TD 19 : Structures algébriques Indications

Groupes : structure et calcul

1 ★ (*Calcul dans un groupe*) Soit $(G,\cdot)$ un groupe. Développer et simplifier les expressions suivantes, ou résoudre les équations suivantes, avec $a,b,c,d,x \in G$ et $n \in \mathbb{Z}$:

1) $(axa^{-1})^{-1}$
2) $(abcd)^{-1}$
3) $(axa^{-1})^n$
4) $axa^{-1} = b$
5) $a^n x b^n = c$
6) $a^{-1}x^{-1} = b^{-1}$

Il s'agit essentiellement d'appliquer scrupuleusement les opérations licites dans un groupe et uniquement celles-là.

2 ★ Soit $n \in \mathbb{N}$. Montrer que $(n\mathbb{Z},+)$ est un groupe.
C'est une simple vérification. Pour rappel, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.

3 ★★☆ On définit sur $\mathbb{R}$ la loi $*$ par $a*b = a+b-ab$.

1) Montrer que $*$ est une l.c.i. associative sur $\mathbb{R}$. Trouver son élément neutre.
2) Est-ce que $(\mathbb{R},*)$ est un groupe ?
3) Déterminer $z \in \mathbb{R}$ tel que $(\mathbb{R}\setminus\{z\},*)$ soit un groupe abélien.

4 ★★☆ On note $\mathrm{Bij}(\mathbb{C})$ l'ensemble des bijections de $\mathbb{C}$ dans $\mathbb{C}$. On admet que $(\mathrm{Bij}(\mathbb{C}),\circ)$ est un groupe. On pose T l'ensemble des translations de $\mathbb{C}$ et S l'ensemble des similitudes de $\mathbb{C}$:

$$T = \{t_a \mid a \in \mathbb{C}\} \qquad \text{avec} \quad t_a : z \mapsto z+a$$

$$S = \left\{\sigma_{a,b} \;\middle|\; (a,b) \in \mathbb{C}^* \times \mathbb{C}\right\} \qquad \text{avec} \quad \sigma_{a,b} : z \mapsto az+b$$

Montrer que T et S sont des sous-groupes de $(\mathrm{Bij}(\mathbb{C}),\circ)$.
En déterminant des symétriques de t_a et $\sigma_{a,b}$ pour $\circ$, on montre en particulier que ces applications sont bijectives, donc que T et S sont bien inclus dans $\mathrm{Bij}(\mathbb{C})$.

5 ★★ Soit H un sous-groupe de $\mathbb{Z}$. Montrer que si $1 \in H$, alors $H = \mathbb{Z}$.
La loi en question est la loi $+$ (sous-entendu car cette loi fait de $\mathbb{Z}$ un groupe). Du fait que $1 \in H$ et que H est un sous-groupe de $\mathbb{Z}$, que peut-on en déduire ?

6 ★★ Soit $(G,\cdot)$ un groupe. On définit le centre de G comme l'ensemble des éléments $a \in G$ qui commutent avec tous les éléments de G, c'est-à-dire :

$$Z(G) := \{a \in G \mid \forall x \in G \quad ax = xa\}$$

Montrer que $Z(G)$ est un sous-groupe de G. Si G est commutatif, que vaut son centre $Z(G)$?
C'est une vérification, mais il faut bien exploiter la caractérisation qui découle de la définition de $Z(G)$: pour tout $a \in G$, on a :

$$a \in Z(G) \iff \forall x \in G \quad ax = xa$$

7 ★★ Soit $\cdot$ une l.c.i. sur un ensemble E. On dit que $a \in E$ est absorbant si : $\forall x \in E \quad ax = xa = a$.

1) Montrer que s'il existe un élément absorbant de E, celui-ci est unique.
2) Déterminer l'élément absorbant de $(\mathbb{R},\times)$.
3) Soit X un ensemble. Déterminer l'élément absorbant de $(\mathscr{P}(X),\cup)$ et de $(\mathscr{P}(X),\cap)$.
4) On suppose que $(E,\cdot)$ est un groupe d'élément neutre e et qui possède un élément absorbant a. Montrer que $e = a$, puis $E = \{e\}$.

