16 décembre 2015
L3
Mathématiques

UNIVERSITÉ de Cergy-Pontoise

STRUCTURES ALGÉBRIQUES

Aucun document autorisé, calculatrice et téléphone interdits. Barème indicatif.

Toute réponse doit être justifiée.

Petites Questions (4 points + 1 de bonus si au moins deux bonnes réponses)**.**

a) Décrire les idéaux de l'anneau euclidien $\mathbb{Z}[i]$ et démontrer que tout idéal non réduit à $\{0\}$ contient un nombre entier positif non nul.

b) Écrire la décomposition en cycles disjoints, puis calculer le signe et l'ordre de la permutation σ de S_8:

$$\sigma = (5236)(134)(28)(347).$$

c) Dire si les polynômes f et g sont dans la même classe de l'anneau quotient $\mathbb{R}[x]/(x^2-2)$:

$$f = 4x^5 - 9x^3 - 5, \quad g = -3x^4 + x^2 - 2x + 5$$

d) Donner le nombre d'éléments d'ordre 2 dans les groupes diédraux D_{128} et dans D_{129}.

Exercice 1 (3 points)**.**

a) Soient G et H deux groupes et soit $\varphi : G \to H$ un morphisme de groupes. Soit $g \in G$ un élément d'ordre fini n. Démontrer que l'ordre de $\varphi(g)$ divise n.

b) Trouver tous les morphismes de groupes

$$\varphi : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \qquad \text{et} \qquad \varphi : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}.$$

c) Soient p un nombre premier et $2 \leq n \in \mathbb{N}$. Donner une condition, nécessaire et suffisante sur p et n, pour qu'il existe un morphisme de groupes non trivial (i.e. non nul)

$$\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}.$$

Dans ce cas, combien en existent-ils ? Justifier la réponse.

Exercice 2 (4 points)**.** Pour tout anneau R on note par $R^\star$ le groupe multiplicatif des inversibles. Soit

$$A = (\mathbb{Z}/3\mathbb{Z})[x], \qquad f = x^4 + \bar{2}x^3 + \bar{2}x + \bar{2} \in A.$$

a) Lister les polynômes unitaires irréductibles de degré 2 de $(\mathbb{Z}/3\mathbb{Z})[x]$.

b) Factoriser f comme produit d'irréductibles de A.

c) En utilisant le lemme chinois, écrire un isomorphisme d'anneaux explicite entre $A/(f)$ et un produit direct de deux anneaux, on les note A_1 et A_2.

d) Calculer $|A_1^\star|$, $|A_2^\star|$. À quel groupe connu sont isomorphes $A_1^\star$ et $A_2^\star$ et pourquoi?

TOURNER SVP

Exercice 3 (4 points)**.**

a) Donner les décompositions possibles en cycles disjoints d'un élément d'ordre 6 dans S_5. En déduire le nombre d'éléments d'ordre 6 de S_5.

b) Combien de générateurs a un groupe cyclique de cardinal 6? En déduire le nombre de sous-groupes cycliques de cardinal 6 de S_5.

c) Rappeler un résultat du cours de classification (à isomorphisme près) des groupes de cardinal 6.

d) Expliquer comment trouver au moins 10 sous-groupes de S_5 de cardinal 6 mais pas cycliques.

Exercice 4 (8 points)**.** Dans cet exercice A est un sous anneau de $\mathbb{Q}$, $A^\star$ est le sous-ensemble des inversibles de A, et $\mathcal{P} = \{p \in \mathbb{N} \,|\, p \text{ premier}\}$ est l'ensemble des nombres premiers positifs de $\mathbb{Z}$.

Si $S \subseteq \mathcal{P}$ on note par $\mathbb{Z}_S \subseteq \mathbb{Q}$ l'ensemble des nombres rationnels tels que tous les facteurs premiers du dénominateur sont dans S. En particulier $\mathbb{Z} \subseteq \mathbb{Z}_S$. On a

$$\mathbb{Z}_S = \{\frac{m}{n} \,|\, m \in \mathbb{Z}, n \in \mathbb{N} \setminus \{0\} \text{ tel que } \forall p \in \mathcal{P},\ p|n \Rightarrow p \in S\}.$$

