UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Feuille n°1 : Groupes et sous-groupes

Exercices à savoir faire chez soi

Les exercices de cette section portent soit sur des notions antérieures au cours d'AR3 et censées être déjà acquises au moment d'aborder le contenu d'AR3, soit sur la compréhension élémentaire des notions introduites dans le cours d'AR3. Il n'est sans doute pas indispensable de les chercher en intégralité, mais il faut au minimum s'assurer qu'on est un tant soit peu à l'aise avec le contenu de ces exercices. Ils ne seront ni traités ni corrigés en TD, et il n'y aura pas de corrigé écrit. Bien entendu, le responsable de module reste à votre disposition pour toute question concernant ces exercices.

Exercice 1

1 Soit E et F des ensembles et $f : E \to F$ une application. Définir « f est injective », « f est surective », « f est bijective ». Donner des exemples.

2 Soit E, F, G et H des ensembles, $f : E \to F$ et $g : G \to H$ des applications. À quelle condition peut-on définir $g \circ f$? Lorsque cette condition est remplie, rappeler la définition de $g \circ f$.

3 Soit E, F, G et H des ensembles, $f : E \to F$, $g : F \to G$ et $h : G \to H$ des applications. Montrer qu'on a

$$h \circ (g \circ f) = (h \circ g) \circ f$$

4 Soit E, F, G des ensembles, $f : E \to F$ et $g : F \to G$ des applications.

1. On suppose f et g injectives ; montrer que $g \circ f$ est injective.
2. On suppose f et g surjectives ; montrer que $g \circ f$ est surjective.
3. On suppose que $g \circ f$ est injective ; montrer que f est injective.
4. On suppose que $g \circ f$ est surjective ; montrer que g est surjective.
5. Donner un exemple où $g \circ f$ est injective et g n'est pas injective.
6. Donner un exemple où $g \circ f$ est surjective et f n'est pas surjective.

5 Soit E, et F des ensembles, et $f : E \to F$ une application.

1. On suppose E non vide ; montrer que f est injective si et seulement s'il existe $g : F \to E$ telle que $g \circ f = \mathrm{Id}_E$.
2. Montrer que f est surjective si et seulement s'il existe $g : F \to E$ telle que $f \circ g = \mathrm{Id}_F$.
3. Montrer que f est bijective si et seulement s'il existe $g : F \to E$ telle que $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$.
4. Donner un exemple où il existe $g : F \to E$ telle que $g \circ f = \mathrm{Id}_E$ et pourtant f n'est pas bijective.

Exercice 2

Soit n un entier naturel non nul. Dans cet exercice, une application f de $F_n = \{1, \ldots, n\}$ dans F_n sera décrite par un tableau à 2 lignes et n colonnes. La première ligne contient les entiers de 1 à n rangés dans l'ordre croissant. Sous l'entier i figure la valeur de $f(i)$. Par exemple

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 2 & 1 & 5 & 2 & 6 \end{pmatrix}$$

représente l'application de $f : F_6 \to F_6$ telle que $f(1) = 2$, $f(2) = 2$, etc...

1 Parmi les applications de F_5 dans F_5 ci-dessous, dire lesquelles sont bijectives.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 3 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$$

Donner d'autres exemples d'applications $F_5 \to F_5$ bijectives. Prenez deux applications f et g parmi les précédentes (celles de l'énoncé et/ou celles que vous avez écrites) et calculer $f \circ g$ et $g \circ f$. Recommencez avec un autre choix de f et g...

2 On considère

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$$

Vérifier que f est une bijection de F_5 sur F_5. Calculer $f^2 = f \circ f$, $f^3 = f \circ f \circ f$. Calculer f^n (f composée avec elle-même n fois) pour tout entier naturel n.

