Contrôle final - Mercredi 5 janvier 2022
durée : 3 h

Le candidat attachera la plus grande importance à la clarté, à la précision et à la concision de la rédaction. Dans toutes les questions, il sera tenu le plus grand compte de la rigueur de la rédaction.
L'usage de tout document et de tout matériel électronique est interdit.

1 Anneaux et corps

Préambule : Par anneau on entend anneau unitaire. Pour p premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$. On notera $\langle a \rangle$ l'idéal engendré par un élément a d'un anneau commutatif.

Exercice 1 (Question de cours)**.**

1. Rappeler la définition d'un élément *irréductible* dans un anneau intègre.
2. Répondre sans justifier : Donner un exemple de deux anneaux intègres $R \subset S$ et d'un élément $r \in R$ qui est irréductible dans R mais pas dans S.
3. Répondre sans justifier : Donner un exemple de deux anneaux intègres $R \subset S$ et d'un élément $r \in R$ qui est irréductible dans S mais pas dans R.

Exercice 2 (Exercice de TD)**.**

1. Déterminer lesquels des anneaux quotients suivants sont des corps en justifiant vos réponses :
$$\mathbb{Q}[x]/\langle x^2 - x - 1 \rangle \,;\, \mathbb{F}_3[x]/\langle x^2 + 2 \rangle \,;\, \mathbb{F}_5[x]/\langle x^2 + 2 \rangle$$
2. Trouver l'inverse multiplicatif de $x + 1$ dans $\mathbb{F}_5[x]/\langle x^2 + 2 \rangle$.

Exercice 3. On considère l'anneau $\mathbb{Z}[i] = \{a + bi \ : a, b \in \mathbb{Z}\}$ et un idéal $I \neq \{0\}$ de $\mathbb{Z}[i]$. On admet que $\mathbb{Z}[i]$ est un anneau euclidien relativement à la norme $N : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$ donnée par $N(a + bi) = a^2 + b^2$ (démontré en TD).

1. En déduire que $I = \langle \alpha \rangle$ pour un certain $\alpha \in \mathbb{Z}[i] \setminus \{0\}$.
2. Soit $x + I \in \mathbb{Z}[i]/I$. Montrer que si $x \notin I$ alors $x + I = r + I$ pour un certain $r \in \mathbb{Z}[i] \setminus \{0\}$ avec $N(r) < N(\alpha)$.
3. En déduire que $\mathbb{Z}[i]/I$ est fini.

Posons $I = \langle 1 + 2i \rangle$. On considère le morphisme $\varphi : \mathbb{Z} \to \mathbb{Z}[i]/I$ donné par $n \mapsto n + I$.

4. Montrer que $a + 2b + I = a + bi + I$ pour tout $a, b \in \mathbb{Z}$. (Indication : On remarque que $2 - i = -i(1 + 2i)$).
5. En déduire que φ est surjectif.
6. Montrer que $n \in \operatorname{Ker} \varphi$ si et seulement si $n \in \mathbb{Z}$ et $n = (a + bi)(1 + 2i)$ avec $a, b \in \mathbb{Z}$.
7. En déduire que $\operatorname{Ker} \varphi = 5\mathbb{Z}$.
8. En déduire que $\mathbb{Z}[i]/I \simeq \mathbb{F}_5$.

Exercice 4. Soit R un anneau commutatif fini et I un idéal de R. Montrer que si I est premier alors I est maximal. (Indication : On pourra montrer que tout anneau intègre fini est un corps).

2 Représentations de groupes

Préambule : Par *représentation* d'un groupe fini G on entendra un morphism $\rho_V : G \to GL(V)$ où V est un $\mathbb{C}$-espace vectoriel de dimension fini. La dimension de V est appelée le *degré* de la représentation ρ_V. On note par $\langle \cdot, \cdot \rangle_G : \mathbb{C}^G \times \mathbb{C}^G \to \mathbb{C}$ le produit scalaire hermitien

$$\langle f, g \rangle_G = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}$$

où $\mathbb{C}^G$ l'ensemble des applications de G vers $\mathbb{C}$. L'énoncé dans la partie représentation comporte un seul exercice constitué de 15 questions.

