Contrôle final - Mardi 7 janvier 2025

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

Préambule : Par anneau on entend anneau unitaire. On notera (a) l'idéal engendré par un élément a d'un anneau commutatif.

Exercice 1. (Questions de cours) Soit R un anneau intègre. On note R^* l'ensemble des unités de R.

1. Rappeler la définition d'un élément *premier* et d'un élément *irréductible* de R.
2. Montrer que tout élément premier est irréductible.
3. Montrer que si $p \in R$ est premier et $u \in R^*$, alors up est premier.
4. Montrer que si $p_1 p_2 \cdots p_n = u q_1 q_2 \cdots q_m$ avec p_i premiers, q_j irréductibles et $u \in R^*$, alors $m = n$ et il existe une bijection σ de $\{1, 2, \ldots, n\}$ tel que p_i et $q_{\sigma(i)}$ sont associés pour tout $1 \leq i \leq n$. (Indication : On pourra procéder par récurrence sur $n \geq 1$.)

Solution. 1. Un élément $p \in R$ est dit premier s'il n'est ni nul ni inversible et si, pour tout produit ab divisible par p, l'un des deux facteurs a ou b est divisible par p. Un élément $p \in R$ est dit irréductible si $p \notin R^* \cup \{0\}$ et si $p = ab$ avec $a, b \in R$ alors $a \in R^*$ ou $b \in R^*$. □

Solution. 2. Soit $p \in R$ premier. Alors $p \notin R^* \cup \{0\}$. Montrons que si $p = ab$ avec $a, b \in R$ alors $a \in R^*$ ou $b \in R^*$. Comme p est premier et p divise ab ($1p = p = ab$), il s'ensuit que p divise a ou p divise b. Si p divise a, alors $a = rp$ pour un certain $r \in R$. Ainsi, $1p = ab = rpb$ ou encore $(1 - rb)p = 0$. Comme R est un anneau intègre et $p \neq 0$, il s'ensuit que $1 - rb = 0$ et donc $b \in R^*$. De même si p divise b on a que $a \in R^*$. □

Solution. 3. Soit $p \in R$ premier et $u \in R^*$. Montrons que up est premier. On remarque que $up \notin R^* \cup \{0\}$. Supposons que up divise un produit ab avec $a, b \in R$. Ainsi p divise ab et donc p divise a ou p divise b. Or si p divise a, alors $a = rp$ pour un certain $r \in R$. Mais alors $a = rp = 1rp = uu^{-1}rp$ qui montre que up divise a. De même si p divise b alors up divise b. □

Solution. 4. On procède par récurrence sur $n \geq 1$. Pour $n = 1$, on a $p_1 = u q_1 q_2 \cdots q_m$. Comme p_1 est premier et donc irréductible, on trouve que $m = 1$ et donc $p_1 = u q_1$ qui montre que p_1 et q_1 sont associés.

On fixe $n \geq 1$ et on suppose (hypothèse de récurrence) que si $p_1 p_2 \cdots p_n = u q_1 q_2 \cdots q_m$ avec p_i premiers, q_j irréductibles et $u \in R^*$, alors $m = n$ et il existe une bijection σ de $\{1, 2, \ldots, n\}$ tel que p_i et $q_{\sigma(i)}$ sont associés pour tout $1 \leq i \leq n$. On suppose $(*)$ $p_1 p_2 \cdots p_{n+1} = u q_1 q_2 \cdots q_m$. Comme p_1 est premier et divise le produit $u q_1 q_2 \cdots q_m$, il

s'ensuit que p_1 divise un des termes du produit. Or comme p_1 ne divise pas u (sinon p_1 serait inversible), on a que p_1 divise un certain q_j. Ainsi, quitte à échanger l'ordre des q_j, on peut supposer que p_1 divise q_1. Ainsi $q_1 = u_1 p_1$ avec $u_1 \in R^*$ (car q_1 est irréductible) qui montre que p_1 et q_1 sont associés. On a donc $(*)$ $p_1 p_2 \cdots p_{n+1} = u u_1 p_1 q_2 \cdots q_m$ qui implique $p_2 \cdots p_{n+1} = u' q_2 \cdots q_m$ avec $u' = u u_1 \in R^*$. Par application de l'hypothèse de récurrence on obtient que $m = n+1$ et qu'il existe une bijection σ de $\{2, \ldots, n+1\}$ tel que p_i et $q_{\sigma(i)}$ sont associés pour tout $2 \leq i \leq n+1$. □

Exercice 2. Le but de cet exercice est de démontrer la caractérisation suivante des anneaux factoriels du à Irving Kaplansky : Un anneau intègre R est factoriel si et seulement si tout idéal premier non-nul de R contient un élément premier. Vous pouvez utiliser les résultats obtenus dans l'exercice précédent.

