.

Exercice 2 [15 pts]

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

(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 $\mathbb{Z}\big[i\sqrt{2}\big]$ est un anneau factoriel.

Solution:

Rappelons que pour $a+bi\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$, on pose $N(a+bi\sqrt{2}) = a^2+2b^2 \in \mathbb{Z}_{\geq 0}$. Cette opération est multiplicative.

Tout le long de l'exercice, nous utiliserons le fait vu en cours que pour tout $z \in \mathbb{Z}[i\sqrt{2}]$, z est inversible si et seulement si $N(z) = 1$.

(a). **3 points total** On a $N(1 + i\sqrt{2}) = 3$ qui est un nombre premier, donc si l'on avait une décomposition $1 + i\sqrt{2} = z_1 z_2$, nécessairement $N(z_i) = 1$ pour un $i \in \{1, 2\}$. Ainsi, l'un des z_i est automatiquement inversible, et donc on a prouvé que $1 + i\sqrt{2}$ est irréductible.

(b). **4 points total** On a $2 - i\sqrt{2} = (-i\sqrt{2}) \cdot (1 + i\sqrt{2})$. On a vu au point précédent que $1 + i\sqrt{2}$ était irréductible, et vu que $N(-i\sqrt{2}) = 2$ qui est premier, le même argument montre que $-i\sqrt{2}$ est aussi irréductible. Ainsi, on a trouvé la décomposition on facteurs irréductibles que l'on cherchait.

(c). **4 points total** On a $N(3 + i\sqrt{2}) = 11$ qui est premier, donc le même argument qu'au point 1 montre que cet élément est irréductible.

(d). **4 points total** On a $4 + i\sqrt{2} = (2 - i\sqrt{2})(1 + i\sqrt{2}) = (-i\sqrt{2})(1 + i\sqrt{2})^2$, et on a vu aux deux premiers points que les éléments $-i\sqrt{2}$ et $1 + i\sqrt{2}$ sont irréductibles. On a donc notre décomposition.

Grading scheme:

- Correct method and answer: maximum points
- Correct method but minor miscalculation: (maximum - 1) points
- Correct method but several/major miscalculations: (maximum - 2) points
- Correct answer but missing/incorrect justfication: 1 point

Exercice 3 [20 pts]

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 $\psi\colon L \to L'$.*

Solution:

Soit $F \supseteq K$ le corps de décomposition de $f \cdot m_{\alpha,K}$ sur L. Comme F contient en particulier un corps de décomposition de f, on obtient par unicité du corps de décomposition (qui suit directement du deuxième théorème cité dans la donnée) qu'il existe un plongement $L \hookrightarrow F$ de K-algèbres. Pour simplifier la notations, nous noterons l'image de cette injection par L.

Nous allons montrer que:

- $\mathrm{Gal}(F/K)$ agit transitivement sur les racines de $m_{\alpha,K}$;
- $F = L$,

et cela conclura donc la preuve. Pour le premier point, soient $a, b \in F$ deux racines de $m_{\alpha,K}$ dans K. Comme $m_{\alpha,K}$ est irréductible, on sait par le premier théorème de la donnée que l'on a un isomorphisme

$$K(a) \cong K[x]/(m_{\alpha,K}) \cong K(b)$$

en tant que K-algèbres (et donc K est fixé par cet isomorphisme), envoyant a sur b. Par le deuxième théorème appliqué au polynôme $f \cdot m_{\alpha,K}$, il existe un automorphisme $\theta\colon F \to F$ qui étende l'isomorphisme $K(a) \to K(b)$. En particulier, $\theta \in \mathrm{Gal}(F/K)$ et $\theta(a) = b$. On a donc montré que $\mathrm{Gal}(F/K)$ agit transitivement sur les racines de $m_{\alpha,K}$.

Montrons maintenant que $F = L$. Par définition, F est engendré sur K par les racines de f et de $m_{\alpha,K}$. Or, L contient les racines de f, et donc F est engendré sur L par les racines de $m_{\alpha,K}$. Soit β une de ces racines, et montrons que $\beta \in L$. Par ce que l'on a déjà montré, il existe $\sigma \in \mathrm{Gal}(F/K)$ tel que $\sigma(\alpha) = \beta$. Il suffit donc de montrer que $\sigma(L) \subseteq L$ pour conclure, car cela montrerait que $\beta \in L$.