Par exemple $\mathbb{Z}_{\mathcal{P}} = \mathbb{Q}$ et

$$\mathbb{Z}_{\{2,3\}} = \{\frac{m}{2^r 3^s} \,|\, m \in \mathbb{Z}, r, s \in \mathbb{N}\}.$$

Le but de l'exercice est de démontrer que tous les sous-anneaux de $\mathbb{Q}$ sont de ce type et, puis, de démontrer qu'ils sont tous factoriels.

a) Démontrer que $\mathbb{Z}_{\{2,3\}}$ est un sous-anneau de $\mathbb{Q}$.

b) Pour tout $S \subseteq \mathcal{P}$ (donc même de cardinal infini), démontrer que $\mathbb{Z}_S$ est un sous-anneau de $\mathbb{Q}$.

c) Soit $S = A^\star \cap \mathcal{P}$. Démontrer que $\mathbb{Z}_S \subset A$.

d) Démontrer que si $\frac{m}{n} \in A$, avec $m \wedge n = 1$, alors $\frac{1}{n} \in A$

e) En déduire que $A = \mathbb{Z}_S$.

f) Soit I un idéal de A. Démontrer que $I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$, puis démontrer que I est principal.

g) Démontrer que tout sous-anneau de $\mathbb{Q}$ est factoriel.

h) Soit D un anneau principal et soit $Q = Frac(D)$. Que peut on dire, en justifiant la réponse, sur les sous-anneaux de Q?

CORRIGE

P.Q. a) $\mathbb{Z}[i]$ est euclidien, donc principal. Si I est un idéal de $\mathbb{Z}[i]$ différent de $\{0\}$ il existe $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ t.q. $I = (a+ib)$

Puisque I est un idéal $\forall z \in \mathbb{Z}[i]$ $z(a+ib) \in I$ Si on prend $z = a-ib$

on a $(a-ib)(a+ib) = a^2+b^2 \in I \cap (\mathbb{N}\setminus\{0\})$

b) $\sigma = (16\,5\,2\,8\,3)(4\,7) \Rightarrow |\sigma| = 6 \vee 2 = 6$; $\operatorname{sgn}\sigma = (-1)^{6-1}(-1)^{2-1} = +1$

c) $f + (x^2-2) = g + (x^2-2) \iff x^2-2 \mid f-g$ ce qui est le cas car

$$
\begin{array}{l|l}
4x^5+3x^4-9x^3-x^2+2x-10 & x^2-2 \\
\cline{2-2}
-4x^5 \qquad +8x^3 & 4x^3+3x^2-x+5 \\
\cline{1-1}
3x^4-x^3-x^2+2x-10 & \\
-3x^4 \qquad +6x^2 & \\
\cline{1-1}
-x^3+5x^2+2x-10 & \\
+x^3 \qquad -2x & \\
\cline{1-1}
5x^2-10 & \\
-5x^2+10 & \\
\cline{1-1}
0 &
\end{array}
$$

d) $D_{128} = \{R^i, S_1, \dots, S_{128} \mid i = 0, \dots, 127\}$ $\begin{cases} \forall j = 1,\dots,128 \\ |S_j| = 2 \\ |R| = 128 \end{cases}$ $2 \mid 128 \Rightarrow \exists^{\varphi(2)=1}$ 1 élément d'ordre 2 dans $\langle R \rangle$

donc 129 éléments d'ordre 2 dans D_{128}

$D_{129} = \{R^i, S_1, \dots, S_{129} \mid i = 0, \dots, 128\}$ $|S_j| = 2$, $\forall j = 1,\dots,129$ $|R| = 129$ $2 \nmid 129$

$\Rightarrow \nexists$ élément d'ordre 2 dans $\langle R \rangle$

donc 129 éléments d'ordre 2 dans D_{129}

Exercice 1 a) $g^n = 1 \Rightarrow \varphi(g^n) = \varphi(g)^n = 1 \Rightarrow |\varphi(g)| \mid n$

b) $\mathbb{Z}/3\mathbb{Z}$ est cyclique $\Rightarrow \varphi$ est déterminé par l'image d'un générateur.