1. Montrer que si R est un anneau factoriel et $P \neq (0)$ un idéal premier de R, alors P contient un élément premier de R. (**Rappel :** Un idéal premier est en particulier un idéal propre de R.)

   On pose
   $$S = R^* \cup \{p_1 p_2 \cdots p_n \,|\, n \geq 1, p_i \in R \text{ premiers}\}.$$

2. Montrer que R est factoriel si et seulement si $S = R \setminus \{0\}$.
3. Montrer que S est stable par produit : $a, b \in S \Rightarrow ab \in S$.
4. Montrer que pour tout $a, b \in R$, si $ab \in S$ alors $a \in S$ et $b \in S$.

   On suppose dorénavant que R n'est pas factoriel et on montrera l'existence d'un idéal premier $P \neq (0)$ qui ne contient aucun élément premier de R.

5. Montrer que si R n'est pas factoriel, alors il existe un élément $x_0 \in R$ non-nul avec $x_0 \notin S$. En déduire que $(x_0) \cap S = \emptyset$.
6. On pose
   $$\mathcal{Z} = \{I \subseteq R \,|\, I \text{ un idéal de } R \text{ contenant } x_0,\ I \cap S = \emptyset\}.$$
   Montrer par application du lemme de Zorn que $\mathcal{Z}$ admet un élément P_0 maximal par l'inclusion.
7. Montrer que P_0 est un idéal premier non-nul de R.
8. En déduire la caractérisation de Kaplansky.

Solution. 1. On suppose R factoriel. Soit P un idéal premier non-nul de R. Montrons que P contient un élément premier de R. Soit $x \in P$ avec $x \neq 0$. Comme P est premier et donc en particulier un idéal propre de R, on a que x n'est pas inversible. Ainsi comme R est factoriel on a $x = p_1 p_2 \cdots p_n$ avec $p_i \in R$ irréductibles et donc premiers (car dans un anneau factoriel un élément est premier si et seulement si il est irréductible). Or comme $p_1 p_2 \cdots p_n = x \in P$ et P est premier, il s'ensuit qu'il existe $1 \leq i \leq n$ avec $p_i \in P$. Ainsi P contient l'élément premier p_i. □

Solution. 2. On suppose d'abord R factoriel. Alors, pour tout $x \in R\setminus\{0\}$ on a que $x \in R^*$ ou $x = p_1p_2\cdots p_n$ avec p_i irréductibles. Si $x \in R^*$ alors $x \in S$, et si $x = p_1p_2\cdots p_n$ avec p_i irréductibles (et donc premiers), alors $x \in S$ car x est un produit d'éléments premiers de R. Cela montre que $R \setminus \{0\} \subseteq S$ et comme $0 \notin S$ on a que $S \subseteq R \setminus \{0\}$.

Supposons que $S = R \setminus \{0\}$ et montrons que R est factoriel. Il faut d'abord montrer que tout $x \in R \setminus (R^* \cup \{0\})$ peut s'écrire comme produit d'rréductibles. Or comme $x \in S$ mais $x \notin R^*$, il s'ensuit que x peut s'écrire comme un produit $p_1p_2\cdots p_n$ avec p_i premiers. Mais d'après la question 2. de l'exercice prédédent, tout élément premier est irréductible. Ainsi $x = p_1p_2\cdots p_n$ avec p_i irréductibles.

Il reste à montrer que si $q_1q_2\cdots q_k = r_1r_2\cdots r_l$ avec q_i et r_j irréductibles, alors $k = l$ et il existe une bijection de $\{1, 2, \ldots, k\}$ tel que q_i et $r_{\sigma(i)}$ sont associés pour tout $1 \leq i \leq k$. On pose $x = q_1q_2\cdots q_k = r_1r_2\cdots r_l$. Comme $x \neq 0$ on a que $x \in S$, et comme $x \notin R^*$, il s'ensuit que $x = p_1p_2\cdots p_n$ avec p_i premiers. Par application de la question 4. de l'exercice préceedent, on a que $n = k = r$ et qu'il existe deux bijections σ, τ de $\{1, 2, \ldots, n\}$ tels que $p_i, q_{\sigma(i)}$ et $r_{\tau(i)}$ sont associés pour tout $1 \leq i \leq n$. Ainsi pour tout $1 \leq j \leq k$ on a q_j et $r_{\tau(\sigma^{-1}(j)}$ sont associés. □

