Université de Paris Diderot **Second semestre**
A3 – Arithmétique **Mercredi, 14 janvier 2015**

Examen

L'épreuve dure trois heures. Les documents ne sont pas autorisés. Les questions sont presque indépendantes, mais il est toutefois recommandé de les traiter dans l'ordre. Barème : un point par question ; les questions étoilées valent, en revanche, le double. Enfin, il sera tenu compte de la qualité de la rédaction.

1. Déterminer les sous-groupes du groupe additif $(\mathbb{Z}, +)$. En donner la preuve.
   Pour quelles valeurs de l'entier $n \in \mathbb{Z}$ le quotient $\mathbb{Z}/n\mathbb{Z}$ est-il fini ? Justifier.
2. Soit $\mathcal{B}$ la bande $\{M = (x, y) \in \mathbb{R}^2,\ -1 \leq x - y \leq 1\}$. Montrer que la relation d'équivalence $M\,\mathcal{R}\,N \ \Leftrightarrow\ M + \mathcal{B} = N + \mathcal{B}$ est compatible avec la loi du groupe additif $(\mathbb{R}^2, +)$. Quel est le sous-groupe dont elle relève ?
3. Montrer que le groupe alterné $\mathfrak{A}_4$ ne possède pas de sous-groupe d'ordre 6. Dessiner ensuite le treillis de ses sous-groupes.
4. Déterminer les carrés des éléments d'ordre 4 dans $\mathfrak{S}_4$. En déduire que les automorphismes de $\mathfrak{S}_4$ appliquent une double-transposition sur une double-transposition.
5. Montrer que $\sigma \circ (i\,j) \circ \sigma^{-1} = (\sigma(i)\,\sigma(j))$. En déduire le centre de $\mathfrak{S}_n$ pour $n \geq 3$.
6. Montrer qu'un automorphisme Φ de $\mathfrak{S}_4$ envoie deux éléments conjugués a et b sur deux éléments conjugués. Que fait donc un tel automorphisme sur les neuf éléments d'ordre 2 ? En déduire que le sous-groupe de Klein $\mathfrak{V}_4$ est caractéristique dans $\mathfrak{S}_4$.
7. Montrer que le seul sous-groupe d'indice 2 du groupe symétrique $\mathfrak{S}_4$ est son sous-groupe $\mathfrak{A}_4$. En déduire que le sous-groupe de Klein $\mathfrak{V}_4$ est caractéristique dans $\mathfrak{S}_4$.
8. Montrer que le sous-groupe de Klein $\mathfrak{V}_4$ est distingué dans $\mathfrak{S}_4$. Déterminer le groupe-quotient $\mathfrak{S}_4/\mathfrak{V}_4$.
9. (*) Déterminer le cardinal du sous-groupe de $\mathfrak{S}_4$ engendré par les deux permutations $(1\,2)$ et $(1\,3)(2\,4)$. On pourra remarquer que ces deux permutations commutent toutes deux avec $(12)(34)$ et ne peuvent donc engendrer $\mathfrak{S}_4$ tout entier.
10. Montrer que $\bar{k}$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ si, et seulement si, $\bar{k}$ engendre le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$. Calculer ensuite l'inverse de $\overline{13}$ dans l'anneau $(\mathbb{Z}/21\mathbb{Z}, +, \cdot)$.
11. Résoudre dans $\mathbb{Z}$ le système de congruences :
$$x \equiv 2 \mod 17 \qquad \text{et} \qquad x \equiv 2 \mod 28.$$
12. On note $n \mapsto \varphi(n)$ la fonction indicatrice d'Euler. Montrer que si $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1 \mod n$. Calculer $\varphi(1001)$. Pour quelles valeurs de n, l'entier $\varphi(n)$ est-il pair ? Justifier.
13. Dessiner le treillis du groupe multiplicatif $(U_{24}, \cdot)$ des racines vingt-quatrièmes de l'unité dans $\mathbb{C}$. Y placer les deux racines $w_7 = \mathrm{e}^{7i\pi/12}$ et $w_{10} = \mathrm{e}^{5i\pi/6}$.
14. Montrer que le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ possède un nombre impair de sous-groupes si, et seulement si, l'entier n est un carré parfait.
15. Calculer l'exposant des groupes $G_1 = (\mathbb{Z}/8\mathbb{Z}, +)$ et $G_2 = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$. On pose $G_3 = (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$. Montrer que deux quelconques parmi les trois groupes G_1, G_2 ou G_3 ne sont pas isomorphes.
16. Déterminer les quotients de $(\mathbb{Z}/15\mathbb{Z})^\times$ par chacun de ses sous-groupes d'ordre 2.

17. Montrer que les groupes additifs $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/(m \wedge n)\mathbb{Z}) \times (\mathbb{Z}/(m \vee n)\mathbb{Z})$ sont isomorphes.
18. Calculer le cardinal du groupe multiplicatif $((\mathbb{Z}/32\mathbb{Z})^\times, \cdot)$. Y déterminer les éléments d'ordre 2 ainsi que l'ordre de $\bar{5}$. Montrer que ce groupe n'est pas cyclique.
19. (*) Dessiner le treillis du groupe $((\mathbb{Z}/32\mathbb{Z})^\times, \cdot)$.
20. Calculer l'exposant du groupe multiplicatif $G = (\mathbb{Z}/100\mathbb{Z})^\times$. Quel est l'exposant du groupe $G \times G$?
21. Montrer qu'il y a autant d'éléments inversibles que de non inversibles dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ si, et seulement si, n est une puissance de 2.
22. Déterminer les homomorphismes du groupe quaternionique $\mathbb{H}_8$ [1] dans le groupe multiplicatif $(\mathbb{C}^\star, \cdot)$. On commencera par déterminer le sous-groupe dérivé de $\mathbb{H}_8$.
23. (*) Une matrice monomiale est une matrice qui possède un seul terme non nul par ligne et par colonne. Montrer que ces matrices forment un sous-groupe du groupe linéaire $GL(n, \mathbb{K})$, et dont le sous-groupe des matrices diagonales est distingué. Déterminer le nombre de telles matrices qui sont de déterminant 1 lorsque $\mathbb{K} = \mathbb{F}_5$ [2] et $n = 2$, ainsi que le groupe qu'elles forment.
24. Dessiner le treillis du groupe additif $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, +)$.
25. Combien y a-t-il d'isomorphismes entre le groupe symétrique $\mathfrak{S}_3$ et le groupe $\mathcal{D}_3$ des isométries du triangle équilatéral ?
26. Dessiner le treillis des sous-groupes du groupe diédral $\mathcal{D}_4$ des isométries du carré. En déduire le groupe-quotient de $\mathcal{D}_4$ par son centre. Justifier.
27. (*) On se donne un groupe G (commutatif ou non) d'ordre 20 possédant un élément a tel que a^{10} soit d'ordre 2. Le groupe G est-il cyclique ? Examiner cela dans le cas du groupe multiplicatif $(\mathbb{Z}/25\mathbb{Z})^\times$. Qu'ajoute de plus l'hypothèse que le groupe est commutatif ? Calculer l'ordre de $\bar{4}$ dans le groupe multiplicatif $(\mathbb{Z}/75\mathbb{Z})^\times$.

1. On rappelle que le groupe $\mathbb{H}_8$ est le seul groupe non commutatif à huit éléments qui n'a qu'un seul élément d'ordre 2 ; il a donc six éléments d'ordre 4.

2. Où $\mathbb{F}_5$ désigne le corps fini $(\mathbb{Z}/5\mathbb{Z}, +, \cdot)$ à cinq éléments.