UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Contrôle continu (7 avril)

Documents, notes de cours ou de TD, téléphones portables, calculatrices sont interdits. Justifiez toutes vos réponses. Il est bon de relire sa copie...

Durée : 2 heures

Le barème est donné à titre indicatif.

Exercice 1 (QUESTIONS DE COURS, 8 points)

1. Décrire sans démonstration les sous-groupes de $(\mathbf{Z},+)$.
2. Soit n entier naturel. Donner la définition de $\mathbf{Z}/n\mathbf{Z}$.
3. Comment est définie dans $\mathbf{Z}/n\mathbf{Z}$ la somme de deux classes d'équivalence c et c' ?
4. L'application
$$\begin{array}{ccc} \mathbf{Z}/12\mathbf{Z} & \to & \mathbf{Z}/8\mathbf{Z} \\ [a]_{12} & \mapsto & [a]_8 \end{array}$$
est-elle bien définie ?
5. Soit $(A,+,\cdot)$ un anneau commutatif. Donner la définition d'un idéal de A.
6. Soit $(A,+,\cdot)$ un anneau commutatif intègre. Montrer que la relation binaire $\mathcal{R}$ définie sur $A\times A-\{(0,0)\}$ par
$$(p,q)\mathcal{R}(p',q') \iff pq'=p'q$$
est transitive.
7. Soit $(G,\star)$ un groupe et a un élément de G d'ordre ν. Démontrer que $\{m\in\mathbf{Z}, a^m=e_G\}$ est l'ensemble $\nu\mathbf{Z}$ des multiples de ν (on pourra raisonner par double inclusion).
8. Soit $(G,\star)$ un groupe et a un élément d'ordre ν. Donner sans démonstration l'ordre de a^3.

Exercice 2 (4 points)

1. Donner la définition de la fonction φ d'Euler.
2. Quel est le nombre d'éléments inversibles dans $\mathbf{Z}/9\mathbf{Z}$?
3. Établir la liste des éléments du groupe $\big((\mathbf{Z}/9\mathbf{Z})^\star,\times\big)$.
4. Établir sa table de multiplication.
5. À l'aide d'un théorème du cours à énoncer, déterminer les ordres possibles des éléments du groupe $\big((\mathbf{Z}/9\mathbf{Z})^\star,\times\big)$.
6. Ce groupe est-il cyclique ?

Exercice 3 (2 points)

1. Énoncer le théorème chinois.
2. Le groupe $(\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}, +)$ est-il cyclique ?
3. Si oui, en déterminer un générateur.

Exercice 4 (2 points)

Soient $P = 2X^2 - 5X + 3$ et $Q = 2X^3 + X^2 - 10X + 6$ deux polynômes de $\mathbf{R}[X]$. Calculer leur pgcd D, et déterminer des polynômes $U, V \in \mathbf{R}[X]$ tels que $UP + VQ = D$.

Exercice 5 (4 points)

Pour tout $n \in \mathbf{N}^*$, notons C_n l'ensemble des racines n-ièmes de l'unité dans $\mathbf{C}$,

$$C_n = \{z \in \mathbf{C}, z^n = 1\} = \left\{e^{\frac{2ik\pi}{n}},\ 0 \leqslant k \leqslant n-1\right\}.$$

1. Montrer que pour tout $n \in \mathbf{N}^*$, C_n est un sous-groupe de $(\mathbf{C}^*, \cdot)$.
2. Soit $n \in \mathbf{N}^*$. Donner un générateur de C_n. Montrer que $\mathbf{C}_n$ est un groupe cyclique, et expliciter un isomorphisme de groupes entre $\mathbf{Z}/n\mathbf{Z}$ et C_n.
3. Soient $n, d \in \mathbf{N}^*$, montrer que

$$C_d \subset C_n \text{ si et seulement si } d|n.$$

4. Soit H un sous-groupe fini de $(\mathbf{C}^*, \cdot)$. Notons n son cardinal.
   (a) Montrer que $H \subset C_n$.
   (b) En déduire que $H = C_n$.
5. Soient $n, m \in \mathbf{N}^*$, et soit $q = \mathrm{ppcm}(n, m)$.
   (a) Notons $\left\langle e^{\frac{2i\pi}{n}}, e^{\frac{2i\pi}{m}} \right\rangle$ le sous-groupe de $\mathbf{C}^*$ engendré par $e^{\frac{2i\pi}{n}}$ et $e^{\frac{2i\pi}{m}}$. À l'aide des questions précédentes, montrer que

$$C_q \subset \left\langle e^{\frac{2i\pi}{n}}, e^{\frac{2i\pi}{m}} \right\rangle.$$

   (b) En déduire que $\left\langle e^{\frac{2i\pi}{n}}, e^{\frac{2i\pi}{m}} \right\rangle = C_q$.