Solution. 3. Montrons que pour tout $a, b \in S$ on a $ab \in S$. Si $a, b \in R^*$, alors $ab \in R^* \subseteq S$. Si $a \in R^*$ et $b = p_1p_2\cdots p_n$ avec p_i premiers, alors $ab = ap_1p_2\cdots p_n \in S$ car ap_1 est premier (voir question 3. de l'exercice 1). De même si $b \in R^*$ et $a = p_1p_2\cdots p_n$ avec p_i premiers, alors $ab \in S$. Et si $a = p_1p_2\cdots p_n$ et $b = q_1q_2\cdots q_m$ avec p_i, q_j premiers, alors $ab = p_1p_2\cdots p_n \cdot q_1q_2\cdots q_m \in S$. □

Solution. 4. Soient $a, b \in R$ tels que $ab \in S$. Montrons que $a \in S$ et $b \in S$. Si $ab \in R^*$ alors $abr = 1$ pour un certain $r \in R$ qui montre que a et b sont inversibles et donc dans S. Si $ab = p_1p_2\cdots p_n$ avec p_i premiers, alors quitte à échanger l'ordre des p_i, on peut supposer que $p_1\cdots p_k$ divise a et $p_{k+1}\cdots p_n$ divise b pour un certain $0 \leq k \leq n$. Ainsi $a = rp_1\cdots p_k$ et $b = sp_{k+1}\cdots p_n$ avec $r, s \in R$. Or, $p_1p_2\cdots p_n = ab = rp_1\cdots p_k \cdot sp_{k+1}\cdots p_n = rsp_1p_2\cdots p_n$ et comme R est intègre, il s'ensuit que $rs = 1$ et donc $r, s \in R^* \subseteq S$. Ainsi $a \in S$ et $b \in S$. □

Solution. 5. Par application de la question 5., si R n'est pas factoriel alors S est une partie propre de $R \setminus \{0\}$ et donc il existe $x_0 \in R \setminus \{0\}$ avec $x_0 \notin S$. Montrons que $(x_0) \cap S = \emptyset$. En fait, si $rx_0 \in S$ pour un certain $r \in R$, alors d'après la question 4. on aurait $r \in S$ et $x_0 \in S$ qui est une contradiction car on avait supposé $x_0 \notin S$. Ainsi $(x_0 \cap S = \emptyset$. □

Solution. 6. On remarque que $\mathcal{Z}$ est un ensemble non-vide (car $(x_0) \in \mathcal{Z}$) partiellement ordonné par l'inclusion $\subseteq$. Montrons que toute chaîne $\mathcal{C}$ de $\mathcal{Z}$ possède un majorant dans $\mathcal{Z}$. Pour cela il suffit de prendre $\bigcup\mathcal{C}$. D'abord on a que $A \subseteq \bigcup\mathcal{C}$ pour tout $A \in \mathcal{C}$. De plus, omme $\mathcal{C}$ est une chaîne de $\mathcal{Z}$, on vérifie facilement que $\bigcup\mathcal{C}$ et un idéal de R contenant x_0. Ainsi pour montrer que $\bigcup\mathcal{C} \in \mathcal{Z}$ il suffit de montrer que $\bigcup\mathcal{C} \cap S = \emptyset$. Supposons au contraire que $\bigcup\mathcal{C} \cap S \neq \emptyset$. Soit $a \in \bigcup\mathcal{C} \cap S$. Ainsi il existe $A \in \mathcal{C}$ avec $a \in A$. Mais alors $A \cap S \neq \emptyset$ (car $a \in A \cap S$) qui est une contradiction car $A \in \mathcal{C} \subseteq \mathcal{Z}$. Ayant montré que toute chaîne $\mathcal{C}$ de $\mathcal{Z}$ admet un majorant dans $\mathcal{Z}$, on peut appliquer le lemme de Zorn pour obtenir l'existence d'un élément $P_0 \in \mathcal{Z}$ qui est maximal par l'inclusion. □