3 On rappelle que $\mathfrak{S}_n$ désigne l'ensemble des bijections de F_n dans F_n. Écrire la liste des éléments de $\mathfrak{S}_n$ pour $n \in \{2, 3, 4\}$. Pour f et g dans $\mathfrak{S}_3$, calculer $f \circ g$. Donner un exemple de deux éléments f et g de $\mathfrak{S}_3$ tels que $f \circ g \neq g \circ f$.

Exercice 3

Soit G un groupe noté multiplicativement, g un élément de G, n et m deux entiers relatifs tels que $g^m = g^n$. A-t-on nécessairement $m = n$?

Exercices à savoir faire

Les exercices de cette catégorie sont conçus pour être d'un niveau suffisamment raisonnable pour pouvoir être abordés sans trop de difficultés et en relative autonomie. Être à l'aise avec le contenu de ces exercices doit constituer un objectif primordial. Les plupart seront traités en TD, mais il est vivement conseillé d'y jeter un oeil avant la séance de TD.

Exercice 4

Soit $(G, \star)$ un groupe.

1 Soit P une partie de G. De préférence sans regarder votre cours, rappeler la définition du sous-groupe de G engendré par P.

2 Soit $g \in G$. On considère l'ensemble $H = \{g^n, \quad n \in \mathbf{Z}\}$. Donner quelques éléments de H. Soit $m \in \mathbf{Z}$. L'élément g^m est-il dans H ?

3 Montrer que H est un sous-groupe de G qui contient g.

4 Soit H' un sous-groupe de G qui contient g. Montrer par récurrence que pour tout entier naturel n, g^n est dans H'. Montrer que H est inclus dans H'.

5 Quel résultat annoncé dans le cours vient-on de démontrer ?

6 Décrire le sous-groupe de $(\mathbf{Z}, +)$ engendré par un élément a.

Exercice 5

Soit E un ensemble. Dans chacune des situations suivantes, déterminer si l'ensemble G est un sous-groupe de $\mathfrak{S}_E$.

1 F est une partie de E, $G = \{\sigma \in \mathfrak{S}_E, \quad \sigma(F) = F\}$;

2 F est une partie de E, $G = \{\sigma \in \mathfrak{S}_E, \quad \sigma(F) \subset F\}$;

3 F est une partie de E, $G = \{\sigma \in \mathfrak{S}_E, \quad \forall x \in F, \quad \sigma(x) = x\}$;

4 E est un **R**-espace vectoriel ;

1. $G = \mathrm{GL}(E) = \{\sigma \in \mathfrak{S}_E, \quad \sigma \text{ est linéaire}\}$;
2. $F \subset E$ un sous-espace vectoriel de dimension finie, $G = \{\sigma \in \mathrm{GL}(E), \quad \sigma(F) \subset F\}$;
3. G est l'ensemble des homothéties de E ;
4. $G = \{\sigma \in \mathrm{GL}(E), \quad \sigma^2 = \mathrm{Id}_E\}$ (ensemble des symétries vectorielles de E) ;

5 $E = \mathbf{R}^n$;

1. $G = \{M \in \mathrm{GL}_n(\mathbf{R}), \quad M \text{ est une matrice diagonale}\}$;
2. $G = \{M \in \mathrm{GL}_n(\mathbf{R}), \quad M \text{ est une matrice triangulaire supérieure}\}$;
3. $G = \{M \in \mathrm{GL}_n(\mathbf{R}), \quad M \text{ est une matrice triangulaire supérieure avec des 1 sur la diagonale}\}$;
4. $G = \{M \in \mathrm{GL}_n(\mathbf{R}), {}^tM.M = I_n\}$;

6 $E = \mathbf{R}^2$ muni du produit scalaire usuel ;

1. G est l'ensemble des isométries ;
2. G est l'ensemble des translations ;
3. G est l'ensemble des rotations vectorielles ;
4. G est l'ensemble des rotations ;
5. G est l'ensemble des homothéties et des translations ;
6. G est l'ensemble des rotations et des translations.