Exercice 5. Soit G un groupe fini et N un sous-groupe distingué dans G. Notons $\pi : G \to G/N$ la projection canonique donnée par $g \mapsto gN$. Etant donné une représentation $\tilde{\rho}_V : G/N \to GL(V)$ du groupe quotient G/N, on considère la composition

$$\rho_V : G \xrightarrow{\pi} G/N \xrightarrow{\tilde{\rho}_V} GL(V).$$

1. Montrer que l'application $\rho_V : G \to GL(V)$ définit une représentation du groupe G du même degré que $\tilde{\rho}_V$ et que $N \subseteq \operatorname{Ker} \rho_V$.
2. Inversement, étant donné une représentation $\rho_W : G \to GL(W)$ avec $N \subseteq \operatorname{Ker} \rho_W$, montrer que l'application $\tilde{\rho}_W : G/N \to GL(W)$ donnée par $\tilde{\rho}_W(gN) = \rho_W(g)$ définit une représentation de G/N. (Indication : Il faudra d'abord montrer que $\tilde{\rho}_W$ est bien définie).
3. Notons par χ_V (resp. $\tilde{\chi}_V$) le caractère associé à ρ_V (resp. $\tilde{\rho}_V$). Montrer que $\chi_V(g) = \tilde{\chi}_V(gN)$ pour tout $g \in G$.
4. Montrer que $\langle \chi_V, \chi_V \rangle_G = \langle \tilde{\chi}_V, \tilde{\chi}_V \rangle_{G/N}$.
5. En déduire que ρ_V est irréductible si et seulement si $\tilde{\rho}_V$ est irréductible.
6. En déduire que l'application $\tilde{\rho} \mapsto \rho$ définie une bijection entre les représentations irréductibles $\tilde{\rho}$ de G/N et les représentations irréductibles ρ de G dont le noyau $\operatorname{Ker} \rho$ contient N.

Application : Le nombre de représentations de degré 1

Rappel du cas abélien - répondre sans justifier (cours) :

7. Quel est le degré d'une représentation irréductible d'un groupe abélien fini ?
8. Quel est le nombre de représentations irréductibles d'un groupe abélien d'ordre n ?

Rappel : Le *groupe dérivé* d'un groupe G est le sous-groupe $D(G)$ engendré par les *commutateurs*, c'est à dire par les éléments de la forme $xyx^{-1}y^{-1}$. On admet les deux résultats suivants : **i)** $D(G)$ est un sous-groupe distingué de G et le quotient $G_{ab} = G/D(G)$ (appelé *l'abélianisé de* G) est un groupe abélien ; **ii)** si H est un sous-groupe distingué de G tel que G/H est abélien, alors $D(G) \subseteq H$.

Dans ce qui suit, nous proposons de montrer que l'ensemble des représentations de G de degré 1 est en bijection avec l'ensemble des représentations irréductibles du groupe abélien G_{ab}. Par application de la question 6. ci-dessus il suffira de montrer que l'ensemble des représentations de G de degré 1 est en bijection avec l'ensemble des représentations irréductibles ρ de G dont le noyau $\operatorname{Ker} \rho$ contient $D(G)$.

9. En prenant $N = D(G)$ dans la question 6. ci-dessus, en déduire que si $\rho_V : G \to GL(V)$ est une représentation irréductible de G telle que $D(G) \subseteq \operatorname{Ker} \rho_V$, alors ρ_V est de degré 1. (Indication : D'après la propriété **i)** le quotient $G/N = G_{ab}$ est abélien).
10. Inversement montrer que si $\rho_V : G \to GL(V)$ est une représentation de G de degré 1, alors $D(G) \subseteq \operatorname{Ker} \rho_V$.
11. En déduire que le nombre ℓ de représentations de G de degré 1 est égal à $|G_{ab}|$, en particulier ℓ divise $|G|$.

Le cas du groupe diédral

On suppose dorénavant que $G = D_{2n}$ ($n \geq 2$) le groupe diédral d'ordre $2n$ engendré par r d'ordre n et s d'ordre 2 tel que $srs = r^{-1}$. Tout élément x de D_{2n} s'écrit de manière unique comme $r^i s^j$ avec $0 \leq i \leq n-1$ et $0 \leq j \leq 1$.

12. Montrer que le sous-groupe $\langle r^2 \rangle$ engendré par r^2 est distingué et d'indice 2 si n est impair et d'indice 4 si n est pair. (Indication : On remarque que $\langle r^2 \rangle = \langle r \rangle$ quand n est impair).
13. En déduire que $D(G) \subseteq \langle r^2 \rangle$. (Indication : D'après la question précédente le quotient $G/\langle r^2 \rangle$ est un groupe d'ordre 2 ou 4 selon la parité de n. On pourra donc appliquer l'inclusion **ii)** ci-dessus).
14. Montrer que $\langle r^2 \rangle = D(G)$. (Indication : Il reste à montrer que $\langle r^2 \rangle \subseteq D(G)$ et pour cela on remarque que $r^{-2} = srsr^{-1}$).
15. Par application de la question 11., en déduire que le nombre de représentations de G de degré 1 est égal à 2 si n est impair et 4 si n est pair.