Solution. 7. Montrons que P_0 est un idéal premier non-nul de R. Or comme P_0 est dans $\mathcal{Z}$ on a que P_0 est un idéal non-nul (car $x_0 \in P_0$) et propre (car $P_0 \cap S = \emptyset$ et donc en particulier $1 \notin P_0$). Pour montrer que P_0 est premier il reste à montrer que pour tout $a, b \in R$, si $ab \in P_0$ alors $a \in P_0$ ou $b \in P_0$. Supposons au contraire que $ab \in P_0$ avec $a \notin P_0$ et $b \notin P_0$. Alors l'idéal P_0 est proprement inclus dans les idéaux $P_0 + (a)$ et $P_0 + (b)$. Ainsi par maximalité de P_0 dans $\mathcal{Z}$ on a que $P_0 + (a) \notin \mathcal{Z}$ et $P_0 + (b) \notin \mathcal{Z}$. Ainsi $(P_0 + (a)) \cap S \neq \emptyset$ et $(P_0 + (b)) \cap S \neq \emptyset$. Soit $x \in (P_0 + (a)) \cap S$ et $y \in (P_0 + (b)) \cap S$. Alors on peut écrire $x = p + ra$ et $y = p' + r'b$ avec $p, p' \in P_0$ et $r, r' \in R$. Mais alors $xy = p'' + rr'ab$ avec $p'' \in P_0$. Or, $xy \in S$ par la question 3. et comme $ab \in P_0$ on a que $p'' + rr'ab \in P_0$ qui montre que $P_0 \cap S \neq \emptyset$ (car $xy \in P_0 \cap S$) qui est une contradiction car $P_0 \in \mathcal{Z}$. Cela montre que si $ab \in P_0$ alors $a \in P_0$ ou $b \in P_0$ et donc P_0 est un idéal premier de R. □

Solution. 8. On vient de montrer que si R n'est pas factoriel, alors il existe un idéal premier $P_0 \neq (0)$ de R tel que $P_0 \cap S = \emptyset$. En particulier, P_0 ne contient aucun élément premier de R car tout élément premier de R est dans S. Dans la question 1. on a montré que si R est factoriel alors tout idéal premier $P \neq (0)$ de R contient un élément premier de R. Ainsi on retrouve la caractérisation de Kaplansky des anneaux factoriels énoncée au début de l'exercice. □

2 Corps

Préambule : Pour p premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$. Il sera admis que le groupe multiplicative $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ est cyclique. Étant donné une extension finie de corps E/F, le degré de E sur F (c.-à.-d. la dimension de E comme espace vectoriel sur F) sera noté par (E/F).

Exercice 3. On pose $g(x) = x^4 + 1$.

1. Montrer que $g(x)$ est irréductible dans $\mathbb{Q}[x]$.
2. Montrer que $E = \mathbb{Q}(i, \sqrt{2})$ est un corps de rupture de $g(x)$ sur $\mathbb{Q}$.
3. Trouver un corps de décomposition K de $g(x)$ sur $\mathbb{Q}$ ainsi que le degré de K sur $\mathbb{Q}$.
4. Montrer que $g(x)$ n'est pas irréductible dans $\mathbb{R}[x]$ et trouver une factorisation de $g(x)$ dans $\mathbb{R}[x]$ comme produit d'irréductibles.

   On propose de montrer que pour tout nombre premier p, le polynome $g(x)$ n'est pas irréductible dans $\mathbb{F}_p[x]$.

5. Montrer que si -1 est un carré dans $\mathbb{F}_p$ (par exemple quand $p = 2$) alors $g(x)$ peut s'écrire comme une différence de deux carrés et ainsi $g(x)$ peut se factoriser dans $\mathbb{F}_p[x]$ comme produit de deux polynômes de degré 2.
6. Montrer que si p est impair et que 2 ou -2 est un carré dans $\mathbb{F}_p$, alors $g(x)$ peut s'écrire comme une différence de deux carrés et ainsi $g(x)$ peut se factoriser dans $\mathbb{F}_p[x]$ comme produit de deux polynômes de degré 2.

7. Montrer que si p est impair, alors parmi $-1, 2$ et -2 il y a au moins un qui est un carré dans $\mathbb{F}_p$. En déduire que pour tout nombre premier p, $g(x)$ n'est pas irréductible dans $\mathbb{F}_p[x]$.

Solution. 1. Il suffit de montrer que $g(x)$ est irréductible dans $\mathbb{Z}[x]$. On remarque d'abord que $g(x) = x^4 + 1$ n'a pas de racines dans $\mathbb{R}$ (sinon on aurait $a^4 = -1$ pour un certain $a \in \mathbb{R}$). Ainsi si $g(x)$ peut se factoriser dans $\mathbb{Z}[x]$ (ou même dans $\mathbb{R}[x]$) on aurait $g(x) = p(x)q(x)$ avec $p(x), q(x)$ de degré 2. On pose $p(x) = x^2 + ax + b$ et $q(x) = x^2 + cx + d$ avec $a, b, c, d \in \mathbb{Z}$. On comparant le nombre de x^3 des deux côtés on trouve $a + c = 0$ ou $a = -c$. On comparant les x^2 des deux côtés on trouve $b + d + ac = 0$ ou $b + d = a^2$. On comparant les x des deux côtés on trouve $ad + bc = 0$ ou $a(d - b) = 0$ qui implique $a = 0$ ou $b = d$. Et on a $bd = 1$. Ainsi si $a = 0$ on obtient $b^2 = -1$ qui est impossible. D'autre part si $b = d$ alors $1 = bd = b^2$ et donc $b = \pm 1$. Mais cela donne $a^2 = b + d = 2b = \pm 2$ qui est impossible dans $\mathbb{Z}$ (mais possible dans $\mathbb{R}$.) . Ainsi $g(x)$ est irréductible dans $\mathbb{Z}[x]$ et donc irréductible dans $\mathbb{Q}[x]$.

