16 décembre 2015
L3
Mathématiques

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?