Université Claude Bernard Lyon 1
Master 1 de mathématiques : Algèbre
Année 2021–2022

Examen final, 5 janvier 2022

I Exercice 1

1° Rappeler la définition d'un élément *irréductible* dans un anneau intègre.

Solution. Un élément est dit irréductible s'il n'est ni inversible, ni produit de deux éléments non inversibles. □

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.

Solution. Le polynôme $x^2 + 1 \in \mathbb{Z}[x] \subset \mathbb{C}[x]$ est irréductible dans $\mathbb{Z}[x]$ mais pas dans $\mathbb{C}[x]$. □

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.

Solution. Le polynôme $2x + 2 \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ est irréductible dans $\mathbb{Q}[x]$ mais pas dans $\mathbb{Z}[x]$. □

II Exercice 2

1° Déterminer lesquels des anneaux quotients suivants sont des corps en justifiant vos réponses :

$$\mathbb{Q}[x]/\langle x^2 - x - 1\rangle \,;\, \mathbb{F}_3[x]/\langle x^2 + 2\rangle \,;\, \mathbb{F}_5[x]/\langle x^2 + 2\rangle$$

Solution. L'anneau quotient $k[x]/\langle p(x)\rangle$ (où k est un corps) est un corps ssi. $p(x)$ est irréductible. Dans le cas d'un polynôme $p(x)$ de degré 2 (ou 3) on a que $p(x)$ est irréductible dans $k[x]$ ssi. $p(x)$ n'a pas de racines dans k. Or, $x^2 - x - 1$ n'a pas de racines dans $\mathbb{Q}$ et donc $\mathbb{Q}[x]/\langle x^2 - x - 1\rangle$ est un corps. De même, $x^2 + 2$ n'a pas de racines dans $\mathbb{F}_5$ et donc $\mathbb{F}_5[x]/\langle x^2 + 2\rangle$ est un corps. D'autre part, 1 est une racine de $x^2 + 2$ dans $\mathbb{F}_3$. Il s'ensuit que $\mathbb{F}_3[x]/\langle x^2 + 2\rangle$ n'est pas un corps. □

2° Trouver l'inverse multiplicatif de $x + 1$ dans $\mathbb{F}_5[x]/\langle x^2 + 2\rangle$.

Solution. On cherche $a, b \in \mathbb{F}_5$ tels que $(x + 1)(ax + b) = 1$ dans $\mathbb{F}_5[x]/\langle x^2 + 2\rangle$. Il s'ensuit que $a + b = 0$ et $-2a + b = 1$ et donc $a = 3$ et $b = 2$. On a donc que l'inverse multiplicatif de $x + 1$ dans $\mathbb{F}_5[x]/\langle x^2 + 2\rangle$ est $3x + 2$. □

III 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 $\alpha \in \mathbb{Z}[i] \setminus \{0\}$.

Solution. Tout anneau euclidien est principal. On a donc que $I = \langle\alpha\rangle$ pour un certain $\alpha \in \mathbb{Z}[i]$. Comme $I \neq \{0\}$ il s'ensuit que $\alpha \in \mathbb{Z}[i] \setminus \{0\}$. □

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 $N(r) < N(\alpha)$.

Solution. Comme $\mathbb{Z}[i]$ est euclidien on a que pour tout $x \in \mathbb{Z}[i]$ il existe $q, r \in \mathbb{Z}[i]$ tels que $x = q\alpha + r$ avec $N(r) < N(\alpha)$ si $r \neq 0$. On a donc que $x + I = q\alpha + r + I = r + I$ car $q\alpha \in I$. Finalement, si $r = 0$ alors $x = q\alpha \in I$. Donc pour $x \notin I$ on a $r \in \mathbb{Z}[i] \setminus \{0\}$ et $N(r) < N(\alpha)$. □

3° En déduire que $\mathbb{Z}[i]/I$ est fini.

Solution. D'après la question 2. on a que $\mathbb{Z}[i]/I = \{r + I : r = 0 \,\text{ou}\, N(r) < N(\alpha)\}$. Mais pour tout choix de $\alpha \in \mathbb{Z}[i] \setminus \{0\}$, il existe un nombre fini d'entiers a, b tels que $a^2 + b^2 < N(\alpha)$. Il s'ensuit 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 $2 - i = -i(1 + 2i)$).

Solution. $a + 2b + I = a + bi + I \Leftrightarrow a + 2b - (a + bi) \in I \Leftrightarrow b(2 - i) \in I$. Mais $b(2 - i) = -bi(1 + 2i) \in I$. □

5° En déduire que φ est surjectif.