Exercice 6

1 Déterminer si les couples suivants sont des groupes : $(\mathbf{Z}, +)$; $(\mathbf{Z}, \times)$; $(\mathbf{C}^\times, +)$; $(\mathbf{C}^\times, \times)$; $(\mathbf{N} \setminus \{0\}, \star)$ où $a \star b = a^b$.

2 Construire une loi de composition interne pour laquelle $\{-1, 1\}$ est un groupe. Même question avec $\mathbf{R} \times \mathbf{R}$.

3 L'ensemble $\{a, b, c\}$ muni de la loi de composition interne $\star$ définie par la table

$\star$	a	b	c
a	a	b	c
b	b	a	b
c	c	b	a

admet-il un élément neutre ? est-il commutatif ? tout élément admet-il un symétrique ? est-il un groupe ?

4 La réunion de deux sous-groupes d'un groupe G est-elle un sous-groupe ? Et l'intersection ?

5 Donner un exemple d'ensemble avec une loi de composition interne associative sans élément neutre.

Exercice 7

Soit $(E,\star)$ un ensemble muni d'une loi interne associative admettant un élément neutre, noté ε.

1 Soit ε' un élément neutre. Montrer qu'on a $\varepsilon = \varepsilon'$ (en d'autres termes, montrer qu'un élément neutre, s'il existe, est unique). Indication : considérer $\varepsilon \star \varepsilon'$.

2 Soit x un élément de E qui admet un symétrique x'. Soit x'' un symétrique de x. Montrer qu'on a $x' = x''$ (en d'autres termes, montrer qu'un élément symétrique, s'il existe, est unique).

3 Soit x et y dans E qui admettent un symétrique. Montrer que $x \star y$ admet un symétrique, et donner son expression en fonction des symétriques de x et y.

Exercice 8

Soit a et b deux entiers relatifs et $\langle a,b\rangle$ le sous-groupe de $(\mathbf{Z},+)$ engendré par $\{a,b\}$. On rappelle qu'on note $a\mathbf{Z}$ l'ensemble $\{n.a, \quad n\in\mathbf{Z}\}$.

1 Montrer que $a\mathbf{Z}$ est inclus dans $\langle a,b\rangle$.

2 On note $a\mathbf{Z}+b\mathbf{Z}$ l'ensemble $\{n.a+m.b, \quad (n,m)\in\mathbf{Z}^2\}$. Montrer que $a\mathbf{Z}+b\mathbf{Z}$ est inclus dans $\langle a,b\rangle$.

3 Montrer que $a\mathbf{Z}+b\mathbf{Z}$ est un sous-groupe de $(\mathbf{Z},+)$, contenant $\{a,b\}$.

4 Montrer que $\langle a,b\rangle$ est inclus dans $a\mathbf{Z}+b\mathbf{Z}$.

5 Montrer qu'on a $\langle a,b\rangle = a\mathbf{Z}+b\mathbf{Z}$.

6 Montrer qu'on a $\langle a,b\rangle = a\mathbf{Z}+b\mathbf{Z} = \mathrm{pgcd}(a,b)\mathbf{Z}$.

7 Plus généralement, si $a_1,\ldots,a_n$ sont des entiers et $\langle a_1,\ldots,a_n\rangle$ désigne le sous-groupe de $(\mathbf{Z},+)$ engendré par $\{a_1,\ldots,a_n\}$, montrer qu'on a

$$\langle a_1,\ldots,a_n\rangle = a_1\mathbf{Z}+\cdots+a_n\mathbf{Z} = \mathrm{pgcd}(a_1,\ldots,a_n)\mathbf{Z}$$

8 Montrer qu'on a $a\mathbf{Z}\cap b\mathbf{Z} = \mathrm{ppcm}(a,b)\mathbf{Z}$. Généraliser.

9 Application numérique : déterminer $45\mathbf{Z}\cap 60\mathbf{Z}$ et $56\mathbf{Z}+63\mathbf{Z}$.

Exercice 9

1 Soit a et b des entiers relatifs. Montrer qu'on a $a\mathbf{Z}\subset b\mathbf{Z}$ si et seulement si b divise a.

2 Trouver les sous-groupes de $\mathbf{Z}$ contenant $48\mathbf{Z}$ et donner les relations d'inclusion existant entre eux.

