Exercices Mathématiques Discrètes : Théorie des groupes finis

1. Parmi les structures suivantes, déterminer lesquelles sont des groupes.

   (a) $< \mathbb{Z}_2, +_2, 0 >$ (b) $< \mathbb{Z}_2, \cdot_2, 1 >$ (c) $< \{\mathbf{True}, \mathbf{False}\}, \vee, \mathbf{False} >$
   (d) $< \{\mathbf{True}, \mathbf{False}\}, \wedge, \mathbf{True} >$ (e) $< \mathbb{N}, +, 0 >$ (f) $< \{z \in \mathbb{C} \mid z^n = 1\}, \cdot, 1 >$

2. Dessiner la table d'opérations de $< \mathbb{Z}_5, +_5, 0 >$ et celle de $< \mathbb{Z}_8^*, \cdot_8, 1 >$.

3. Donner tous les sous-groupes de $< \mathbb{Z}_{14}^*, \cdot_{14}, 1 >$ et donner un générateur de chacun de ces sous-groupes.

4. Donner un générateur de $< \mathbb{Z}_3, +_3, 0 >$.

5. Donner l'ordre de chacun des éléments de $< \mathbb{Z}_5^*, \cdot_5, 1 >$.

6. Montrer, sans utiliser la fonction d'Euler, que $|\mathbb{Z}_{p^e}^*| = p^{e-1}(p-1)$ où p est premier et $e \geq 1$.

7. Soit $< G, \cdot, 1 >$ un groupe et g un élément de G. Prouver que l'inverse de g est unique.

8. Soit $< G, \cdot, 1 >$ un groupe et $g \in G$, prouver que l'ordre de g divise $|G|$.

9. Soit φ un morphisme entre deux groupes $< G_1, \cdot_1, \mathbf{1}_1 >$ et $< G_2, \cdot_2, \mathbf{1}_2 >$.
   (a) Prouver que $\varphi(\mathbf{1}_1) = \mathbf{1}_2$.
   (b) Prouver que pour tout $g \in G_1$, $\varphi(g^{-1}) = (\varphi(g))^{-1}$.
   (c) Prouver que pour tout $g \in G_1$, si l'ordre de g est n, alors l'ordre de $\varphi(g)$ divise n (et qu'il vaut n si φ est injectif).
   (d) On définit le noyau de φ, noté $\ker(\varphi)$, comme suit :

   $$\ker(\varphi) \;=\; \{g_1 \in G_1 \mid \varphi(g_1) = \mathbf{1}_2\}.$$

   Prouver que $\ker(\varphi)$ est un sous-groupe normal de G_1.
   (e) On définit l'image de φ, notée $\mathrm{Im}(\varphi)$, comme suit :

   $$\mathrm{Im}(\varphi) \;=\; \{g_2 \in G_2 \mid \exists g_1 \in G_1 \; g_2 = \varphi(g_1)\}.$$

   Prouver que $\mathrm{Im}(\varphi)$ est un sous-groupe de G_2.

10. Soit $< G, \cdot, 1 >$ un groupe et H un sous-groupe de G.
    Montrer que la relation R sur G définie par

    $$R = \{(a, b) \in G^2 \mid \exists g \in G, a \in gH \wedge b \in gH\}$$

    est une relation d'équivalence.

11. Soit S_n l'ensemble des permutations de $E_n = \{1, \ldots, n\}$ (i.e l'ensemble des bijections de E_n dans lui-même). Prouver que S_n, muni de la loi de composition de fonctions, est un groupe. *(Vous ne devez pas prouver que la composition de fonctions est une opération associative)*

12. Soit G un ensemble de matrices carrées à coefficients entiers défini par :

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \mid a \in \mathbb{Z} \right\}$$

    (a) Prouver que $\langle G, \cdot, \mathbf{1} \rangle$ est un groupe, où $\cdot$ représente la multiplication matricielle et $\mathbf{1}$ la matrice identité.

    (b) Ce groupe est-il commutatif ? Justifier votre réponse.