Solution. Soit $y \in \mathbb{Z}[i]/I$. Alors il existe a et b dans $\mathbb{Z}$ tels que $y = a + bi + I$. D'après la question 4., on a que $y = a + bi + I = a + 2b + I = \varphi(a + 2b)$ qui montre 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 $a, b \in \mathbb{Z}$.

Solution. $\operatorname{Ker} \varphi = \{n \in \mathbb{Z} : \varphi(n) = I\}$. Mais $\varphi(n) = I \Leftrightarrow n + I = I \Leftrightarrow n \in I$ et de plus, comme $\mathbb{Z}[i]$ est un anneau unitaire et commutatif, on a que $I = \langle 1 + 2i \rangle = \{r(1 + 2i) : r \in \mathbb{Z}[i]\}$. Il s'ensuit que $n \in \operatorname{Ker} \varphi$ ssi. $n \in \mathbb{Z}$ et $n = (a + bi)(1 + 2i)$ avec $a, b \in \mathbb{Z}$. □

7° En déduire que $\operatorname{Ker} \varphi = 5\mathbb{Z}$.

Solution. On vérifie que pour $a, b \in \mathbb{Z}$, le produit $(a + bi)(1 + 2i) \in \mathbb{Z}$ ssi. $b = -2a$ et dans ce cas $(a + bi)(1 + 2i) = 5a$. On a donc que $n \in \operatorname{Ker} \varphi \Leftrightarrow n = (a + bi)(1 + 2i)$ avec $a \in \mathbb{Z}$ et $b = -2a \Leftrightarrow n = 5a$ avec $a \in \mathbb{Z} \Leftrightarrow n \in 5\mathbb{Z}$. □

8° En déduire que $\mathbb{Z}[i]/I \simeq \mathbb{F}_5$.

Solution. Comme le morphisme $\varphi : \mathbb{Z} \to \mathbb{Z}/I$ est surjectif, par application du 1er théorème d'isomorphisme d'anneaux on a que $\mathbb{Z}[i]/I \simeq \mathbb{Z}/\operatorname{Ker} \varphi$. D'après la question précédente, $\mathbb{Z}/\operatorname{Ker} \varphi = \mathbb{Z}/5\mathbb{Z} = \mathbb{F}_5$. □

IV Exercice 4

Soit R un anneau (unitaire) 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).

Solution. On rappelle que si R est un anneau (unitaire) commutatif et I un idéal de R, alors I est premier (resp. maximal) ssi. R/I est intègre (resp. un corps). Supposons que I est un idéal premier de R. On a donc que R/I est un anneau intègre fini (car R est fini). Pour montrer que I est maximal, il suffit de montrer que tout anneau intègre fini est un corps.
Soit S un anneau intègre fini. Pour montrer que S est un corps, il suffit de montrer que tout $a \in S \setminus \{0_S\}$ est une unité. On considère l'application $f_a : S \to S$ donnée par $f_a(x) = ax$. Montrons que f_a est injective : Pour tout $x, y \in S$ on a $f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow a(x-y) = 0_S \Rightarrow x - y = 0_S$ (car S est intègre et $a \neq 0_S$) $\Rightarrow x = y$. Or, comme S est fini, il s'ensuit que l'application f_a est surjective. On a donc que pour tout $a \in S \setminus \{0_S\}$ il existe $b \in S$ tel que $f_a(b) = 1_S$, c'est à dire $ab = 1_S$ qui montre que a est inversible. □

V 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 $N \subseteq \operatorname{Ker} \rho_V$.

Solution. Etant la composition de deux morphismes de groupes, l'application ρ_V est un morphisme de G vers $GL(V)$ et donc ρ_V est une représentation du groupe G. Le degré de ρ_V est égal à la dimension de l'espace vectoriel V qui à son tour est égal au degré de $\tilde{\rho}_V$. Pour $x \in N$ on a que $\rho_V(x) = \tilde{\rho}_V(\pi(x)) = \tilde{\rho}_V(xN) = \tilde{\rho}_V(N) = 1_V$ et donc $x \in \operatorname{Ker} \rho_V$. □

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).

Solution. Pour montrer que $\tilde{\rho}_W$ est bien définie il faut vérifier que pour tout $x, y \in G$, si $xN = yN$ alors $\rho_W(x) = \rho_W(y)$. Or, $xN = yN \Rightarrow N = x^{-1}yN \Rightarrow x^{-1}y \in N \Rightarrow \rho_W(x^{-1}y) = 1_W \Rightarrow \rho_W(x^{-1})\rho_W(y) = 1_W \Rightarrow \rho_W(x)^{-1}\rho_W(y) = 1_W \Rightarrow \rho_W(x) = \rho_W(y)$. Pour vérifier que $\tilde{\rho}_W$ est un morphisme on a que

$$\tilde{\rho}_W(xNyN) = \tilde{\rho}_W(xyN) = \rho_W(xy) = \rho_W(x)\rho_W(y) = \tilde{\rho}_W(xN)\tilde{\rho}_W(yN).$$

□

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 $g \in G$.