On remarque que si on suppose $p(x), q(x) \in \mathbb{R}[x]$, alors si en posant $b = d = 1$ et $a = \sqrt{2}$ et $c = -\sqrt{2}$, on obtient la factorisation

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1) \in \mathbb{R}[x].$$

De plus ces deux polynômes dans $\mathbb{R}[x]$ sont irréductibles (car ils n'ont pas de racines dans $\mathbb{R}$). On peut utiliser cette factorisation de $g(x)$ dans $\mathbb{R}[x]$ pour donner une autre démonstration que $g(x)$ est irréductible dans $\mathbb{Q}[x]$. En fait, cette factorisation de $g(x)$ comme produit d'irréductibles dans $\mathbb{R}[x]$ est unique et donc s'il y avait une factorisation de $g(x)$ dans $\mathbb{Q}[x] \subseteq \mathbb{R}[x]$, elle donnerait lieu à la même factorisation que celle dans $\mathbb{R}[x]$. Mais $\sqrt{2} \notin \mathbb{Q}$. □

Solution. 2. Dans $\mathbb{C}$ on peut factoriser

$$g(x) = x^4 + 1 = (x^2 - i)(x^2 + i) = (x - \zeta)(x + \zeta)(x - \zeta^3)(x + \zeta^3)$$

où $\zeta = e^{\frac{2\pi i}{4}}$. Ainsi $\mathbb{Q}(\zeta)$ est un corps de rupture de $g(x)$ sur $\mathbb{Q}$. Il reste à montrer que $\mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{2})$. Or, $\zeta = \frac{1+i}{\sqrt{2}} \in \mathbb{Q}(i, \sqrt{2})$, et donc $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(i, \sqrt{2})$. On a que $i = \zeta^2 \in \mathbb{Q}(\zeta)$ et de plus comme $\zeta^{-1} = \frac{\sqrt{2}}{1+i} \in \mathbb{Q}(\zeta)$ et $1 + i \in \mathbb{Q}(\zeta)$ on obtient $\sqrt{2} \in \mathbb{Q}(\zeta)$. Ayant montré que $i, \sqrt{2} \in \mathbb{Q}(\zeta)$, on obtient $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\zeta)$. □

Solution. 3. Un corps de décomposition K de $g(x)$ est une extension minimale de $\mathbb{Q}$ contenant toutes les racines de $g(x)$. Ainsi, $K = \mathbb{Q}(\pm\zeta, \pm\zeta^3) = \mathbb{Q}(\zeta)$ qui est un corps de rupture du polynôme irréductible $g(x)$. Ainsi $(K/\mathbb{Q}) = \deg g(x) = 4$. □

Solution. 4. Voir la fin de la solution à la question 1. □

Solution. 5. Si $-1 = a^2$ avec $a \in \mathbb{F}_p$, alors

$$g(x) = x^4 + 1 = x^4 - (-1) = x^4 - a^2 = (x^2 - a)(x^2 + a).$$

□

Solution. 6. Si p est impair et $2 = a^2$ avec $a \in \mathbb{F}_p$ alors

$$g(x) = x^4 + 1 = x^4 + 2x^2 + 1 - 2x^2 = (x^2+1)^2 - (ax)^2 = (x^2 + 1 + ax)(x^2 + 1 - ax).$$

Si $-2 = a^2$ avec $a \in \mathbb{F}_p$ alors

$$g(x) = x^4 + 1 = x^4 - 2x^2 + 1 + 2x^2 = (x^2-1)^2 - (ax)^2 = (x^2 - 1 + ax)(x^2 - 1 - ax).$$

□

Solution. 7. On suppose p premier impair. Soit $a \in \mathbb{F}_p^\times$ est générateur du groupe cyclique $\mathbb{F}_p^\times$. Si -1 et 2 ne sont pas des carrés dans $\mathbb{F}_p$ alors on a que $-1 = a^n$ et $2 = a^m$ avec m et n impairs. Ainsi $-2 = a^{m+n} = a^{2k}$ car $m+n$ est pair. Par application des questions 5. et 6. on a montré que pour tout nombre premier p, le polynôme $g(x)$ peut se factoriser comme produit de deux polynômes de degré 2 sur $\mathbb{F}_p$ et donc n'est pas irréductible sur $\mathbb{F}_p$. □

Exercice 4. On pose $f(x) = x^4 + x^3 - 5x^2 + 3x + 1$. On remarque que $f(0) = f(1) = f(-3) = 1$.

