UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Examen final (première session)
Vendredi 19 avril 2013
Durée : 2h

Le sujet comporte deux pages et huit exercices.
Documents de cours, calculatrices, téléphones portables, etc... sont INTERDITS.
Sauf mention expresse du contraire, TOUTES les réponses et TOUS les calculs doivent être soigneusement JUSTIFIÉS.
Il sera tenu compte du soin apporté à la rédaction et à l'argumentation dans la notation. Le sujet est long, attachez vous à bien rédiger et argumenter ce que vous faites plutôt que de chercher à tout aborder.
RELISEZ VOS COPIES !

Exercice 1

(tiré de la liste d'exercices « Connaissances mathématiques élémentaires pour le L2 ») Soit f et g deux applications d'un ensemble E dans lui-même. Démontrer que si $f \circ g$ est injective alors g est injective.

Exercice 2

Pour chacune des assertion suivantes, on dira si elle est vraie ou fausse (et on justifiera bien entendu soigneusement la réponse...)

1 Soit $\mathbf{K}$ un corps et $P \in \mathbf{K}[X]$. Si P n'a pas de racine dans $\mathbf{K}$, alors P est un élément irréductible de $\mathbf{K}[X]$.

2 Soit $\mathbf{K}$, $\mathbf{L}$ des corps, avec $\mathbf{K} \subset \mathbf{L}$ et soit $P \in \mathbf{K}[X]$. Si P est un élément irréductible de $\mathbf{K}[X]$, alors P est un élément irréductible de $\mathbf{L}[X]$.

3 Soit p un nombre premier. Pour tous $x, y \in \mathbf{F}_p$, l'égalité $x^2 + y^2 = 0$ entraîne $x = y = 0$.

4 Le groupe $(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, +)$ est cyclique (on rappelle que la loi de groupe est définie par $(a, b) + (a', b') = (a + a', b + b')$).

5 Soit $n \geqslant 1$. Une racine n-ème de l'unité, vue comme élément du groupe $(\mathbf{C}^\times, \times)$, est d'ordre n.

6 L'écriture $3 + 3\,i = 1.(1 + 2\,i) + (2 + i)$ est une division euclidienne de $3 + 3i$ par $1 + 2i$, dont le quotient est 1 et le reste $2 + i$.

Exercice 3

Soit G un groupe noté multiplicativement, d'élément neutre e, soit $g \in G$, et $n \geqslant 1$ un entier.

1 Donner la démonstration, vue en cours, du résultat suivant : $g^n = e$ si et seulement si g est d'ordre fini et son ordre divise n.

2 On suppose g d'ordre n. Donner la démonstration, vue en cours, du résultat suivant : pour tout $k \in \mathbf{Z}$, g^k est d'ordre $\frac{n}{\mathrm{pgcd}(n,k)}$.

Exercice 4

1 Résoudre l'équation $x^2 - [2]_{17}.x + [2]_{17} = [0]_{17}, \quad x \in \mathbf{Z}/17\mathbf{Z}$.

2 Soit p un nombre premier. L'équation

$$x^2 - [2]_p.x + [2]_p = [0]_p, \quad x \in \mathbf{Z}/p\mathbf{Z}$$

a-t-elle des solutions ?

Exercice 5

1 Soit $n \geqslant 1$. Rappeler la définition de la signature d'un cycle de $\mathfrak{S}_n$, puis celle de la signature d'un élément $\sigma \in \mathfrak{S}_n$ quelconque en termes de sa décomposition en produit de cycles à supports disjoints.

2 Soit $n \geqslant 1$. Déterminer l'ordre d'un 3-cycle de $\mathfrak{S}_n$.

3 On rappelle que $\mathfrak{A}_4$ est le sous-groupe de $\mathfrak{S}_4$ constitué des éléments de signature 1. Donner la liste des éléments de $\mathfrak{A}_4$; pour chaque élément on donnera sa décomposition en produit de cycles à supports disjoints. *Indication :* $\mathfrak{A}_4$ possède 12 éléments.

4 Exhiber un sous-groupe de $\mathfrak{A}_4$ qui est d'ordre 4. Démontrer que $\mathfrak{A}_4$ possède un unique sous-groupe d'ordre 4, que l'on notera K. *Indication :* on pourra utiliser le théorème de Lagrange.

5 Déterminer la table d'addition du groupe $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. En déduire que K est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Exercice 6

1 Compléter l'équivalence « soit $z \in \mathbf{Z}[i]$; alors $z \in \mathbf{Z}[i]^\times$ si et seulement si ... » par une assertion portant sur $N(z)$. Donner ensuite la démonstration (vue en cours) de l'équivalence ainsi complétée.

2 $\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$ est-il un élément de $\mathbf{Z}[i]^\times$?

3 Soit $z \in \mathbf{Z}[i]$ tel que $N(z)$ est un nombre premier. Montrer que z est un élément irréductible de $\mathbf{Z}[i]$.

Exercice 7

1 Soit $n \geqslant 1$ et $c = (d_1, d_2, \ldots, d_{r-1}, d_r)$ un r-cycle de $\mathfrak{S}_n$. Soit $\tau \in \mathfrak{S}_n$. Montrer l'égalité

$$\tau.c.\tau^{-1} = (\tau(d_1), \tau(d_2), \ldots, \tau(d_{r-1}), \tau(d_r))$$

2 Soit σ l'élément de $\mathfrak{S}_7$ donné par $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 1 & 5 & 7 & 6 \end{pmatrix}$. Déterminer la décomposition de σ en produit de cycles à supports disjoints *(on ne demande pas le détail des calculs).*

3 On conserve les notations de la question précédente. Déduire des questions précédentes une description de l'ensemble des éléments $\tau \in \mathfrak{S}_7$ qui vérifient $\tau\sigma = \sigma\tau$.

Exercice 8

Soit $(A, +, \times)$ et $(B, +, \times)$ des anneaux commutatifs. Soit $\varphi : A \to B$ un morphisme d'anneaux. Montrer que le noyau de φ est un idéal de A. Compléter l'assertion suivante : « $\varphi(A)$ est un ... de B ». Démontrer ensuite l'assertion ainsi complétée.