Exercice 10

1 L'application $F\ :(\mathbf{Z},+)\to(\mathbf{Z},+)$, $n\mapsto 1$ est-elle un morphisme de groupes ?

2 Déterminer deux morphismes de groupes de $(\mathbf{R},+)$ vers $(\mathbf{R}_+^\times,\times)$.

Exercice 11

1 Soit F un morphisme de groupes de $(\mathbf{Z},+)$ dans lui-même. Montrer qu'il suffit de connaître $F(1)$ pour connaître l'image de chaque entier par F.

2 Existe-t-il un morphisme de groupes de $(\mathbf{Z},+)$ dans lui-même tel que $F(2)=3$?

3 Déterminer tous les morphismes de groupes de $(\mathbf{Z},+)$ dans lui-même tels que $F(2)=\ 4$.

4 Montrer qu'une condition nécessaire et suffisante sur $(a, b) \in \mathbf{Z}^2$ pour qu'il existe un morphisme de groupes de $(\mathbf{Z}, +)$ dans lui-même tel que $F(2) = a$ et $F(5) = b$ est : $5a = 2b$.

Exercice 12

Soit $(G, \star)$ un groupe. Pour tout $g \in G$, on note τ_g l'application de G dans lui-même définie par $\tau_g(h) = g \star h$.

1 Montrer que pour tout $g \in G$, τ_g est une bijection.

2 Montrer que l'application $G \to \mathfrak{S}_G$ qui à g associe τ_g est injective.

3 Montrer que l'application définie à la question précédente est un morphisme de groupes.

Exercices à chercher

Les exercices de cette catégorie sont en général (pas toujours !) d'un niveau de difficulté supérieure à ceux de la catégorie « à savoir faire ». Votre priorité absolue doit être de vous sentir à l'aise avec les exercices de la catégorie « à savoir faire », mais certains d'entre vous (le plus grand nombre possible, je l'espère !) pourront ensuite aborder avec fruit ces exercices un peu plus délicats. Sauf exception a priori rarissime, ils ne seront ni traités ni corrigés en TD, et il n'y aura pas de corrigé écrit. Bien entendu, le responsable de module reste à votre disposition pour toute question concernant ces exercices.

Exercice 13

Soit $E = \{a, b\}$ un ensemble à deux éléments. On cherche à déterminer toutes les structures de groupes sur cet ensemble, c'est-à-dire toutes les lois de composition internes $\star$ sur E qui font de $(E, \star)$ un groupe.

1 Si a est l'élément neutre, quel doit être le symétrique de b ? En déduire la table de multiplication dans ce cas.

2 Combien y a-t-il de structures de groupes différentes sur E ?

Exercice 14

Soit $E = \mathbf{R}^2 \setminus \{(0, 0)\}$, et $\star$ la loi de composition interne définie par :

$$(x, y) \star (x', y') = (xx' - yy', xy' + yx').$$

$(E, \star)$ est-il un groupe ? la loi est-elle commutative ? Indication : on pourra essayer de « reconnaître » $\star$.

Exercice 15

Soit G un groupe noté multiplicativement, d'élément neutre ε, tel que $\forall x \in G, x^2 = \varepsilon$.

Montrer que tout élément de G est son propre inverse. Calculer pour tout $(a, b) \in G^2$, le produit $a.b.a^{-1}.b^{-1}$ et en déduire que G est commutatif.

Exercice 16

Soit $(G, \star)$ un groupe.

1 Montrer que $G \times G$ peut-être muni d'une structure « naturelle » de groupe. Même question pour G^n où n est un entier $\geqslant 3$, puis pour $\mathcal{A}(E, G)$ où E est un ensemble et $\mathcal{A}(E, G)$ est l'ensemble des applications de E dans G.