1. Montrer que si $f(x) = p(x)q(x)$ avec $p(x), q(x) \in \mathbb{Z}[x]$, alors $p(x) = q(x)$.
2. En déduire que $f(x)$ est irréductible dans $\mathbb{Z}[x]$. **Indication :** On remarque que $f(-1) = -7 < 0$.
3. En déduire que $f(x)$ est irréductible dans $\mathbb{Q}[x]$ et que $\mathbb{Q}[x]/(f(x))$ est un corps de rupture de $f(x)$ sur $\mathbb{Q}$.
4. On pose $K = \mathbb{Q}(\alpha)$ où $\alpha \in \mathbb{C}$ est une racine de $f(x)$. Soit $g(x) \in \mathbb{Q}[x]$ un polynôme irréductible de degré 3. Montrer que $g(x)$ n'a pas de racines dans K.

Solution. 1. On suppose que $f(x) = p(x)q(x)$ avec $p(x), q(x) \in \mathbb{Z}[x]$. Or comme $f(0) = f(1) = f(-3) = 1$ on a que $p(a) = q(a) = \pm 1$ pour tout $a \in \{0, 1, -3\}$. Ainsi $p(x)$ et $q(x)$ sont de degrés ≥ 2 et donc on a que $\deg p(x) = \deg q(x) = 2$. Mais comme $p(a) = q(a)$ pour trois réels distincts ($a \in \{0, 1, -3\}$) on a que $p(x) = q(x)$. □

Solution. 2. On a vu dans la question précédente que si $f(x) = p(x)q(x)$ avec $p(x), q(x) \in \mathbb{Z}[x]$ alors $p(x) = q(x)$ qui veut dire que $f(x) = p^2(x)$. Mais comme $f(-1) = -7 < 0$, il s'ensuit que $f(x)$ n'est pas un carré. Cela montre que $f(x)$ est irréductible dans $\mathbb{Z}[x]$. □

Solution. 3. Comme $f(x)$ est irréductible dans $\mathbb{Z}[x]$, par application du lemme de Gauss il s'ensuit que $f(x)$ est irréductible dans $\mathbb{Q}[x]$. Ainsi (d'après les résultats de cours) $\mathbb{Q}[x]/(f(x))$ est un corps de rupture de $f(x)$ sur $\mathbb{Q}$. □

Solution. 4. On pose $K = \mathbb{Q}(\alpha)$ où $\alpha \in \mathbb{C}$ est une racine de $f(x)$. Alors K est un corps de rupture du polynôme irréductible $f(x)$ sur $\mathbb{Q}$. Ainsi $(K/Q) = \deg f(x) = 4$. Or, si $\beta \in K$ est racine d'un polynôme irréductible $g(x) \in \mathbb{Q}[x]$ de degré 3, alors on aurait $\mathbb{Q} \subseteq \mathbb{Q}(\beta) \subseteq K$ avec $(\mathbb{Q}(\beta)/\mathbb{Q}) = 3$. Mais alors $4 = (K/\mathbb{Q}) = (K/\mathbb{Q}(\beta))(\mathbb{Q}(\beta)/\mathbb{Q})$ qui est une contradiction car 4 n'est pas divisible pas 3. □

3 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 non-nul de dimension finie. La dimension de V est appelée le *degré* de la représentation ρ_V.

Exercice 5. On pose $G = \langle a, b, c \,|\, a^3 = b^3 = c^3 = 1\,;\, ac = ca\,;\, bc = cb\,;\, c = b^{-1}aba^{-1}\rangle$. Il sera admis que G est un groupe non-abélien d'ordre 27 ayant 11 classes de conjugaison. De plus tout $g \in G$ peut s'écrire de manière unique sous la forme $g = c^i b^j a^k$ avec $0 \leq i, j, k \leq 2$.

