Structures algébriques I

1 Groupes – Généralités

EXERCICE 1. ◐○○ *Des lois curieuses*

1. On considère sur $\mathbb{Z}$ la loi $\star$, donnée par $x \star y = x + y - xy$. Étudier ses propriétés : associativité, commutativité, élément neutre, éléments inversibles. Si $x \in \mathbb{Z}$ et $n \in \mathbb{N}$, donner une formule explicite pour la puissance n-ème $x^{\star n}$.

2. On considère sur $\mathbb{R}$ la loi $\star$, donnée par $x \star y = |x - y|$. Associativité, commutativité ?

3. On considère E l'ensemble à trois éléments $E = \{\text{Pierre}, \text{Feuille}, \text{Ciseaux}\}$. En vous inspirant des règles du Chifoumi, définir sur E une LCI commutative mais non associative.

EXERCICE 2. ●◐○ *Élément neutre et inverse à droite*
Soit G un ensemble, muni d'une loi de composition interne associative $\star$. On suppose que G admet un élément neutre à droite e et que tout élément $x \in G$ admet un inverse à droite.
Montrer que G est un groupe.

EXERCICE 3. ♣/♢ – ●◐○ *Tout élément est régulier*
Soit G un ensemble fini non vide, muni d'une loi de composition interne associative $\star$. On suppose que tous les éléments de G sont réguliers. On fixe $a \in G$.

1. Montrer qu'il existe $e \in G$ tel que $a \star e = a$.
   Montrer que e est élément neutre de $\star$, puis que $(G, \star)$ est un groupe.

2. Qu'en est-il si G est infini ?

EXERCICE 4. ◐○○ *Élément égal à son inverse*
Soit G un groupe fini de cardinal pair. Montrer qu'il existe $x \neq e$ dans G tel que $x = x^{-1}$.

EXERCICE 5. ◐○○ *Conditions pour être abélien*
Soit G un groupe.

1. On suppose que tout $x \in G$ vérifie $x^2 = e$. Montrer que G est abélien.

2. On suppose que pour tous $x, y \in G$, $(xy)^2 = x^2 y^2$. Montrer que G est abélien.

3. Montrer que G est abélien ssi $x \mapsto x^{-1}$ est un automorphisme de G.

EXERCICE 6. ♣ – ●◐○ *Produit interne*
Soit G un groupe, soient H et K deux sous-groupes de G.

1. Montrer que HK est un sous-groupe de G ssi $HK = KH$.
2. Soient $h, h' \in H$ et $k, k' \in K$.
   Montrer que $hk = h'k'$ ssi il existe $x \in H \cap K$ tel que $h' = hx^{-1}$ et $k' = xk$.
3. On suppose H et K finis. Montrer que $|HK| = \dfrac{|H| \times |K|}{|H \cap K|}$.

EXERCICE 7. ♣ – ●●○ *Produit de groupes cycliques*
Soit G et H deux groupes cycliques de cardinal n et m.
Montrer que $G \times H$ est un groupe cyclique ssi $n \wedge m = 1$.

EXERCICE 8. ♣/♢ – ●●◐ *Défaut de commutativité dans un groupe non abélien*
Soit G un groupe fini non abélien.
On note $Z = \{x \in G \mid \forall y \in G, xy = yx\}$ le centre de G et $C = \{x, y \in G^2 \mid xy = yx\}$. Montrer que

$$|Z| \leq \frac{1}{4}|G| \text{ et } |C| \leq \frac{5}{8}|G|^2.$$

EXERCICE 9. ●○○ *Union de deux sous-groupes*
Soient G un groupe, H et K deux sous-groupes de G.
Montrer que $H \cup K$ est un groupe ssi $H \subset K$ ou $K \subset H$.

EXERCICE 10. ●○○ *Sous-groupe et image d'un groupe cyclique*
Soit G un groupe cyclique.

1. Montrer que si $f : G \to G'$ est un morphisme de groupes, alors $f(G)$ est un sous-groupe cyclique de G'.
2. Montrer que si H est un sous-groupe de G, alors H est cyclique.

EXERCICE 11. ♣/♢ – ●◐○ *Sous-groupes finis de* $(\mathbb{C}^*, \times)$
Classifier les sous-groupes finis de $(\mathbb{C}^*, \times)$.

EXERCICE 12. ●●○ *Sous-groupe de Frattini*
Soit G un groupe. Un élément $x \in G$ est mou si pour toute partie X engendrant G, $X - \{x\}$ engendre G. On note $\Phi(G)$ l'ensemble des éléments mous de G.

