UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Contrôle continu// Corrigé

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 (4 points)

1 Soit G un groupe, e son élément neutre et a un élément de G et m un entier naturel tel $a^m = e$. Que peut-on dire de l'ordre de l'élément a ?

Solution : On peut affirmer que l'ordre de a est un diviseur de m.

2 Donner la définition d'un idéal dans un anneau commutatif.

3 Quels sont les idéaux de l'anneau $(\mathbf{Z}, +, \times)$?

4 Le sous-ensemble $28\mathbf{Z} \cap 18\mathbf{Z}$ de $\mathbf{Z}$ est-il un idéal de $\mathbf{Z}$? Si oui, le déterminer.

Solution : Il s'agit de l'idéal $pgcd(18, 28)\mathbf{Z} = 252\mathbf{Z}$

5 Donner l'exemple de deux groupes finis de même ordre non isomorphes. Justifier le fait que les deux groupes choisis ne sont pas isomorphes.

Solution : $\mathbf{Z}/4\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ sont deux groupes d'ordre 4, mais le second dont tous les éléments sont d'ordre 1 ou 2 n'est pas cyclique.

6 Le groupe $\mathfrak{S}_4$ des permutations de $\{1, 2, 3, 4\}$ est-il cyclique ? (justifier)

Solution : Comme $(1, 2)(1, 3)(1, 2) = (2, 3)$, $(1, 2)$ et $(1, 3)$ ne commutent pas. Par conséquent, le groupe $\mathfrak{S}_4$ n'est pas cyclique.

Exercice 2 (3 points)

1 L'entier -1601 est-il un représentant de la classe $[-7387]_{2893}$ de $\mathbf{Z}/2893\mathbf{Z}$?

Solution : $(-7387) - (-1601) = -5786 = (-2)2893$ donc, l'entier -1601 est un représentant de la classe $[-7387]_{2893}$ de $\mathbf{Z}/2893\mathbf{Z}$.

2 Calculer l'élément 11^{329} dans $\mathbf{Z}/13\mathbf{Z}$. Le résultat doit être représenté par un nombre compris entre 0 et 12.

Solution : Par le petit théorème de Fermat, $11^{12} = 1[13]$. On effectue la division euclidienne de 329 par 12. $329 - 27 \times 12 = 5$. Par conséquent, $11^{329} = 11^5[13]$. $11^2 = 121 = 4[13]$, $11^4 = 4^2 = 3[13]$, d'où $11^{329} = 11^5 = 33 = 7[13]$

3 La classe [51] est-elle inversible dans l'anneau $\mathbf{Z}/131\mathbf{Z}$. Si oui, calculer son inverse dans $\mathbf{Z}/131\mathbf{Z}$. Le résultat doit être représenté par un nombre compris entre 0 et 130.

Solution : Puisque $\text{pgcd}(51, 131) = 1$, la classe [51] est inversible dans $\mathbf{Z}/131\mathbf{Z}$. En utilisant l'algorithme d'Euclide on trouve que $1 = 131 \times (-7) + 51 \times 18$. Alors, dans $\mathbf{Z}/131\mathbf{Z}$ on a $51^{-1} = 18$.

Exercice 3 (2 points)

1 Ecrire une relation de Bezout entre $X^2 + X + 1$ et $X^3 + X + 1$ dans $\mathbf{R}[X]$.

Solution : $X^3 + X + 1 = (X^2 + X + 1)(X - 1) + (X + 2)$ et $X^2 + X + 1 = (X + 2)(X - 1) + 3$. Une relation de Bezout entre $X^2 + X + 1$ et $X^3 + X + 1$ dans $\mathbf{R}[X]$ est

$$3 = (X^2 + X + 1) - (X + 2)(X - 1) = (X^2 + X + 1) - (X - 1)[(X^3 + X + 1) - (X^2 + X + 1)(X - 1)]$$

soit

$$3 = (-X + 1)(X^3 + X + 1) + (X^2 - 2X + 2)(X^2 + X + 1).$$

2 La classe du polynôme $X^2 + X + 1$ est-elle inversible dans l'anneau quotient $\mathbf{R}[X]/(X^3 + X + 1)$? Si oui, donner son inverse.

Solution : Puisque $X^3 + X + 1$ et $X^2 + X + 1$ sont premiers entre eux, la classe du polynôme $X^2 + X + 1$ inversible dans l'anneau quotient $\mathbf{R}[X]/(X^3 + X + 1)$. Son inverse est la classe de $(X^2 - 2X + 2)/3$, comme le donne la relation de Bezout.

Exercice 4 (4 points)

1 Quels sont les éléments inversibles de l'anneau $(\mathbf{Z}/12\mathbf{Z})$?
2 À quel groupe le groupe $(\mathbf{Z}/12\mathbf{Z})^\times$ des inversibles de l'anneau $(\mathbf{Z}/12\mathbf{Z})$ est-il isomorphe ?

Solution : Comme $\phi(12) = \phi(3)\phi(2^2) = 2 \times 2 = 4$ il y a quatre éléments inversibles dans l'anneau $(\mathbf{Z}/12\mathbf{Z})$. Il s'agit de $1, -1 = 11, 5, -5 = 7$. Comme $5^5 = 25 = 1[12]$, tous les éléments sont d'ordre 1 ou 2. Le groupe $(\mathbf{Z}/12\mathbf{Z})^\times$ est donc isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. On peut aussi remarquer que par le théorème chinois, $(\mathbf{Z}/12\mathbf{Z})^\times = (\mathbf{Z}/4\mathbf{Z})^\times \times (\mathbf{Z}/3\mathbf{Z})^\times = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Exercice 5 (4 points)

Voici la table d'un groupe G. Quel est l'ordre de G ? Le groupe G est-il nécessairement

commutatif ? Compléter la table en énonçant précisément les propriétés utilisées.

$*$	a	b	c	d	e
a			d		c
b	e		a		d
c		a			
d				d	e
e			b		a

Solution : Comme il s'agit d'un groupe d'ordre 5, il est cyclique donc commutatif. La table se complète donc en

$*$	a	b	c	d	e
a		e	d		c
b	e		a		d
c	d	a			b
d				d	e
e	c	d	b	e	a

Comme $de = e$, d est l'élément neutre. La table se complète donc en

$*$	a	b	c	d	e
a		e	d	a	c
b	e		a	b	d
c	d	a		c	b
d	a	b	c	d	e
e	c	d	b	e	a

Par la propriété de carré latin, on peut terminer le tableau

$*$	a	b	c	d	e
a	b	e	d	a	c
b	e	c	a	b	d
c	d	a	e	c	b
d	a	b	c	d	e
e	c	d	b	e	a

Exercice 6 (3 points)

1 Calculer les produits dans $\mathfrak{S}_7$, $(1,2)(1,3)$ et $(1,2)(2,3)(1,2)$.

Solution : Dans $\mathfrak{S}_7$, $(1,2)(1,3) = (132)$ et par conjugaison $(1,2)(2,3)(1,2) = (1,3)$.

2 L'ensemble des transpositions de $\mathfrak{S}_7$ est-il un sous-groupe de $\mathfrak{S}_7$?

Solution : L'ensemble des transpositions de $\mathfrak{S}_7$ ne contient pas l'identité : ce n'est donc pas un sous-groupe de $\mathfrak{S}_7$. Le premier calcul montre qu'il n'est pas non plus stable par produit.