Le terme « naturel » n'a pas a priori de définition mathématique précise. Le but des questions suivantes est d'expliciter une telle définition dans le cadre qui nous occupe.

2 On note p_1 et p_2 les deux projections $G \times G \to G$. Montrer qu'il existe une unique loi de groupe sur $G \times G$ telle que p_1 et p_2 soient des morphismes de groupes. Vérifier qu'il s'agit bien de la loi « naturelle » déterminée ci-dessus (si ça n'est pas le cas, vous avez l'esprit particulièrement retors...)

3 Généraliser au cas de G^n, où n est un entier $\geqslant 3$.

4 Soit E un ensemble. Pour $x \in E$, on définit comme suit une application $p_x : \mathcal{A}(E, G) \to G$: par composition avec l'injection naturelle $\{x\} \hookrightarrow E$, on obtient une application $\mathcal{A}(E, G) \to \mathcal{A}(\{x\}, G)$. On compose ensuite avec l'application $\mathcal{A}(\{x\}, G) \to G$, $f \mapsto f(x)$ (qui est d'ailleurs une bijection). Montrer qu'il existe une unique loi de groupe sur $\mathcal{A}(E, G)$ telle que pour tout $x \in E$, l'appliction p_x est un morphisme de groupes. Pourquoi les deux questions précédentes sont-elles un cas particulier de celle-ci ?

Exercice 17

Soit E une partie de $\mathbf{R}$. On rappelle que E est dense dans $\mathbf{R}$ si on a la propriété suivante :

$$\forall x \in \mathbf{R}, \quad \forall \varepsilon > 0, \quad \exists y \in E, \quad |x - y| \leqslant \varepsilon$$

Par exemple $\mathbf{Q}$ est dense dans $\mathbf{R}$. Par ailleurs E est dit discret si on a la propriété suivante :

$$\forall x \in E, \quad \exists \varepsilon > 0, \quad E \cap]x - \varepsilon, x + \varepsilon[= \{x\}$$

1 Vérifier qu'un ensemble discret n'est pas dense. Vérifier que $\mathbf{Z}$ est discret, puis que $a\mathbf{Z}$ est discret pour tout $a \in \mathbf{R}$. $\{\frac{1}{n}\}_{n \in \mathbf{N} \setminus \{0\}}$ est-il discret ? Et $\{0\} \cup \{\frac{1}{n}\}_{n \in \mathbf{N} \setminus \{0\}}$? Le but de la suite de l'exercice est de montrer que les sous-groupes de $(\mathbf{R}, +)$ sont soit denses, soit discrets, et que dans ce dernier cas ils sont de la forme $a\mathbf{Z}$.

2 Soit G un sous-groupe discret. Montrer qu'il existe $\varepsilon > 0$ tel que $]0, \varepsilon[\cap G = \varnothing$. En déduire que $a = \mathrm{Inf}(G \cap \mathbf{R}_+^\times)$ est un réel strictement positif.

3 On suppose que $a \notin G$. Montrer qu'il existe deux éléments distincts b, c de G vérifiant $0 < b - a < \varepsilon$ et $0 < c - a < \varepsilon$. Aboutir à une contradiction. Montrer que $G = a\,\mathbf{Z}$.

4 Soit G un sous-groupe non discret. Montrer que pour tout $\varepsilon > 0$, $G \cap]0, \varepsilon[$ est non vide. En déduire que G est dense.

5 Soit $a \in \mathbf{R}$. Trouver une condition nécessaire et suffisante sur a pour que $\mathbf{Z} + \mathbf{Z}\,a$ soit un sous-groupe dense de $\mathbf{R}$.

6 Soit $a \in \mathbf{R}$. Montrer que l'ensemble des valeurs d'adhérence de la suite $\{\sin(2\,\pi\,n\,a)\}$ est soit fini, soit égal à $[-1, 1]$.