1. Montrer que $\Phi(G)$ est un sous-groupe de G.
2. Déterminer $\Phi(\mathbb{Z})$, puis $\Phi(\mathbb{Q})$.

EXERCICE 13. ●●○ *Sous-groupes caractéristiques*
Soit G un groupe. Un sous-groupe H est caractéristique si pour tout automorphisme ϕ de G, $\phi(H) = H$.

1. Montrer qu'un sous-groupe caractéristique H est distingué : $\forall x \in G, xH = Hx$.
2. Montrer que le centre $Z(G)$ de G est caractéristique.
3. Montrer que le sous-groupe de Frattini $\Phi(G)$ de G est caractéristique.

EXERCICE 14. ♣ – ●●○ *Groupe quotient*
Soit G un groupe, H un sous-groupe de G. On considère sur G la relation $\mathscr{R}$ définie par

$$\forall x, y \in G, x \mathscr{R} y \iff xy^{-1} \in H.$$

On dit que H est distingué dans G ssi $\forall g \in G, xH = Hx$.

1. Montrer que $\mathscr{R}$ est une relation d'équivalence. Expliciter la classe d'un élément $x \in G$.

2. On note G/H le quotient $G/\mathscr{R}$. Montrer l'équivalence entre les assertions suivantes :

   i) Il existe une structure de groupe sur $G/\mathscr{R}$, telle que $\pi : G \to G/H, g \mapsto \mathrm{cl}_{\mathscr{R}}(g)$ soit un morphisme de groupes ;

   ii) H est distingué dans G.

3. Soit $f : G \to G'$ un morphisme de groupes surjectif.
   Montrer qu'on a un isomorphisme $\bar{f} : G/\operatorname{Ker}(f) \to G'$.

4. On suppose G abélien. Montrer que tout sous-groupe H est distingué dans G.

5. Soit G un groupe cyclique de cardinal n et H un sous-groupe de G, de cardinal d.
   A quel groupe est isomorphe G/H ?

EXERCICE 15. ●●● *Sous-groupes de* $\mathbb{Z}^2$
Soit H un sous-groupe de $(\mathbb{Z}^2, +)$.
Montrer qu'il existe $u, v \in \mathbb{Z}^2$ tel que $H = \mathbb{Z}u + \mathbb{Z}v = \left\{au + bv, (a, b) \in \mathbb{Z}^2\right\}$.

2 Morphismes de groupes

EXERCICE 16. ○○○ *Morphismes de groupes*

1. Montrer que $f : (\mathbb{R}^*, \times) \to (\mathbb{R}^*, \times), x \mapsto \dfrac{x}{|x|}$ est un morphisme de groupes.

   Déterminer son noyau et son image.

2. Même question avec $g : (\mathbb{C}^*, \times) \to (\mathbb{C}^*, \times), z \mapsto \dfrac{z}{|z|}$.

3. Même question avec $\theta_n : (\mathbb{Z}, +) \to (\mathbb{C}^*, \times), k \mapsto e^{2ik\pi/n}$ (où $n \in \mathbb{N}^*$).

EXERCICE 17. ●○○ *Automorphismes intérieurs*
Soit G un groupe, soit $g \in G$. On note $\phi_g : G \to G, x \mapsto gxg^{-1}$.

1. Montrer que, pour tout $g \in G$, ϕ_g est un automorphisme de G. Que vaut ϕ_g si G est abélien ?

2. Montrer que $\operatorname{Aut}(G)$, ensemble des automorphismes de G, est un sous-groupe du groupe des permutations de G.

3. Montrer que $\Phi : G \to \operatorname{Aut}(G), g \mapsto \phi_g$ est un morphisme de groupes. Quand est-il injectif ?

Exercice 18. ●○○ *Transport de structure*

1. Soient $(G,\star)$ un groupe, E un ensemble et $f : E \to G$ une bijection. Montrer que la loi $*$ définie sur E par $\forall x,y \in E, x*y = f^{-1}\big(f(x)\star f(y)\big)$ munit E d'une structure de groupe et que $(E,*)$ est isomorphe à $(G,\star)$.

2. En déduire que tout ensemble fini non vide peut être muni d'une structure de groupe.

3. On définit la loi $\star$ sur $]-1,1[$ par $\forall x,y \in]-1,1[, x\star y = \dfrac{x+y}{1+xy}$. Montrer, en limitant les calculs, que $\big(]-1,1[,\star\big)$ est un groupe, isomorphe à $(\mathbb{R},+)$.

