Soutien d'Algèbre I - Exercices

Allan Merino

Exercice 0.1. 1. Soit $(G, .)$ un groupe et $a \in G$. On définit sur G une nouvelle loi interne $\star$ en posant :

$$x \star y = x.a.y \quad (x, y \in G).$$

Montrer que $(G, \star)$ est un groupe.

2. En déduire que $(\mathbb{R}, \star)$ est un groupe, où $\star$ est la loi interne définie sur $\mathbb{R}$ par :

$$x \star y := x + y - 3 \quad (x, y \in \mathbb{R}).$$

Exercice 0.2. Soit $(G, .)$ un groupe fini d'ordre impair.

1. Montrer que l'application $f : G \to G$, définie par $f(x) = x^2$, $x \in G$, est bijective.
2. Résoudre dans G l'équation $x^2 = e$.

Exercice 0.3. On considère l'ensemble des entiers relatifs $\mathbb{Z}$ comme le groupe additif $(\mathbb{Z}, +)$.

1. Montrer que tout groupe monogène est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}$.
2. Déterminer les générateurs de $\mathbb{Z}$ et de $\mathbb{Z}/n\mathbb{Z}$ pour un n fixé.
3. Montrer que pour tous entiers $n > 1$ et $m > 1$, le produit cartésien des groupes quotients $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$ est isomorphe au groupe quotient $\mathbb{Z}/mn\mathbb{Z}$ si et seulement si n et m sont premiers entre eux.

Exercice 0.4. Montrer qu'une application $f : (\mathbb{Q}, +) \to (\mathbb{Q}, +)$ est un morphisme de groupes si et seulement si il existe $a \in \mathbb{Q}$ tel que $f(x) = ax$ pour tout $x \in \mathbb{Q}$.

Exercice 0.5. Soit $(G, .)$ un groupe et soit H une partie non vide de G.

1. Si H est fini et stable par le produit de G, montrer que H est un sous-groupe de G.
2. Si H n'est pas fini mais H stable par le produit de G, a-t-on que H est un sous-groupe ?

Exercice 0.6. Pour tout entier $n \geqslant 1$, on note $GL(n, \mathbb{R})$ le groupe des matrices carrées réelles d'ordre n qui sont inversibles. On note $SL(n, \mathbb{R})$ le sous-ensemble de $GL(n, \mathbb{R})$ des matrices de déterminant 1.

1. Montrer que $SL(n, \mathbb{R})$ est un sous-groupe distingué de $GL(n, \mathbb{R})$.
2. Montrer que le quotient $GL(n, \mathbb{R})/SL(n, \mathbb{R})$ est isomorphe au groupe multiplicatif $\mathbb{R}^*$.

Exercice 0.7. Montrer que les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont isomorphes.

Exercice 0.8. Soit $T = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} a, c \in \mathbb{R}^*, b \in \mathbb{R}\}$ et $U = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} b \in \mathbb{R}\}$.

1. Montrer que T est un sous-groupe de $GL(2, \mathbb{R})$.
2. Montrer que U est un sous-groupe distingué de T.

Exercice 0.9. Soit G un groupe. On définit le centre de G par $Z(G) = \{g \in G/gh = hg\,(\forall h \in G)\}$.

1. Montrer que $Z(G)$ est un sous-groupe distingué de G.
2. Montrer que si $G/Z(G)$ est monogène, alors G est abélien.
3. Soit p un nombre premier. En admettant que le centre de G est non trivial, montrer que tout groupe d'ordre p^2 est abélien.

Exercice 0.10. Soit H un sous-groupe d'un groupe G d'élément neutre e. On définit la relation $\mathscr{R}$ suivante sur G :

$$y\mathscr{R}x \Leftrightarrow x^{-1}y \in H \quad (\forall x, y \in G).$$

1. Vérifier que $\mathscr{R}$ est une relation d'équivalence sur G.
2. Décrire les classes d'équivalence de $\mathbb{R}$. On notera $\bar{x}$ la classe de $x \in G$.
3. On note G/H l'ensemble des classes d'équivalence de $\mathscr{R}$ dans G. On suppose que H est distingué dans G. Vérifier que si l'on pose, pour $x, y \in G$, $\overline{xy} = \bar{x}\bar{y}$, on obtient une structure de groupe sur G/H.

Définition 0.11. Soit p un nombre premier. On appelle p-groupe tout groupe dont l'ordre est une puissance de p.

Proposition 0.12. *Le centre d'un p-groupe est non trivial (c'est-à-dire non réduit à l'élément neutre).*

Exercice 0.13 (Les groupes d'ordre p^2)**.** Considérons G un groupe d'ordre p^2 avec p premier.

1. Déterminer l'ordre possible des éléments de G.

   Considérons à présent que G n'est pas cyclique.
2. Déterminer alors l'ordre de tous les éléments de G.
3. Soit $a \neq e \in Z(G)$. Montrer qu'il existe b tel que b n'appartient pas au sous-groupe engendré par a.
4. Notons $< a >$ et $< b >$ les sous-groupes engendrés par a et b respectivement. Montrer que l'application :

   $$\psi :< a > \times < b >\to G, \quad (a^n, b^m) \to a^n b^m$$

   est un morphisme de groupe injectif.
5. A isomorphisme près, combien existe-t-il de groupes d'ordre p^2 ?

Exercice 0.14 (Petit théorème de Fermat)**.** Soit p un nombre premier. On se place dans le conoïde $(\mathbb{Z}/p\mathbb{Z}, \times)$.

1. Montrer que tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles pour la multiplication.
2. Montrer que pour tout $a \in \mathbb{Z}$, le nombre p divise $a^p - a$.

Exercice 0.15. Montrer que l'image réciproque d'un sous-groupe distingué par un morphisme est un sous-groupe distingué. Que dire de l'image directe d'un sous-groupe distingué ?

Exercice 0.16. On dit qu'un groupe G est simple si il ne possède pas de sous-groupes distingué trivial. Considérons un groupe simple G. Soit H un groupe quelconque. Montrer que tout morphisme $f : G \to H$ est soit constante, soit injectif.

Exercice 0.17. Montrer que les seuls idéaux de $M(n, \mathbb{R})$ sont $\{0\}$ et $M(n, \mathbb{R})$.

Exercice 0.18. Soit $P(X) = \sum_{i=0}^{n} a_i X^i$ un polynôme de $\mathbb{Z}[X]$.

1. Montrer que si $r = \frac{p}{q} \in \mathbb{Q}$ (avec p et q premiers entre eux) est une racine de P, alors p divise a_0 et q divise a_n.
2. Montrer que toute racine rationnelle d'un polynôme unitaire de $\mathbb{Z}[X]$ est entière.