Solution. Pour $g \in G$ on a $\chi_V(g) = \operatorname{tr}(\rho_V(g)) = \operatorname{tr}(\tilde{\rho}_V(gN)) = \tilde{\chi}_V(gN)$. □

4° Montrer que $\langle \chi_V, \chi_V \rangle_G = \langle \tilde{\chi}_V, \tilde{\chi}_V \rangle_{G/N}$.

Solution.

$$\begin{aligned}
\langle \chi_V, \chi_V \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \overline{\chi_V(g)} \\
&= \frac{1}{|G|} \sum_{xN \in G/N} \sum_{g \in xN} \chi_V(g) \overline{\chi_V(g)} \\
&= \frac{1}{|G|} \sum_{xN \in G/N} \sum_{g \in xN} \tilde{\chi}_V(gN) \overline{\tilde{\chi}_V(gN)} \\
&= \frac{1}{|G|} \sum_{xN \in G/N} |N| \tilde{\chi}_V(xN) \overline{\tilde{\chi}_V(xN)} \\
&= \frac{1}{|G/N|} \sum_{xN \in G/N} \tilde{\chi}_V(xN) \overline{\tilde{\chi}_V(xN)} \\
&= \langle \tilde{\chi}_V, \tilde{\chi}_V \rangle_{G/N}.
\end{aligned}$$

Nous avons utilisé que a) G/N est une partition de G; b) le résultat de la question 3. et c) si $g \in xN$ alors $gN = xN$. □

5° En déduire que ρ_V est irréductible si et seulement si $\tilde{\rho}_V$ est irréductible.

Solution. Une représentation ρ_V est irréductible ssi. $\langle \chi_V, \chi_V \rangle_G = 1$. En fait, par application de Maschke, ρ_V peut s'écrire comme $\rho_V = \rho_1 \oplus \rho_2 \oplus \cdots \oplus \rho_k$ avec ρ_i irréductible. On a donc que $\chi_V = \chi_1 + \chi_2 + \cdots \chi_k$ où $\chi_i = \mathrm{tr} \rho_i$. De plus, par l'orthonormalité des caractères irréductibles on a que

$$\langle \chi_i, \chi_j \rangle_G = \begin{cases} 1 & \text{si } \chi_i = \chi_j \\ 0 & \text{si } \chi_i \neq \chi_j \end{cases}$$

Or, d'après la question précédente on a que $\langle \chi_V, \chi_V \rangle_G = 1$ ssi. $\langle \tilde{\chi}_V, \tilde{\chi}_V \rangle_{G/N} = 1$. On a donc que ρ_V est irréductible ssi. $\tilde{\rho}_V$ 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 $\mathrm{Ker}\, \rho$ contient N.

Solution. Par application des questions 1. et 5. on a que l'application $\tilde{\rho} \mapsto \rho$ associe à chaque représentation irréductible $\tilde{\rho}$ de G/N une représentation irréductible ρ de G avec $N \subseteq \mathrm{Ker}\, \rho$ donnée par $\rho = \tilde{\rho} \circ \pi$. Inversement, d'après les questions 2. et 5., pour tout représentation irréductible ρ de G avec $N \subseteq \mathrm{Ker}\, \rho$ il existe une représentation irréductible $\tilde{\rho}$ de G/N telle que $\rho = \tilde{\rho} \circ \pi$. Il est évident que ces deux opérations sont l'inverse l'une de l'autre. □

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

7° Quel est le degré d'une représentation irréductible d'un groupe abélien fini ?

Solution. Tout représentation irréductible d'un groupe abélien fini est de degré 1. □

8° Quel est le nombre de représentations irréductibles d'un groupe abélien d'ordre n ?

Solution. Chaque groupe abélien d'ordre n admet précisément n représentations irréductibles. □

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).

Solution. Par application de la question 6., si $\rho_V : G \to GL(V)$ est une représentation irréductible de G telle que $D(G) \subseteq \operatorname{Ker}\rho_V$, alors il existe une représentation irréductible $\tilde{\rho}_V$ de $G/D(G)$ telle que $\rho_V = \tilde{\rho}_V \circ \pi$. Or, comme $G/D(G)$ est un groupe abélien, on a que $\tilde{\rho}_V$ est de degré 1 et donc ρ_V est de degré 1. □

10° Inversement montrer que si $\rho_V : G \to GL(V)$ est une représentation de G de degré 1, alors $D(G) \subseteq \operatorname{Ker}\rho_V$.