Exercice 19. ♣ – ●◐○ *Morphismes de groupes, avec $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{Z}/n\mathbb{Z}$*

Soient $n, m \geq 1$. Déterminer les morphismes de groupes :

1. de $(\mathbb{Z},+)$ dans $(\mathbb{Z},+)$
2. de $(\mathbb{Z},+)$ dans $(\mathbb{Q},+)$
3. de $(\mathbb{Q},+)$ dans $(\mathbb{Q},+)$
4. de $(\mathbb{Q},+)$ dans $(\mathbb{Z},+)$
5. de $(\mathbb{Z}/n\mathbb{Z},+)$ dans $(\mathbb{Z}/m\mathbb{Z},+)$

Exercice 20. ●◐○ *Théorème de Cayley*

1. Soient G un groupe, $g \in G$. Montrer que l'application $\tau_g : G \to G, x \mapsto gx$ est une permutation de G.

2. On note $(S_G,\circ)$ le groupe des permutations de G.
   Montrer que $T : G \to G, g \mapsto \tau_g$ est un morphisme de groupes injectif.

Exercice 21. ♣ – ●●○ *Groupes non isomorphes*

Montrer que les groupes suivants ne sont pas isomorphes :

1. $(\mathbb{Z},+)$ et $(\mathbb{Q},+)$
2. $(\mathbb{Q},+)$ et $(\mathbb{Q}_+^*,\times)$
3. $(\mathbb{Q},+)$ et $(\mathbb{R},+)$
4. $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$.

Exercice 22. ♣ – ●●◐ *Nombre d'automorphismes d'un groupe fini*

Soit G un groupe fini de cardinal n.

1. Montrer que G est engendrée par une partie de cardinal $r \leq \lfloor \log_2(n) \rfloor$.

2. En déduire que G possède au plus $n^{\lceil \log_2(n) \rceil}$ automorphismes.

3 Anneaux et corps

Exercice 23. ○○○ *Anneaux et sous-anneaux*
Dans les exemples suivants, A est un anneau, B est une partie de A. B est-il un sous-anneau de A ?

1. $A = \mathbb{Z}$ et $B = \mathbb{N}$;
2. $A = \mathbb{R}$ et $B = \left\{\frac{k}{10^n}, (k, n) \in \mathbb{Z} \times \mathbb{N}\right\}$ est l'ensemble des nombres décimaux ;
3. $A = \mathbb{R}^{\mathbb{N}}$ et B est l'ensemble des suites tendant vers 1 ;
4. $A = \mathbb{R}^{\mathbb{N}}$ et B est l'ensemble des suites tendant vers 0 ;
5. $A = \mathbb{R}^{\mathbb{N}}$ et B est l'ensemble des suites convergentes ;
6. $A = \mathbb{R}^{\mathbb{R}}$ et B est l'ensemble des fonctions paires.

Exercice 24. ◐○○ *Anneau fini intègre*
Montrer qu'un anneau fini est intègre ssi c'est un corps.

Exercice 25. ●○○ *Racines carrées et intégrité*

1. Montrer que, dans un anneau intègre A, on a pour tout $a \in A$ au plus deux solutions à l'équation $x^2 = a$.
2. Donner un exemple d'anneau non intègre A et d'élément $a \in A$ tel que l'équation $x^2 = a$ admette strictement plus de deux solutions.

Exercice 26. ♣ – ●◐○ *Nilpotents dans un anneau*
Un élément a d'un anneau A est nilpotent s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$.

1. Quels sont les éléments nilpotents d'un anneau intègre ?
2. On suppose que $a, b \in A$ sont nilpotents et commutent. Montrer que ab et $a+b$ sont nilpotents.
3. On suppose que a est nilpotent. Montrer que $1 - a$ est inversible.
4. Donner un exemple d'anneau non intègre sans autre élément nilpotent que 0.

Exercice 27. ●◐○ *L'anneau* $\mathbb{Z}[j]$
On note $\mathbb{Z}[j] = \{a + bj, (a, b) \in \mathbb{Z}^2\}$.

1. Montrer que c'est un sous-anneau de $\mathbb{C}$.
2. Pour tout $z \in \mathbb{Z}[j]$, on note $N(z) = |z|^2$. Montrer que $u \in \mathbb{Z}[j]$ est inversible ssi $N(u) = 1$.
3. En déduire les inversibles de $\mathbb{Z}[j]$.

EXERCICE 28. ♣ – ●●○ *L'anneau* $\mathbb{Z}[\sqrt{3}]$
On note $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3}, (a,b) \in \mathbb{Z}^2\}$.