    (c) On considère la fonction $\varphi : G \to \mathbb{Z}$ définie par :

$$\varphi\left(\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \right) = a.$$

    Prouver que φ est un isomorphisme entre les groupes $\langle G, \cdot, \mathbf{1} \rangle$ et $\langle \mathbb{Z}, +, 0 \rangle$.

13. On considère le groupe $(S_3, \circ, \mathbf{1})$. Donner un exemple de sous-groupe normal de S_3 (justifier votre réponse). Donner un exemple de sous-groupe de S_3 qui n'est pas normal (justifier votre réponse).

14. On considère le groupe $\langle \mathbb{Z}, +, 0 \rangle$, prouver que $3\mathbb{Z}$ est un sous-groupe normal de $\mathbb{Z}$. Décrire la partition de $\mathbb{Z}$ induite par $3\mathbb{Z}$. Trouver un groupe connu isomorphe au quotient de $\mathbb{Z}$ par $3\mathbb{Z}$.

15. On considère les groupes $\langle \mathbb{Z}, +, 0 \rangle$, $\langle \mathbb{Z}_2, +_2, 0 \rangle$ et la fonction $\varphi : \mathbb{Z} \to \mathbb{Z}_2$ définie par $\varphi(z) = z \mod 2$. Prouver que φ est un morphisme. Calculer $\ker(\varphi)$ et $\mathrm{Im}(\varphi)$. Comparer le groupe obtenu en quotientant $\mathbb{Z}$ par $\ker(\varphi)$ (vous savez que ce sous-groupe est normal) avec le groupe $\langle \mathbb{Z}_2, +_2, 0 \rangle$.

16. Soit S_3 l'ensemble des permutations de $\{1, 2, 3\}$ et R la relation binaire sur S_3 définie par :

$$R = \{(p_1, p_2) \in S_3 \times S_3 \mid p_1(1) = p_2(1)\}.$$

    (a) Prouver que R est une relation d'équivalence.

    (b) Décrire la partition de S_3 induite par les classes d'équivalence de R.

    (c) Déterminer si l'une des classes d'équivalence de R est un sous-groupe de S_3.

    (Examen juin 2008)

17. Soit G le sous-ensemble de matrices suivant :

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R} \right\}$$

    (a) Prouver que G muni de la multiplication matricielle est un groupe.

(b) Le groupe G (muni de la multiplication matricielle) est-il commutatif ?

(c) Trouver un isomorphisme entre G muni de la multiplication matricielle et le groupe $\langle \mathbb{R}, +, 0 \rangle$.

(Examen juin 2009)

18. Prouver que si G est un groupe qui possède exactement 2 éléments, alors G a un élément d'ordre 2. *(Examen juin 2009)*

19. Décider si les affirmations suivantes sont vraies ou fausses. Justifier. *(Examen juin 2009)*

    (a) Le groupe $\mathbb{Z}_2 \times \mathbb{Z}_3$ muni de l'addition définie composante par composante[1] est isomorphe à S_3, le groupe des permutations à trois éléments.

    (b) Pour tout $n \geq 2$, si G est un groupe à n éléments, alors G a un élément d'ordre n.

20. L'ensemble $G_1 = \{p \in S_5 \mid p(4) = 5 \text{ et } p(5) = 4\}$ est-il un sous-groupe de S_5 ? *(Examen août 2009)*

21. Soit $p \in S_3$, on note $\bar{p}$ la fonction définie par $\bar{p} = (12)p(12)$.

    (a) Prouver que $\bar{p} \in S_3$ quel que soit $p \in S_3$.

    (b) Prouver que $G_2 = \{\bar{p} \mid p \in S_3\}$ est un sous-groupe de S_3.

    (c) Prouver que $\sigma : S_3 \to G_2$ est un isomorphisme de groupes.

    (d) Déterminer combien d'éléments se trouvent dans le quotient de S_3 par G_2.

    (Examen août 2009)

[1] i.e. $(a, b) + (c, d) = (a +_2 c, b +_3 d)$