1. Montrer que pour toute représentation irréductible $\rho : G \to GL(V)$, on a que le degré de ρ est inférieur ou égal à 3.
2. Montrer que G admet neuf représentations de degré 1, aucune représentation irréductible de degré 2, et deux représentations irréductibles de degré 3. On notera ρ_i $(1 \leq 1 \leq 9)$ les neuf caractères de degré 1 (avec ρ_1 la représentation triviale) et χ_j $(j = 1, 2)$ les deux caractères irréductibles de G de degré 3.
3. Déterminer les neuf représentations ρ_i de G de degré 1. Il suffit de préciser les valeurs $\rho_i(a), \rho_i(b)$ et $\rho_i(c)$.
4. Montrer que le centre $Z(G) = \{1, c, c^2\}$. En déduire que $\{1\}, \{c\}, \{c^2\}$ sont des classes de conjugaison.
5. On pose
$$\omega = 2^{\frac{2\pi i}{3}} = \frac{-1 + \sqrt{3}i}{2}.$$
Montrer que pour tout $g \in G \setminus \{1, c, c^2\}$, ils existent $2 \leq i, j \leq 9$ tels que $\rho_i(g) = \omega$ et $\rho_j(g) = \omega^2$.
6. En déduire que $\chi_j(g) = 0$ pour tout $g \in G \setminus \{1, c, c^2\}$ et $j = 1, 2$. **Rappel :** Le produit d'un caractère de degré 1 avec un caractère irréductible est un caractère irréductible.
7. Montrer qu'il existe un caractère irréductible χ de G tel que $\chi(c) \notin \mathbb{R}$. **Indication :** Si $\chi(c) \in \mathbb{R}$, alors $\chi(c^2) = \chi(c)$. Pourquoi ?
8. En déduire que $\chi_j(c) \notin \mathbb{R}$ pour $j = 1, 2$ et que $\chi_2(g) = \overline{\chi_1(g)}$ pour tout $g \in G$.
9. Montrer que
$$\chi_1(c) = \frac{-3 \pm 3\sqrt{3}i}{2} \in \{3\omega, 3\omega^2\}.$$
10. **Bonus :** Compléter la table des caractères de G sans calculer explicitement les classes de conjugaison. Il faudra juste distinguer les classes de cardinalité 1 de $\{1, c, c^2\}$. Les autres classes on pourra les noter $[g_4], [g_5], \ldots, [g_{11}]$.

Solution. 1. G admet 11 classes de conjugaison et donc 11 représentations irréductibles. De plus, la somme des carrés des degrés des représentations irréductibles est égal à 27 qui est $|G|$. Ainsi, s'il y avait une représentation irréductible de degré 4, alors on aurait que $11 = 27 - 16 = d_1^2 + d_2^2 + \cdots + d_{10}^2$ avec $d_i \in \mathbb{N}^*$ qui est impossible. De même, G n'admet pas de représentations irréductibles de degré ≥ 5. □

Solution. 2. Pour $1 \leq i \leq 3$, on note n_i le nombre de représentations irréductibles de G de degré i. On a ainsi que $n_1 + 4n_2 + 9n_3 = 27$ et $n_1 + n_2 + n_3 = 11$. Ainsi $3n_2 + 8n_3 = 16$ et donc n_2 est divisible par 8 qui implique (par la première équation) que $n_2 = 0$. Ainsi $n_3 = 2$ et donc $n_1 = 11 - 2 = 9$. □

Solution. 3. Soit $\rho : G \to \mathbb{C}^*$ une représentation de degré 1. One pose $\alpha = \rho(a)$, $\beta = \rho(b)$ et $\gamma = \rho(c)$. Ainsi par application des relations dans G on trouve $\alpha^3 = \beta^3 = \gamma^3 = 1$ et $\gamma = \beta^{-1}\alpha\beta\alpha^{-1} = 1$. On note $\omega = e^{\frac{2\pi i}{3}}$. Ainsi, on a que $\alpha, \beta \in \{1, \omega, \omega^2\}$ et $\gamma = 1$. Comme on a 3 choix pour α et 3 choix pour β on retrouve les 9 caractères de degré 1 dans la question précédente. □

Solution. 4. On remarque dans les relations de G que l'élément c commute avec a et b. Comme G est engendré par a, b, c, il s'ensuit que c (et donc aussi c^2) est dans le centre de G. Ainsi $\{1, c, c^2\} \subseteq Z(G)$. Montrons que $|Z(G)| = 3$. Comme G est non-abélien, si $|Z(G)| > 3$, on aurait que $|Z(G)| = 9$. Si $|Z(G)| = 9$, alors pour tout $x \in G \setminus Z(G)$ on aurait que $|C(x)| = 27$ où $C(x) = \{g \in G \,|\, gx = xg\}$. En fait $Z(G) \cup \{x\} \subseteq C(x)$ et donc $|C(x)| \geq 10$. D'autre part, comme $C(x)$ est un sous-groupe de G, son cardinal divise 27. Or, si $|C(x)| = 27$, alors $C(x) = G$ et donc $x \in Z(G)$, une contradiction. Pour tout $z \in Z(G)$ on a que la classe de conjugaison $[z] = \{gzg^{-1} \,|\, g \in G\} = \{z\}$. □