$\bar{1}$ est un générateur et il a ordre 3 $\Rightarrow \varphi(\bar{1}) =$ / $\bar{0}$ ou élément d'ordre 3 à cause de a)

puisque $|\varphi(\bar{1})| \mid 4$ par Lagrange on a que le seul morphisme $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ est le trivial $(\bar{1} \mapsto \bar{0})$

Par contre on a 3 morphismes $\varphi : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ $\bar{1} \mapsto$ $\bar{0}$ (morphisme trivial), $\bar{2}$ (élément d'ordre 3), $\bar{4}$ (élément d'ordre 3)

c) Si $p \mid n$ il y a $p-1$ éléments d'ordre p dans $\mathbb{Z}/n\mathbb{Z}$, si $p \nmid n$ aucun

Donc le même argument que en b) nous donne que l'on doit avoir $p \mid n$ et dans ce cas il y a $p-1$ morphismes non triviaux.

Exercice 2

a) $x^2 + \bar{1}$, $x^2 + x + \bar{2}$, $x^2 + \bar{2}x + \bar{2}$

b) $x^4 + \bar{2}x^3 + \bar{2}x + \bar{2} = x^4 - \bar{1} + \bar{2}x(x^2 + \bar{1}) = (x^2+\bar{1})(x^2 - \bar{1} + \bar{2}x) = (x^2+\bar{1})(x^2 + \bar{2}x + \bar{2})$

c) $A/(f) \simeq \frac{\mathbb{Z}/3\mathbb{Z}[x]}{(x^2+\bar{1})} \times \frac{\mathbb{Z}/3\mathbb{Z}[x]}{(x^2+\bar{2}x+\bar{2})} = A_1 \times A_2$ car $x^2+\bar{1} \wedge x^2+\bar{2}x+\bar{2} = \bar{1}$

$a + (f) \mapsto \left(a + (x^2+\bar{1}),\ a + (x^2+\bar{2}x+\bar{2}) \right)$ $\forall a \in A$.

d) A_1, A_2 corps car $x^2+\bar{1}$ et $x^2+\bar{2}x+\bar{2}$ irréductibles Donc A_1^* et A_2^* sont des gps cycliques (car, théorème, le gpe multiplicatif d'un corps fini est cyclique)

$|A_2^*| = |A_2| - 1 = 3^2 - 1 = 8 = |A_2^*| \Rightarrow A_1^* \simeq A_2^* \simeq \mathbb{Z}/8\mathbb{Z}$

Exercice 3

a) $\sigma \in S_5$, $|\sigma| = 6 \Rightarrow \sigma = (abc)(de)$ avec $\{a,b,c,d,e\} = \{1,2,3,4,5\}$

Compter ces éléments revient à compter les cycles de longueur 3 dans S_5

(car il existe une unique façon de compléter (abc) avec un 2-cycle disjoint)

$\Rightarrow$ on a $\binom{5}{3} \times 2! = 20$ éléments d'ordre 6 dans S_5

b) un gp cyclique de cardinal 6 a $\varphi(6) = \varphi(3)\varphi(2) = 2$ générateurs $\Rightarrow$

il y a $\frac{20}{2} = 10$ sous gps cycliques de S_5 de cardinal 6

c) Si G est un gp de cardinal 6 alors G est isomorphe soit à $\mathbb{Z}/6\mathbb{Z}$ soit à S_3

d) $\forall \{a,b\} \subseteq \{1,2,3,4,5\}$ le sous gp $H_{\{a,b\}} = \{\sigma \in S_5 \mid \sigma(a) = a, \sigma(b) = b\}$ est

isomorphe à S_3 via $H_{\{a,b\}} \xrightarrow{\sim} S_{\overline{\{a,b\}}} \simeq S_3$ où $\overline{\{a,b\}} = \{1,2,3,4,5\} \setminus \{a,b\}$

$\sigma \mapsto \sigma|_{\overline{\{a,b\}}}$

$\Rightarrow$ on a $\binom{5}{2} = 10$ sous gps de S_5 isomorphes à S_3

Exercice 4

a) Il faut vérifier $1 \in \mathbb{Z}_{\{2,3\}}$ et $q_1, q_2 \in \mathbb{Z}_{\{2,3\}} \Rightarrow q_1 q_2 \in \mathbb{Z}_{\{2,3\}}$, $q_1 - q_2 \in \mathbb{Z}_{\{2,3\}}$

Par def $\mathbb{Z} \subseteq \mathbb{Z}_{\{2,3\}}$ donc $1 \in \mathbb{Z}_{\{2,3\}}$ en plus ecrit $q_1 = \frac{m}{2^r 3^s}$, $q_2 = \frac{n}{2^t 3^z}$ alors