1) Pour montrer l'unicité, se donner deux éléments absorbants a_1, a_2 et montrer que $a_1 = a_2$.
4 Utiliser les définitions d'élément absorbant pour e et pour a.

8 ★★ Soit $*$ la l.c.i. définie sur $\mathbb{R}$ par $x*y = x+e^x y$.

1) Montrer que $*$ admet un élément neutre qu'on notera n.
2) Est-ce que $*$ est commutative ?
3) Est-ce que $*$ est associative ?

4) Quels réels sont symétrisables par $*$?

9 ★★☆ Soit $(G,\cdot)$ un groupe. Soit H et K deux sous-groupes de G.

1) Montrer que $H\cap K$ est un sous-groupe de G.
2) Montrer que $H\cup K$ est un sous-groupe de G si et seulement si $H\subset K$ ou $K\subset H$.

1) C'est un classique. Il faut utiliser la caractérisation des sous-groupes et le fait que $z\in H\cap K \iff z\in H$ et $z\in K$.
2) Le sens réciproque est évident. Pour le sens direct, raisonner par contraposée. Utiliser le fait que $H\not\subset K$ équivaut à dire qu'il existe un élément $u\in H\setminus K$.

10 ★★★ On a vu dans un exercice précédent que pour tout $n\in\mathbb{N}$, $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$. Réciproquement, si H est un sous-groupe de $(\mathbb{Z},+)$, montrer que H est de la forme $n\mathbb{Z}$ avec $n\in\mathbb{N}$ à déterminer.
Lorsque $H\neq\{0\}$, on pourra commencer par montrer que $H\cap\mathbb{N}^*$ admet un minimum qu'on note m. Que peut valoir H en fonction de m ?

Morphismes de groupes

11 ★ Soit $(G,\cdot)$ un groupe d'élément neutre e, et soit $a\in G$. On pose

$$f_a : G\to G,\ x\mapsto ax \qquad g_a : G\to G,\ x\mapsto xax$$

Déterminer, en fonction de a, si f_a et g_a sont des morphismes, des endomorphismes, des isomorphismes, des automorphismes.
Utiliser les définitions. Pour ce qui est de montrer si un morphisme φ est un isomorphisme, on peut ou bien exhiber une fonction ψ qui serait sa réciproque, ou bien vérifier que $\operatorname{Ker}\varphi=\{e\}$ et $\operatorname{Im}\varphi=G$.

12 ★★☆ On pose $E=\mathbb{R}_+^*\times\mathbb{R}$ et on définit

$$*: E\times E\to E,\ (r_1,\theta_1),(r_2,\theta_2)\mapsto(r_1r_2,\theta_1+\theta_2)$$

Justifier que $(E,*)$ est un groupe. On pose

$$\varphi: E\to\mathbb{C}^*,\ (r,\theta)\mapsto re^{i\theta}$$

Montrer que φ est un morphisme de $(E,*)$ dans $(\mathbb{C}^*,\times)$. Déterminer son image et son noyau.
$\mathbb{R}_+^*$ est un groupe pour $\times$ et $\mathbb{R}$ est un groupe pour $+$. On peut donc munir E d'une structure de groupe à peu de frais...

13 ★★☆ Soit $n\in\mathbb{N}$, $n\geq 2$. On pose

$$\varphi_n : \mathbb{C}^*\to\mathbb{C}^*,\ x\mapsto x^n$$

1) Montrer que φ_n est un endomorphisme de $(\mathbb{C}^*,\times)$. Est-ce un automorphisme ?
2) En déduire que $\mathbb{U}_n$ est un sous-groupe de $\mathbb{C}^*$.

1) Il faut vérifier si φ_n est un isomorphisme, donc si φ_n est bijective. On peut notamment conclure sur l'injectivité en déterminant $\operatorname{Ker}\varphi_n$.
2) Cela découle naturellement du cours et de la question 1.