Cela suit du fait que L est engenré par les racines de f, et que si σ agit sur les racines de f par le cours. Ainsi, on a bel et bien $\sigma(L) \subseteq L$, et donc $\beta \in L$. Ainsi, $m_{\alpha,K}$ se scinde sur L et donc $L = F$.

Grading scheme:

For full points, all the following steps must be included in the answer. Partial credit is given when only part of a step is included, or when insufficient justification is given.

- **2 points**: Consider the splitting field F of $f \cdot m_{\alpha,K}$ (or the splitting field of $m_{\alpha,K} \in L[x]$).
- **6 points**: Use the first provided theorem to show that $K(a) \cong K(b)$ for two roots a, b of $m_{\alpha,K}$ (or use corollary 4.23 in the lecture notes). Mention that this isomorphism fixes K.
- **6 points**: Apply the second provided theorem to extend the mentioned isomorphism to an isomorphism $\sigma\colon F \to F$. Conclude that $\mathrm{Gal}(F/K)$ (or $\mathrm{Gal}(L/K)$) acts transitively on the roots of $m_{\alpha,K}$.

- **6 points**: Show that $\sigma(L) \subseteq L$. Conclude that $F = L$, or otherwise conclude the problem.

In many answers, the last two points were done in another order: After constructing σ, one shows that $\sigma(L) \subseteq L \Rightarrow \sigma(L) = L$. One then uses the isomorphisms $\sigma|_L \colon L \to L$ to conclude that $m_{\alpha,K}$ splits in L and that $\mathrm{Gal}(L/K)$ acts transitively on the roots. This solution, of course, also gives full points.

Exercice 4 [**25 pts**]

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 $p \equiv 1 \mod 4$.

Solution:

Nous utiliserons la même notations et les mêmes faits qu'à l'exercice 2.

(a). **7 points total**

Si n est irréductible dans $\mathbb{Z}[i]$, alors il est dans $\mathbb{Z}$, et donc premier vu que $\mathbb{Z}$ est principal. En effet, si l'on pouvait écrire $n = ab$ avec $a, b \notin \mathbb{Z}^\times$, alors nécessairement $N(a), N(b) > 1$. Ainsi, $a, b \notin \mathbb{Z}[i]^\times$, et on a donc une contradiction. (**1 pt**)

De plus, s'il existe $a, b \in \mathbb{Z}$ tel que $n = a^2 + b^2$, alors $n = (a+bi)(a-bi)$, et vu que $N(n) > 1$ et $N(a+bi) = N(a-bi) = \sqrt{N(n)} > 1$, on conclut que ni $a+bi$ ni $a-bi$ ne sont inversibles, ce qui contredirait le fait que n est irréductible. (**2 pts**)

Montrons l'autre direction, et supposons par l'absurde que n n'est pas irréductible dans $\mathbb{Z}[i]$. Ecrivons alors $n = z_1 z_2$, avec $z_j \in \mathbb{Z}[i]$ non-inversibles. En particulier, $N(z_j) \neq 1$ pour $j = 1, 2$ (**1 pt**). Ainsi, $n^2 = N(z_1)N(z_2)$ et vu que n est premier, on en déduit forcément que $N(z_1) = N(z_2) = n$. Cela contredit que n ne s'écrive pas $a^2 + b^2$ avec $a, b \in \mathbb{Z}$. (**3 pts**)

(b). **9 points total**

On sait par les exercices que le morphisme $\mathbb{Z}[x] \to \mathbb{Z}[i]$ donné par l'évaluation en i induit un isomorphisme $\theta \colon \mathbb{Z}[x]/(x^2+1) \to \mathbb{Z}[i]$. (**2 pts**) De plus, $p + (x^2+1)$ est envoyé sur p par cet isomorphisme, et donc on en déduit un isomorphisme

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

(**2 pts**) Par le théorème du quotient en deux temps appliqué deux fois, on a que

$$(\mathbb{Z}[x]/(x^2+1))/(p + (x^2+1)) \cong \mathbb{Z}[x]/(p, x^2+1) \cong (\mathbb{Z}[x]/(p))/(x^2 + 1 + (p)).$$

(**3 pts**)

De plus, il est immédiat que le morphisme $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ induit par la réduction modulo p et envoyant x sur x est surjectif, de noyau $(p) \subseteq \mathbb{Z}[x]$. Il induit donc un isomorphisme $\mathbb{Z}[x]/(p) \cong \mathbb{F}_p[x]$. Comme ce morphisme envoit $x^2 + 1 + (p)$ sur $x^2 + 1$, on a donc un isomorphisme induit

$$\mathbb{Z}[x]/(p, x^2+1) \cong (\mathbb{Z}[x]/(p))/(x^2 + 1 + (p)) \cong \mathbb{F}_p[x]/(x^2+1).$$

(**2 pts**)

(c). **9 points total**

Supposons tout d'abord que p n'est pas premier dans $\mathbb{Z}[i]$, et supposons que $p \neq 2$ (on veut alors montrer que 4 divise $p-1$).