$q_1 q_2 = \frac{mn}{2^{r+t} 3^{s+z}} \in \mathbb{Z}_{\{2,3\}}$ et $q_1 - q_2 = \frac{m 2^t 3^z - n 2^r 3^s}{2^{r+t} 3^{s+z}} \in \mathbb{Z}_{\{2,3\}}$

b) Encore une fois $1 \in \mathbb{Z}_S$ car $\mathbb{Z} \subseteq \mathbb{Z}_S$ en plus soit $\begin{cases} q_1 = \frac{m}{n}, q_2 = \frac{r}{s} \\ q_1, q_2 \in \mathbb{Z}_S \end{cases}$

alors $q_1 q_2 = \frac{mr}{ns}$ et $\forall p \in \mathcal{P} : p \mid ns \Rightarrow p \mid m$ ou $p \mid s$ Donc $p \in S$

$q_1 - q_2 = \frac{sm - rn}{ns}$ et $p \mid ns \Rightarrow p \mid m$ ou $p \mid s$ Donc $p \in S$

c) A sous anneau de $\mathbb{Q}$, $S = A^* \cap \mathcal{P} \Rightarrow \forall p \in S$ on a $\frac{1}{p} \in A$

Soit $\frac{m}{n} \in \mathbb{Z}_S$ et soit $m = p_1^{d_1} \cdots p_r^{d_r}$ la factorisation de n comme produit de premiers dans $\mathbb{Z}$.

alors $p_i \in S$ donc $\frac{1}{p_i}, \left(\frac{1}{p_i}\right)^{d_i}, m \cdot \frac{1}{p_i^{d_i}} \in A$ ie $\frac{m}{n} \in A$

d) $m \wedge n = 1 \Rightarrow \exists \alpha, \beta \in \mathbb{Z}$ et $1 = \alpha m + \beta n$ alors puisque $m/n \in A$, $\mathbb{Z} \subseteq A$, A sous anneau de $\mathbb{Q}$

$\frac{1}{n} = \frac{\alpha m + \beta n}{n} = \alpha \frac{m}{n} + \beta \in A$

e) Soit $m/n \in A$ $m \wedge n = 1$ $\forall p \in \mathcal{P}$ t.q. $p \mid n$ on pose $n = n'p$

On a $A \ni \frac{1}{n} \Rightarrow n' \cdot \frac{1}{n} = \frac{1}{p} \in A \Rightarrow p \in S$ et donc $m/n \in \mathbb{Z}_S$

f) $0 \in I \cap \mathbb{Z}$ en plus $a, b \in I \cap \mathbb{Z} \Rightarrow a - b \in I \cap \mathbb{Z}$ car I idéal de A et $\mathbb{Z}$ sous anneau de A

si $z \in \mathbb{Z} \subseteq A$ et $x \in I \cap \mathbb{Z}$ alors $z \cdot x \in I$ car I idéal et $z \cdot x \in \mathbb{Z}$ car $\mathbb{Z}$ anneau. Donc ie $\exists n \in \mathbb{N}$ et $I \cap \mathbb{Z} = n\mathbb{Z}$. On veut d.q. $I = nA$. On a $n \in I$, I idéal $\Rightarrow nA \subseteq I$

Vice versa si $x \in I$ $x = \frac{r}{s} \Rightarrow r = sx \in I \cap \mathbb{Z} = n\mathbb{Z} \Rightarrow \exists z \in \mathbb{Z}$ et $r = nz$

$r/s \in I \subseteq A \Rightarrow \frac{1}{s} \in A$ donc $x = \frac{nz}{s} = n z \cdot \frac{1}{s} \in nA$

g) Puisque A est principal on a que A est factoriel

h) Dans ce qui précède on a seulement utilisé que $\mathbb{Z}$ est principal et $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$

$\Rightarrow$

on peut dire que tous les sous anneaux de $\mathbb{Q}$ sont principaux (donc factoriels)

et qu'ils sont du type $D_S = \left\{ \frac{m}{n} \in \mathbb{Q} \;\middle|\; n \wedge m = 1 \text{ et } \forall p \in P \;\; p \mid n \Rightarrow p \in S \right\}$

où $P = \{$éléments premiers de $D\}$ et $S \subseteq P$.