14 ★★ Soit $(G,\cdot)$ un groupe d'élément neutre e, et soit $a\in G$. On pose

$$\varphi_a : G\to G,\ x\mapsto axa^{-1}$$

1) Montrer que φ_a est un endomorphisme.
2) Soit $a,b\in G$. Montrer que $\varphi_a\circ\varphi_b=\varphi_c$ pour un élément c de G que l'on précisera.
3) En déduire que que φ_a est bijective et déterminer $(\varphi_a)^{-1}$.
4) On pose $Q=\{\varphi_a \mid a\in G\}$. Montrer que $(Q,\circ)$ est un groupe.
5) Montrer que l'application $\Psi: G\to Q$ définie par $\Psi(a)=\varphi_a$ est un morphisme de groupes.
6) On pose $Z(G)=\{a\in G\mid\forall x\in G\quad ax=xa\}$, i.e. $Z(G)$ est l'ensemble des éléments qui commutent avec tous les éléments de G. Déduire, en utilisant la question précédente, que $Z(G)$ est un sous-groupe de G.

Anneaux : structure et calcul

15 ★★☆ Soit $(G,+)$ un groupe abélien. On note $\mathrm{End}(G)$ l'ensemble des endomorphismes de G. On définit sur $\mathrm{End}(G)$ les lois $+$ et $\circ$ usuelles : $f+g : x \mapsto f(x)+g(x)$ et $g\circ f : x \mapsto g(f(x))$.

1) Montrer que $(\mathrm{End}(G),+,\circ)$ est un anneau.
2) On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G. Montrer que $(\mathrm{Aut}(G),\circ)$ est un groupe.

1) C'est très long ! En effet, il faut vérifier A1–A3 puisqu'on ne connait pas de « sur-anneau » qui contienne $\mathrm{End}(G)$.
2) C'est très court ! Et aussi « très cours ».

16 ★★ Soit $(A,+,\times)$ un anneau. Un élément $x \in A$ est dit nilpotent lorsqu'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0_A$.

1) Soit $x,y \in A$. Montrer que si x est nilpotent et x,y commutent, alors xy est nilpotent.
2) Soit $x,y \in A$. Montrer que si x et y sont nilpotents et commutent, alors $x+y$ est nilpotent.
3) Soit $x \in A$ nilpotent. Montrer que $1-x$ est inversible et calculer $(1-x)^{-1}$, où 1 désigne 1_A.

1) Soit $n \in \mathbb{N}^*$ tel que $x^n = 0_A$. Il faut trouver $m \in \mathbb{N}^*$ tel que $(xy)^m = 0_A$...
2) Soit $m,n \in \mathbb{N}^*$ tel que $x^m = y^n = 0_A$. Il faut trouver $N \in \mathbb{N}^*$ tel que $(x+y)^N = 0_A$... Une recherche au brouillon est conseillée !
3) Soit $n \in \mathbb{N}^*$ tel que $x^n = 0_A$. On pourra utiliser le fait que $1 = 1^n - x^n$.

17 ★★ On note $A = \left\{ m+n\sqrt{6} \mid m,n \in \mathbb{Z} \right\}$.

1) Montrer que $(A,+,\times)$ est un anneau.
2) On pose $\varphi : A \to A$ définie pour tous $m,n \in \mathbb{Z}$ par $\varphi(m+n\sqrt{6}) = m-n\sqrt{6}$. Montrer que φ est un automorphisme. On pourra notamment calculer $\varphi \circ \varphi$.
3) On pose $N : A \to \mathbb{Z}$ définie pour tout $x \in A$ par $N(x) = x\varphi(x)$. Montrer que pour tous $x,y \in A$, on a $N(xy) = N(x)N(y)$.
4) Soit $x \in A$. Montrer que x est inversible si et seulement si $N(x) = \pm 1$.
5) Vérifier que $5+2\sqrt{6}$ est inversible (dans A) et calculer son inverse.

18 ★★ (*Entiers de Gauss*) On définit l'ensemble des entiers de Gauss par :

$$\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$$

1) Montrer que $\mathbb{Z}[i]$ muni des lois $+$ et $\times$ usuelles est un sous-anneau de $\mathbb{C}$.
2) Soit $a+bi$ un entier de Gauss inversible. Montrer que $a^2+b^2 = 1$.
3) En déduire les éléments inversibles de $\mathbb{Z}[i]$.
4) Un entier de Gauss x est dit irréductible si, pour tous $y,z \in \mathbb{Z}[i]$,

$$x = yz \implies \big(y \in \mathrm{Inv}(\mathbb{Z}[i]) \text{ ou } z \in \mathrm{Inv}(\mathbb{Z}[i])\big)$$

Montrer que l'entier 2 est irréductible.