Preuve 1 de $p \equiv 3 \mod 4$ implique p irréductible :

Comme $\mathbb{Z}[i]/(p)$ n'est pas intègre, on obtient par le point précédent que $\mathbb{F}_p[x]/(x^2+1)$ n'est pas intègre non plus. (**2 pts**) Ainsi, x^2+1 n'est pas un polynôme irréductible, et comme il est de degré 2, il a forcément une racine. En d'autres termes, il existe $a \in \mathbb{F}_p$ tel que $a^2 = -1$. Vu que $p \neq 2$, a est donc un élément d'ordre 4 dans le groupe multiplicatif $(\mathbb{F}_p^\times, \cdot)$, qui est d'ordre $p-1$. Ainsi, 4 divise $p-1$. (**2 pts, dont 1 pour dire que** $p \neq 2$)

Preuve 2 de $p \equiv 3 \mod 4$ implique p irréductible :

Par le point (a), il suffit de montrer que l'on ne peut pas écrire $p = a^2 + b^2$ pour $a, b \in \mathbb{Z}$. Or, pour tout $a \in \mathbb{Z}$, $a^2 \equiv 0, 1 \mod 4$ et donc p ne peut pas s'écrire comme somme de deux carrés. (**4 pts**)

Montrons l'autre direction. Si $p = 2$, alors $p = (1+i)(1-i)$ et ces deux éléments sont de norme 2, et donc pas des unités. Ainsi, p n'est pas irréductible dans $\mathbb{Z}[i]$. On pouvait aussi argumenter que $2 = 1^2 + 1^2$, et donc conclure par le point (a). (**1 pt**)

Si 4 divise $p-1$, alors vu que l'on sait par le cours que l'on a un isomorphisme de groupes $(\mathbb{F}_p^\times, \times) \cong \mathbb{Z}/(p-1)\mathbb{Z}$, et que dans $\mathbb{Z}/(p-1)\mathbb{Z}$, l'élément $\frac{p-1}{4}$ est d'ordre 4, on obtient l'existence d'un élément a d'ordre 4 dans $(\mathbb{F}_p^\times, \times)$. (**2 pts**) Ainsi, $a^4 = 1$ mais $a^2 \neq 1$. Comme les seules racines carré de l'unité sont 1 et -1 et que $a^2 \neq 1$, on déduit forcément que $a^2 = -1$. Ainsi, x^2+1 n'est pas irréductible dans $\mathbb{F}_p[x]$, et donc par le même argument que dans l'autre direction, on déduit que p n'est pas premier dans $\mathbb{Z}[i]$. (**2 pts**)

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 $g(x)(x^2-c)$.

Solution:

(a). **5 points total** Considérons les deux sous-groupes H_1 et H_2 de $G \coloneqq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ donnés par $H_1 = \mathbb{Z}/2\mathbb{Z} \times \{0\}$ et $H_2 = \{0\} \times \mathbb{Z}/2\mathbb{Z}$, et considérons les sous-corps $F_1 = L^{H_1}$ et $F_2 = L^{H_2}$.

Par le théorème de correspondance de Galois, les extensions F_i/K sont d'ordre $|G|/|H_i| = 2$, et donc on sait qu'il existe $c_i \in K$ tels que $F_i = K(\sqrt{c_i})$. Comme L/K est Galoisienne, on sait que L contient le corps de décomposition de $(x^2-c_1)(x^2-c_2)$, donc il suffit de montrer que L est généré par $\sqrt{c_1}$ et $\sqrt{c_2}$ pour conclure.

Soit L' l'extension générée par ces deux éléments. Alors $F_1 \subseteq L'$, et vu que $[L : F_1] = [L : K]/[F_1 : K] = 2$, on a forcément que soit $L' = F_1$, soit $L' = L$. Si $L' \neq L$, alors on peur faire le même argument avec F_2 et donc $F_1 = L = F_2$. Or, $H_1 \neq H_2$, et donc par la correspondance de Galois, $F_1 \neq F_2$. Ainsi, $L' = L$ et donc la preuve est finie.

