Algèbre

Corrigé examen final

I - Restes chinois (3 points)

1. Théorème des restes chinois sur $\mathbb{Z}$:
   Soient $n, m \in \mathbb{N}$ premiers entre eux, et $a, b \in \mathbb{Z}$. Alors le système $\begin{cases} x \equiv & a & \mod m \\ x \equiv & b & \mod n \end{cases}$ admet des solutions, et si x_0 est une solution, alors l'ensemble des solutions est $\{x_0 + knm;\ k \in \mathbb{Z}\}$.

2. Pour résoudre le système : $\begin{cases} 2x \equiv & 3 & \mod 5 \\ 3x \equiv & 2 & \mod 4 \end{cases}$, on commence par enlever les coefficients devant les x. Pour cela il suffit de multiplier la première ligne par 3 (inverse de 2 modulo 5) et la seconde par 3 (inverse de 3 modulo 4). On obtient le système équivalent

$$\begin{cases} x \equiv & 4 & \mod 5 \\ x \equiv & 2 & \mod 4 \end{cases}$$

   On remarque que 14 est solution, et par le théorème des restes chinois l'ensemble des solutions est $\{14 + 20k;\ k \in \mathbb{Z}\}$.

II - Exemples (4,5 points)

1. $\bar{0}$ et $X^2 + X$ sont deux polynômes distincts dans $(\mathbb{Z}/2\mathbb{Z})[X]$ qui définissent la même fonction (à savoir la fonction nulle) de $\mathbb{Z}/2\mathbb{Z}$ vers $\mathbb{Z}/2\mathbb{Z}$.

2. $\mathbb{Z}$ et $\mathbb{R}[X]$ sont deux exemples typiques d'anneaux euclidiens.

3. $\mathbb{Z}[X]$ et $\mathbb{R}[X,Y]$ sont deux exemples typiques d'anneaux factoriels mais non principaux.

4. La matrice $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ ne commute pas avec $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

5. $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ sont deux exemples de transvections dans $\mathrm{SL}_3(\mathbb{R})$.

6. En collant deux tétraèdres le long d'une face on obtient un polyèdre dont les six faces sont des triangles équilatéraux, mais qui n'est pas régulier : 2 sommets sont de valence 3, les 3 autres sommets sont de valence 4. (complément : il existe un seul autre exemple, qui s'obtient en recollant deux pyramides de base un pentagone régulier).

III - Le groupe alterné A_4 (4 points).

1. Considérons l'action par conjugaison du groupe A_4 sur l'ensemble X des 3-cycles :

$$\begin{aligned} A_4 \times X &\to X \\ \sigma, (i\,j\,k) &\mapsto (\sigma(i)\,\sigma(j)\,\sigma(k)) \end{aligned}$$

   La classe de conjugaison d'un 3-cycle $(i\,j\,k)$ correspond à l'orbite de $(i\,j\,k)$, dont le cardinal est donné par la formule

$$|\mathrm{Orb}(i\,j\,k)| = \frac{|A_4|}{|\mathrm{Stab}(i\,j\,k)|}$$

   Comme $|A_4| = 12$ et $|\mathrm{Stab}(i\,j\,k)| \geq 3$ (car $\langle (i\,j\,k) \rangle \subseteq \mathrm{Stab}(i\,j\,k)$), on obtient $|\mathrm{Orb}(i\,j\,k)| \leq 4$. Par ailleurs en considérant les conjugaison par les doubles transpositions on voit que $|\mathrm{Orb}(i\,j\,k)| \geq 4$. En conclusion il y a exactement deux classes de conjugaison de 3-cycles dans A_4.

2. Outre les deux classes de conjugaison de 3-cycles dans A_4, chacune de cardinal 4, il y a la classe de conjugaison des double transpositions (cardinal 3), et la classe de l'identité (cardinal 1).

3. Si $\mathcal{T}$ est un tétraèdre régulier de sommets p_1, p_2, p_3, p_4, on obtient un isomorphisme de $\mathrm{Isom}^+(\mathcal{T})$ vers A_4 en posant

$$\begin{aligned} \mathrm{Isom}^+(\mathcal{T}) &\to A_4 \\ f \quad &\mapsto \sigma \text{ telle que } f(p_i) = p_{\sigma(i)}. \end{aligned}$$

   En effet ce morphisme est injectif, et le tétraèdre ayant 6 arêtes, on a $|\mathrm{Isom}^+(\mathcal{T})| = 12 = |A_4|$.

4.
   - $(1\,2\,3)$ correspond à une rotation d'angle $2\pi/3$ et d'axe passant par le sommet p_4 (idem pour le 3-cycle inverse $(1\,3\,2)$, qui n'est pas dans la même classe de conjugaison).
   - La double transposition $(1\,2)(3\,4)$ correspond à une rotation d'angle π (aussi appelé retournement) d'axe passant par les milieux des arêtes $[p_1, p_2]$ et $[p_3, p_4]$.
   - la permutation identité correspond bien sûr à l'identité.