1. Montrer que $\mathbb{Z}[\sqrt{3}]$ est un sous-anneau de $\mathbb{R}$.
2. Pour tous $(a,b) \in \mathbb{Z}^2$, on note $N(a + b\sqrt{3}) = a^2 - 3b^2$. Pourquoi N est-elle bien définie sur $\mathbb{Z}[\sqrt{3}]$? Montrer que $\forall z, z' \in \mathbb{Z}[\sqrt{3}], N(zz') = N(z)N(z')$.
3. Soit $z \in \mathbb{Z}[\sqrt{3}]$. Montrer que $N(z) = 0$ ssi $z = 0$.
4. Soit $z \in \mathbb{Z}[\sqrt{3}]$. Montrer que $N(z) = \pm 1$ ssi z est inversible.
5. Montrer que l'équation $x^2 - 3y^2 = -1$ n'admet pas de solution avec $(x,y) \in \mathbb{Z}^2$.
6. Montrer qu'un élément inversible $a + b\sqrt{3}$ de $\mathbb{Z}[\sqrt{3}]$ est > 1 ssi $a, b > 0$. En déduire le plus petit élément inversible > 1 de $\mathbb{Z}[\sqrt{3}]$, qu'on notera ω.
7. En considérant les valeurs de ω^n, pour $n \in \mathbb{Z}$, déterminer l'ensemble des inversibles de $\mathbb{Z}[\sqrt{3}]$.

EXERCICE 29. ♣/♢ – ●●○ $1 - ab$ *inversible*
Soient a, b deux éléments d'un anneau. Montrer que $1 - ab$ est inversible ssi $1 - ba$ est inversible.

EXERCICE 30. ●◐○ *L'anneau* $\mathbb{Z}^2$

1. Déterminer les éléments inversibles de $\mathbb{Z}^2$.
2. Déterminer les morphismes d'anneaux de $\mathbb{Z}^2$ dans $\mathbb{Z}$.
3. Déterminer les sous-anneaux de $\mathbb{Z}^2$.

EXERCICE 31. ●○○ *Deux extensions quadratiques de* $\mathbb{Q}$

1. On note $\mathbb{Q}[i] = \left\{a + ib, (a,b) \in \mathbb{Q}^2\right\}$. Montrer que c'est un sous-corps de $\mathbb{C}$.
2. Déterminer ses automorphismes.
3. Mêmes questions avec $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2}, (a,b) \in \mathbb{Q}^2\right\}$.
4. $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[i]$ sont-ils isomorphes ?

EXERCICE 32. ♣ – ●◐○ *Sous-corps premier et morphisme de Frobenius*

1. On suppose que $\mathbb{K}$ est un corps de caractéristique 0.
   Montrer qu'il existe un sous-corps de $\mathbb{K}$ isomorphe à $\mathbb{Q}$.
2. On suppose que $\mathbb{K}$ est un corps de caractéristique $p \in \mathbb{P}$.
   Montrer qu'il existe un sous-corps de $\mathbb{K}$ isomorphe à $\mathbb{F}_p$.
3. Soit $\mathbb{K}$ un corps de caractéristique $p \in \mathbb{P}$.
   Montrer que $\mathrm{Frob} : \mathbb{K} \to \mathbb{K}, x \mapsto x^p$ est un morphisme de corps.

EXERCICE 33. ♢ – ●◐○ *Corps à 4 éléments*
On note $K = \{0, 1, \alpha, \beta\}$ un ensemble à 4 éléments.

1. Montrer qu'il existe une unique structure de corps sur K telle que 0 et 1 sont les éléments neutres pour l'addition et la multiplication.

2. En déduire qu'il existe, à isomorphisme près, un unique corps à 4 éléments.

On note $\mathbb{F}_4$ un tel corps.

3. Quelle est la caractéristique de $\mathbb{F}_4$? Quels sont les automorphismes de corps de $\mathbb{F}_4$?

4. A quels groupes sont isomorphes $(\mathbb{F}_4, +)$ et $(\mathbb{F}_4^*, \times)$?

Indications

Exercice 3. Montrer que l'application $\tau : G \to G, x \mapsto a \star x$ est bijective.

Exercice 8. On pourra utiliser le théorème de Lagrange (*démontré plus tard*) affirmant que si H est un sous-groupe d'un groupe fini G, alors $|H|$ divise $|G|$.

Exercice 11. Si z appartient à un sous-groupe fini de $(\mathbb{C}, \times)$, quel est le module de z ? Réfléchir ensuite selon les arguments des éléments du sous-groupe.

Exercice 29. Si u est l'inverse de $1 - ab$, considérer l'élément $1 + bua$.

Exercice 33. Pour 1., raisonner avec les tables d'addition et de multiplication de K.