Solution. 5. Soit $g \in G \setminus \{1, c, c^2\}$. Alors on peut écrire $g = c^r b^s a^t$ avec avec $0 \leq r, s, t \leq 2$ et $s \neq 0$ ou $t \neq 0$. On peut supposer que $s \neq 0$ et donc $s = 1, 2$. On pose $\rho, \rho' : G \to \mathbb{C}^*$ avec $\rho(a) = \rho(c) = 1$ et $\rho(b) = \omega$ et $\rho'(a) = \rho'(c) = 1$ et $\rho'(b) = \omega^2$. Ainsi, si $s = 1$, il suffit de prendre $\rho_i = \rho$ et $\rho_j = \rho'$ et si $s = 2$ on prends $\rho_i = \rho'$ et $\rho_j = \rho$. □

Solution. 6. Supposons au contraire qu'il existe $g \in G \setminus \{1, c, c^2\}$ et un caractère irréductible χ de G de degré 3 tel que $\chi(g) \neq 0$. Par la question précédente il existe $2 \leq i, j \leq 9$ tels que $\rho_i(g) = \omega$ et $\rho_j(g) = \omega^2$. Ainsi $\chi, p_i\chi$ et $\rho_j\chi$ sont trois caractères irréductibles de degré 3 distincts (car $\chi(g), \rho_i(g)\chi(g) = \omega\chi(g)$ et $\rho_j(g)\chi(g) = \omega^2\chi(g)$ sont deux à deux distincts). Cela est en contradiction avec la question 2 car G admet seulement deux caractères irréductibles de degré 3. □

Solution. 7. Supposons au contraire que $\chi(c) \in \mathbb{R}$ pour tout caractère irréductible χ de G. Alors $\chi(c^2) = \chi(c^{-1}) = \overline{\chi(c)} = \chi(c)$. Ainsi, dans la table des caractères de G on aurait que la colonne correspondant à la classe de conjugaison $\{c\}$ est égal à la colonne correspondant à la classe de conjugaison $\{c^2\}$. Cela est une contradiction car les colonnes dans la table des caractères de G sont orthonormaux. □

Solution. 8. Dans la question 3. on a montré que $\rho_i(c) = 1 \in \mathbb{R}$ pour tout $1 \leq i \leq 9$. Ainsi par application de la question 7., il s'ensuit que $\chi_1(c) \notin \mathbb{R}$ ou $\chi_2(c) \notin \mathbb{R}$. On peut supposer que $\chi_1(c) \notin R$. Ainsi on pose $\chi_1(c) = z = r + si$ et $\chi_2(c) = z' = r' + s'i$ avec $s \neq 0$. Or, l'orthogonalité des colonnes $\{1\}$ et $\{c\}$ donne $9 + 3z + 3z' = 0$ ainsi $z + z' = -3 \in \mathbb{R}$ et donc $s' = -s$. D'autre part l'orthogonalité des colonnes $\{c\}$ et $\{c^2\}$ donne $9 + z^2 + z'^2 = 0$ et donc $0 = \mathrm{Im}(z^2 + z'^2) = 2s(r - r')$. Ainsi $r = r'$ et donc $z' = \overline{z}$, c.à.d., $\chi_2(c) = \overline{\chi_1(c)}$. On a aussi que $\chi_1(c^2) = \overline{\chi_1(c)} = \chi_2(c)$ et $\chi_2(c^2) = \chi_1(c)$. Pour tout $g \in G \setminus \{1, c, c^2\}$ on a $\chi_j(g) = 0$ pour $j = 1, 2$. Ainsi $\chi_1(g) = \overline{\chi_2(g)}$ pour tout $g \in G$. □

Solution. 9. Dans la question précédente on a montré que $\chi_1(c) + \chi_2(c) = z + z' = z + \overline{z} = 2r = -3$ et donc $r = -3/2$. En prenant le produit scalaire de la colonne $\{c\}$ avec elle même on trouve $27 = 9 + |z|^2 + |\overline{z}|^2 = 9 + 2|z|^2$ et donc $|z| = 3$. Ainsi $s = \pm\sqrt{3^2 - (-3/2)^2} = \pm\sqrt{27/4} = \pm 3\sqrt{3}/2$. □