IV - Anneaux de polynômes (4,5 points)

1. Si $Q(X) \in \mathbb{Z}[X]$ est primitif (PGCD des coefficient égal 1), alors $Q(X)$ est irréductible sur $\mathbb{Z}$ si et seulement s'il est irréductible sur $\mathbb{Q}$.

2. Si $p \in \mathbb{N}$ est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps et donc l'anneau $(\mathbb{Z}/p\mathbb{Z})[X]$ est euclidien, donc principal et factoriel.

3. De façon générale, si K est un corps (comme ici $\mathbb{Z}/3\mathbb{Z}$), et $R \in K[X]$ est de degré 3, alors si R est réductible il admet un facteur de degré 1, ce qui revient à dire que R admet une racine dans K.

4. Par la question 1 le polynôme $P = 5X^3 + 8X^2 + 6X + 2$ étant primitif, il est irréductible sur $\mathbb{Q}$ si et seulement s'il est irréductible sur $\mathbb{Z}$. Ce dernier point découle alors du critère d'Eiseinstein, appliqué avec le nombre premier 2.

5. Par la question 3 il s'agit de vérifier si l'un des trois éléments du corps $\mathbb{Z}/3\mathbb{Z}$ est racine de $\bar{P}$. On observe que $\bar{1}$ est racine, et on en déduit la factorisation dans$(\mathbb{Z}/3\mathbb{Z})[X]$:

$$\bar{P} = \bar{5}X^3 + \bar{8}X^2 + \bar{6}X + \bar{2} = (X - \bar{1})(-X^2 + X + \bar{1}).$$

6. L'anneau quotient $A = \mathbb{Q}[X]/(P)$ est intégre, car P étant irréductible dans l'anneau euclidien $\mathbb{Q}[X]$ il engendre un idéal premier (complément : en fait $\mathbb{Q}[X]/(P)$ est même un corps, car l'idéal est maximal). L'anneau quotient $B = (\mathbb{Z}/3\mathbb{Z})[X]/(\bar{P})$ n'est pas intègre, en effet $X - \bar{1}$ est un diviseur de zéro par la relation établi à la question précédente.

V - Quizz (6 points).

1. Tout groupe commutatif fini est cyclique : faux, un contre-exemple est $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2. Il existe une action transitive (c'est-à-dire avec une seule orbite) d'un groupe à 4 éléments sur un ensemble à 2 éléments : vrai, par exemple si G est le groupe cyclique d'ordre 4 des rotations préservant un carré, considérer l'action de G sur les deux diagonales du carré.

3. Le groupe des isométries directes de $\mathbb{R}^3$ préservant un icosaèdre est simple : vrai, on a vu en cours d'une part que ce groupe est isomorphe au groupe alterné A_5, et d'autre part que A_5 est un groupe simple.

4. Si A est un anneau principal alors l'anneau de polynômes $A[X]$ est également principal : faux, un contre-exemple est donné par l'anneau principal $\mathbb{Z}$, car $\mathbb{Z}[X]$ n'est pas principal, comme on le voit en considérant l'idéal $(2,X)$ (complément : en fait on peut montrer que c'est toujours faux, sauf quand A est un corps).

5. Les anneaux quotients $\mathbb{R}[X]/(X^2-1)$ et $\mathbb{R}[X]/(X^2-2X+1)$ sont isomorphes : faux, on a $X^2-2X+1=(X-1)^2$ donc la classe $\overline{X-1} \in \mathbb{R}[X]/(X^2-2X+1)$ est un élement non nul de carré nul, et il n'existe pas de tel élément dans $\mathbb{R}[X]/(X^2-2X+1) \simeq \mathbb{R}[X]/(X-1) \times \mathbb{R}[X]/(X+1)$.

6. L'anneau quotient $\mathbb{Z}[X]/(X^2+1)$ est principal : vrai, cet anneau est isomorphe à $\mathbb{Z}[i]$ qui est euclidien, donc principal (l'isomorphisme s'obtient en appliquant le théorème d'isomorphisme au morphisme $P(X) \in \mathbb{Z}[X] \mapsto P(i) \in \mathbb{Z}[i]$.

7. L'anneau quotient $(\mathbb{Z}/2\mathbb{Z})[X]/(X^3+X)$ contient exactement 8 éléments : vrai, un système de représentant est donné par les polynômes de degré 2 : $\bar{a}+\bar{b}X+\bar{c}X^2$, où $\bar{a},\bar{b},\bar{c}$ sont dans $\mathbb{Z}/2\mathbb{Z}$, d'où 8 possibilités.

8. Pour tout polynôme $P(X) \in \mathbb{R}[X]$ de degré 1 l'anneau quotient $\mathbb{R}[X]/(P)$ est un corps : vrai, et plus précisément $\mathbb{R}[X]/(P)$ est isomorphe à $\mathbb{R}$. Si $P(X)=a+bX$, $\alpha=-a/b$ est racine de P, et il suffit d'appliquer le théorème d'isomorphisme au morphisme $P(X) \in \mathbb{R}[X] \mapsto P(\alpha)$, dont le noyau est bien l'idéal (P).