2 Remarquer que le module d'un élément de $\mathbb{Z}[i]$ est un entier.
3 Remarquer que a et b sont entiers.
4 Passer au module dans l'égalité $x = yz$.

19 ★★★ Soit $(A,+,\times)$ un anneau tel que

$$\forall x \in A \quad x^2 = x$$

Montrer que pour tout $x \in A$, on a $-x = x$. En déduire que A est commutatif.
Il s'agit de montrer que pour tout $x \in A$, on a $x+x = 0_A$, ou encore $2x = 0_A$. Utiliser la propriété $\forall y \in A \quad y^2 = y$ pour y arriver et choisir y judicieusement pour faire apparaitre $2x$.

Anneaux intègres, corps

20 ★★☆ Soit $\mathbb{K}$ l'ensemble des complexes sous la forme $p+iq$ avec $p,q \in \mathbb{Q}$. Montrer que $\mathbb{K}$ est un corps.
Il suffit de montrer que $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

21 ★★ Soit $(A,+,\times)$ un anneau intègre fini (i.e. de cardinal fini). Soit $a \in A \setminus \{0_A\}$.

1) Montrer que l'application f_a définie ci-dessous est injective :

$$f_a : A \to A$$
$$x \mapsto ax$$

2) Montrer que $f_a(A)$ et A ont le même nombre d'éléments.
3) Expliquer pourquoi on peut affirmer que $f_a(A) = A$. En déduire que f_a est bijective.
4) En déduire que a est inversible.
5) En déduire que A est un corps.

1) Attention, f_a n'est pas un morphisme a priori. Il faut donc revenir à la définition de l'injectivité pour une application quelconque.
2) Poser $n = \text{card}(A)$ et $A = \{a_1, \cdots, a_n\}$. Dans ce cas $f_a(A) = \{f(a_1), \cdots, f(a_n)\}$. Ceci montre déjà que $\text{card}(f(A)) \leq n$, mais il manque une précision pour pouvoir affirmer que $\text{card}(f(A)) = n$. Laquelle ?
3) Utiliser le fait que $f_a(A) \subset A$ et un peu de "bon sens" (le résultat sera vu rigoureusement au chapitre de dénombrement)
4) Utiliser la définition de l'inversibilité de a et faire apparaitre f_a.

22 ★★☆ Soit X un ensemble. On définit sur $\mathscr{P}(X)$ la loi de différence symétrique notée Δ par :

$$A\Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A) = (A \cap B^c) \cup (B \cap A^c)$$

1) Montrer que $(\mathscr{P}(X), \Delta, \cap)$ est un anneau (on pourra admettre l'associativité de Δ...).
2) Cet anneau est-il intègre ? Quels sont les éléments inversibles ?

1) Il faut utiliser la définition d'un anneau. La première expression de $A\Delta B$ suffit pour trouver l'élément neutre et le symétrique d'un ensemble $A \in \mathscr{P}(X)$. Pour la distributivité, il faut montrer que $(A\Delta B) \cap C = (A\Delta C) \cap (B\Delta C)$. L'écriture $A\Delta B = (A \cap B^c) \cup (B \cap A^c)$ et les propriétés des opérations $\cup$ et $\cap$ permettent de s'en sortir.
2) Prendre $A \neq \varnothing$ et $A \neq X$: montrer qu'il existe $B \in \mathscr{P}(X)$ tel que $A \cap B = \varnothing$. Pour la deuxième partie, prouver le fait que pour deux ensembles C et D qui vérifient $C \setminus D = X$, on doit avoir $C = X$ et $D = \varnothing$.

23 ★★☆ Soit K un sous-corps de $\mathbb{C}$. Montrer que $\mathbb{Q} \subset K$.

En utilisant que $1 \in K$, montrer successivement que $\mathbb{Z} \subset K$, puis que $\mathbb{Q} \subset K$.