Barème. On attribuera 1 points pour toute utilisation correcte de la correspondance de Galois. Par exemple, pour déduire le degré du corps. On attribuera 2 points pour la construction de c et d. 2 points pour montrer que c'est le corps de décomposition de $\sqrt{c}$ et $\sqrt{d}$. 1 seul point parmi ces deux si on comprend qu'il faut montrer $L = K(\sqrt{c}, \sqrt{d})$ avec des arguments incomplets.

Notons qu'il est faux de construire justement c puis ré-invoquer le théorème de la donnée pour avoir $K(\sqrt{c})(\sqrt{d}) = L$. Voici un exemple d'extension qui satisfait aux hypothèses de l'énoncé où cela ne pourrait pas fonctionner. $\mathbb{Q}(\sqrt{2+\sqrt{3}})$. Notons que comme

$$\sqrt{2+\sqrt{3}} + \frac{1}{\sqrt{2+\sqrt{3}}} = \sqrt{6}$$

on a $\mathbb{Q}(\sqrt{2+\sqrt{3}}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ Dès lors on pourrait choisir c comme étant racine de 3, puis d comme étant $\sqrt{2+\sqrt{3}}$ dont le carré n'est pas dans $\mathbb{Q}$.

(b). **15 points total** Considérons les deux sous-groupes H_1 et H_2 de $G \coloneqq S_3 \times \mathbb{Z}/2\mathbb{Z}$ donnés par $H_1 = S_3 \times \{0\}$ et $H_2 = \{0\} \times \mathbb{Z}/2\mathbb{Z}$, et considérons les sous-corps $F_1 = L^{H_1}$ et $F_2 = L^{H_2}$.

Comme H_1 et H_2 sont normaux dans G, on sait par le correspondance de Galois que F_1/K est Galoisienne de groupe $\mathbb{Z}/2\mathbb{Z}$, et F_2/K est Galoisienne de groupe S_3. On sait alors automatiquement et qu'il existe $c \in K$ tel que $F_1 = K(\sqrt{c})$. Supposons que l'on sait démontrer que F_2 est le corps de décomposition d'un polynôme irréductible $g(x)$ de degré 3. Alors exactement le même argument qu'au point précédent montrera que L est le corps de décomposition de $(x^2 - c)g(x)$, et donc on aura fini.

Il suffit donc de montrer que F_2 est le corps de décomposition d'un polynôme irréductible de degré 3. Considérons le sous-groupe $U \coloneqq \langle (12) \rangle \subseteq S_3$, et soit $M \coloneqq F_2^U$ le sous-corps correspondant.

Par le théorème de l'élément primitif, on peut écrire $M = K(\alpha)$. Soit g le polynôme minimal de α sur K (il est donc irréductible). Comme $[M : K]$ est de degré $|S_3|/|M| = 6/2 = 3$, on obtient que $\deg(g) = 3$.

De plus, on sait par le cours que l'extension M/K ne peut pas être Galoisienne, vu que U n'est pas normal dans S_3. Ainsi, M ne peut pas contenir toutes les racines de g, En effet, sinon M serait un corps de décomposition sur K, et donc vu que l'extension est séparable ($K \subseteq L$ est séparable), cette extension serait Galoisienne par le cours.

Ainsi, le corps de décomposition de g (qui est contenu dans F_2 vu que F_2/K est Galoisienne) contient strictement M. Comme $[F_2 : M] = [F_2 : K]/[M : K] = 6/3 = 2$, on déduit que F_2 est le corps de décomposition de g.

Barème. On liste les points maximaux selon la résolution typique correcte retrouvée dans les examens.

- 1 point pour toute invocation d'une quelconque correspondance Galoisienne.
- 3 points pour une construction d'une extension de degré 2 qui peut satisfaire aux buts de l'exercice (voir plus bas) et utilisation du théorème rappelé dans l'énoncé.