Solution. Comme $D(G)$ est engendré par l'ensemble des commutateurs, pour montrer que $D(G) \subseteq \operatorname{Ker}\rho_V$ il suffit de montrer que chaque commutateur $xyx^{-1}y^{-1}$ appartient à $\operatorname{Ker}\rho_V$. Or, comme ρ_V est de degré 1, on a que $GL(V)$ est un groupe abélien (en fait, il est isomorphe à $\mathbb{C}^*$) et donc $\rho_V(xyx^{-1}y^{-1}) = \rho_V(x)\rho_V(y)\rho_V(x)^{-1}\rho_V(y)^{-1} = 1_V$. Cela montre que $xyx^{-1}y^{-1} \in \operatorname{Ker}\rho_V$. □

11° En déduire que le nombre ℓ de représentations de G de degré 1 est égal à $|G_{ab}|$, en particulier ℓ divise $|G|$.

Solution. Par application des deux questions précédentes on a que l'ensemble des représentations de G de degré 1 est égal à l'ensemble des représentations irréductibles de G dont le noyau contient $D(G)$. D'après la question 6., celui ci est en bijection avec les représentations irréductibles de $G/D(G) = G_{ab}$. Or, comme G_{ab} est un groupe abélien, le nombre de représentations irréductibles de G_{ab} est égal à $|G_{ab}|$. On a donc que le nombre ℓ de représentations de G de degré 1 est égal à $|G_{ab}|$. De plus, par le théorème de Lagrange, $|G| = |G_{ab}||D(G)|$ et donc $\ell = |G_{ab}|$ divise $|G|$. □

On suppose dorénavant que $G = D_{2n}$ ($n \geqslant 2$) 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 $0 \leqslant i \leqslant n-1$ et $0 \leqslant j \leqslant 1$.

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).

Solution. Si n est pair, alors $|\langle r^2 \rangle| = n/2$ et si n est impair $|\langle r^2 \rangle| = |\langle r \rangle| = n$. On a donc que si n est pair $\langle r^2 \rangle$ est d'indice $4 = \frac{2n}{n/2}$ et si n est impair $\langle r^2 \rangle$ est d'indice $2 = \frac{2n}{n}$. Pour montrer que $\langle r^2 \rangle$ est distingué, il suffit de montrer que $gr^2g^{-1} \in \langle r^2 \rangle$ pour tout $g \in D_{2n}$. Posons $g = r^i s^j$ avec $0 \leqslant i \leqslant n-1$ et $j \in \{0,1\}$. Si $j = 0$ alors $gr^2g^{-1} = r^i r^2 r^{-i} = r^2 \in \langle r^2 \rangle$. D'autre part si $j = 1$, alors

$$gr^2g^{-1} = r^i s r^2 s r^{-i} = r^i s r r s r^{-i} = r^i r^{-1} s r s r^{-i} = r^i r^{-1} r^{-1} s^2 r^{-i} = r^i r^{-2} r^{-i} = r^{-2} = (r^2)^{-1} \in \langle r^2 \rangle.$$

□

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).

Solution. Comme $\langle r^2 \rangle$ est un sous-groupe distingué de D_{2n} d'indice 2 ou 4 (selon la parité de n), on a que le quotient $D_{2n}/\langle r^2 \rangle$ est un groupe d'ordre 2 ou 4 et donc en particulier abélien. Ainsi on peut appliquer l'inclusion **ii)** ci-dessus qui donne $D(G) \subseteq \langle r^2 \rangle$. □

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 $r^{-2} = srsr^{-1}$).

Solution. Ayant montré que $D(G) \subseteq \langle r^2 \rangle$, il reste à montrer que $\langle r^2 \rangle \subseteq D(G)$. D'après l'indication on a que r^2 $(= rsr^{-1}s)$ est un commutateur et donc appartient à $D(G)$. Il s'ensuit que chaque élément de $\langle r^2 \rangle$ est un produit de commutateur et donc dans $D(G)$. □

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.

Solution. Par application de la question 11., le nombre de représentations de D_{2n} de degré 1 est égal au cardinal de l'abélianisé de D_{2n}, c'est à dire l'ordre de $D_{2n}/\langle r^2 \rangle$. D'après la question 12. on a que $|D_{2n}/\langle r^2 \rangle|$ est égal à 4 si n est pair et 2 si n est impair. □