- 2 points pour une construction d'une extension de degré 3
- 2 points pour utiliser le théorème primitif. (à n'importe quel moment dans une rédaction, mais dans une rédaction correcte on s'attend à l'utiliser pour montrer que l'extension de degré 3 construite est primitive)
- 2 points pour construire g comme un polynôme minimal. (Même si le g est faux, si on a l'idée de le construire comme polynôme minimal)
- 3 points pour identifier le corps de décomposition d'une extension de degré 3 – en particulier dans ces 3 points se trouvent le point clé d'utiliser que le sous-groupe choisi pour créer l'extension de degré 3 n'est pas normal.
- 2 points pour toute argument correct qui montre après avoir construit c et g que L est le corps de décomposition de $(x^2 - c)g$

Ces 15 points attribués ainsi se retrouvent dans toutes les réponses qui ont obtenus tous les points. Dans des cas de rédaction plus approximatives on aura aussi attribué ou soustrait

- 2 points si on considère l'extension correspondant à $\{\mathrm{id}\} \times \mathbb{Z}/2\mathbb{Z}$ sans aller plus loin.
- Certains pensent que S_3 a cardinal 3. 1 point de pénalité.
- 2 sur les 3 points attribués usuellement dans le cas où l'on construit l'extension de degré 2 en utilisant $\langle(123)\rangle \times \mathbb{Z}/2\mathbb{Z}$. Les carrés extraits par cette extension ne peuvent jamais conclure à résoudre à cet exercice, voir explication ci-dessous.

Explication. $G = S_3 \times \mathbb{Z}/2\mathbb{Z}$ a 3 sous-groupes d'indice 2[1]. Il y $S_3 \times 0$, le sous-groupe

$$S_3 \times_{\mathrm{sgn}} \mathbb{Z}/2\mathbb{Z} = \{(\sigma, \mathrm{sgn}(\sigma)) \mid \sigma \in S_3\}$$

qui sont tous deux isomorphes à S_3 et le dernier $A_3 \times \mathbb{Z}/2\mathbb{Z}$ qui est cyclique d'ordre 6. Les deux premiers sous-groupes font l'affaire pour construire une extension de degré 2 dans une résolution comme donnée dans le corrigé. En effet cela suit du fait que l'intersection de ces sous-groupes avec $\{\mathrm{id}\} \times \mathbb{Z}/2\mathbb{Z}$ est triviale – le deuxième a été boudée par manque de fantaisie, tout le monde ayant utilisé $S_3 \times 0$. Quelques personnes ont cependant utilisé $A_3 \times \mathbb{Z}/2\mathbb{Z}$. L'extension de degré 2 qu'on obtient avec ce sous-groupe ne pourra jamais conclure. Voici pourquoi.

Notons $M = K(\sqrt{c})$ l'extension de degré 2 correspondant au sous-groupe $\langle(123)\rangle \times \mathbb{Z}/2\mathbb{Z}$. Remarquons que les seuls groupes d'ordre 4 sont de la forme $\langle\tau\rangle \times \mathbb{Z}/2\mathbb{Z}$ pour τ un 2-cycle.[2] Ces sous-groupes correspondent à des extensions de degré 3, qu'on note génériquement F, non Galoisiennes. Si $\alpha \in L$ est de degré 3 alors $K(\alpha)$ est forcément l'une de ces 3 sous-extensions. Tout les polynômes minimaux g de ces α ont alors pour corps de décomposition l'extension de degré 6 qu'on note F' qui correspond au sous-groupe $\{\mathrm{id}\} \times \mathbb{Z}/2\mathbb{Z}$. Mais maintenant comme $M \subset F'$ et $F \subset F'$ chaque fois sans sous-extension intermédiaire comme on l'observe dualement sur les sous-groupes et que F' est Galoisienne, on déduit que le corps de décomposition de $\left(x^2 - c\right) g$ est F', pas ce qu'on veut. (On veut que ça soit L)

[1] En effet, un sous-groupe d'indice est d'ordre 6, donc contient un sous-groupe d'ordre 3. Mais le seul sous-groupe d'ordre 3 est $A_3 \times 0$. Donc par le théorème de correspondance les sous-groupes d'indice 2 correspondent aux sous-groupes d'indice 2 du quotient $G/A_3 \times 0 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Or ce groupe a 3 sous-groupe d'indice 2.

[2] On voit cela ainsi: si H est un sous-groupe d'ordre 4 alors l'image par la première projection est un sous-groupe où tous les éléments sont d'ordre qui divise 2. Ainsi c'est forcément un 2-cycle ou l'élément neutre. Si c'est l'élément neutre alors $H \leq \{\mathrm{id}\} \times \mathbb{Z}/2\mathbb{Z}$ une contradiction sur la cardinalité.