FEUILLE N° 1

LU3MA270 – 2023/24

Exercice 1. — *La loi + est une loi de composition interne associative sur* $\mathbb{Z}$ *et* 0 *est neutre. Tout élément* $n \in \mathbb{Z}$ *est inversible d'inverse* $-n$. $(\mathbb{Z}, +)$ *est donc un groupe.*

— *La loi + est une loi de composition interne associative sur* $\mathbb{N}$ *et* 0 *est neutre. Soit* $n > 0$ *un élément non-nul. S'il admettait un inverse dans* $\mathbb{N}$*, cet inverse serait aussi un inverse dans* $\mathbb{Z}$*. Mais l'inverse est unique et on sait que* $-n < 0$*. Ceci donne une contradiction. Donc* $(\mathbb{N}, +)$ *n'est pas un groupe.*

— *En suivant le même raisonnement : on vérifie que* $(\mathbb{Q}, *)$ *est un groupe. Mais l'inverse de* 2 *qui est* $1/2$ *n'est pas entier.* $(\mathbb{N}, *)$ *et* $(\mathbb{Z}, *)$ *ne peuvent donc pas être des groupes.*

— $(\mathbb{R}, +)$ *et* $(\mathbb{C}, +)$ *sont des groupes.*

— $(\mathbb{R}_{>0}, +)$ *n'est pas un groupe car l'inverse de* 1 *dans* $\mathbb{R}$ *est* $-1 \leq 0$.

— $(\mathbb{R}, *)$ *et* $(\mathbb{C}, *)$ *ne sont pas des groupes. L'élément* 0 *n'est pas simplifiable donc il n'est pas inversible.*

— $(\mathbb{C}^*, *)$ *est un groupe.*

— $(\mathbb{R}_{>0}, *)$ *est non-vide, et stable pas multiplication et par passage à l'inverse. C'est donc un sous-groupe de* $(\mathbb{C}^*, *)$.

Exercice 2. *On pose*

$$x * y = x + y + 1/2.$$

C'est une loi de composition interne sur $\mathbb{R}$*. Elle est associative car + est associative :*

$$(x * y) * z = x + y + z + 1 = x * (y * z).$$

Elle est commutative car + est commutative.

Un élément neutre vérifie $e * e = e$*, c'est-à-dire* $2e + 1/2 = e$*. Ça ne peut-être que* $e = -1/2$*. Or* $x * (-1/2) = x$ *et* $*$ *est commutative.* $e = -1/2$ *est donc bien neutre.*

Pour $x \in \mathbb{R}$*,* $x * y = -1/2 \iff y = -x - 1$*. Donc tout élément* $x \in \mathbb{R}$ *est inversible, d'inverse* $-x - 1$.

En conclusion $(\mathbb{R}, *)$ *est un groupe commutatif.*

Exercice 3. *Pour répondre à l'exercice, la loi doit nécessairement ne pas être commutative. On peut penser par exemple à la composition des endomorphismes ou au produit matriciel de matrices carrées. Réfléchir à pourquoi on ne peut pas trouver d'exemple en dimension finie.*

On considère l'espace des suites à valeurs réelles et les opérateurs de décalage :

$$S : (u_0, u_1, \dots) \mapsto (0, u_0, u_1, \dots)$$

et

$$T : (u_0, u_1, u_2, \dots) \mapsto (u_1, u_2, \dots).$$

On a $T \circ S = \mathrm{id}$*, mais ni* T *ni* S *n'est inversible. En effet* S *n'est pas surjective, et* T *n'est pas injective.*

Exercice 4. E *est muni d'une loi de composition interne associative* $*$ *qui admet un neutre* e*. Pour montrer que* $(E, *)$ *est un groupe il ne reste qu'à montrer que tout élément est inversible.*

Supposons que tout élément est inversible à gauche. Soit $x \in E$*. Il existe* $y \in E$ *tel que* $yx = e$ *puis il existe* $z \in E$ *tel que* $zy = e$*. On a donc* $x = ex = zyx = ze = z$*. Ce qui prouve que* y *est aussi inverse à droite de* x.

$(E, *, e)$ *est donc un groupe.*

Exercice 5. *Soit $(G, \cdot, e)$ un groupe tel que $\forall g \in G\colon g^2 = e$. On a $(xy)^{-1} = y^{-1}x^{-1}$. Or pour tout élément $g \in G$ on a $g^{-1} = g$. En appliquant à x, y et xy dans l'identité précédente, on obtient*

$$xy = yx.$$

Le groupe G est donc abélien.

Exercice 6. *Analyse : Dans un groupe G, la multiplication à gauche (à droite) par un élément $g \in G$ est une bijection, d'inverse la multiplication par g^{-1}. Dans la table de la loi de groupe, tous les éléments de G doivent donc apparaître dans chaque ligne et dans chaque colonne. La loi possède aussi un élément neutre.*

Si $G = \{a\}$, la seule table possible est $\begin{bmatrix} * & a \\ a & a \end{bmatrix}$.

Si $G = \{a, b\}$, les seules tables possibles sont $\begin{bmatrix} * & a & b \\ a & a & b \\ b & b & a \end{bmatrix}$ *et* $\begin{bmatrix} * & a & b \\ a & b & a \\ b & a & b \end{bmatrix}$.

Si $G = \{a, b, c\}$, à permutation des éléments a, b, c près (on a choisit de prendre a comme neutre, ce qui donne la première ligne et la première colonne), la seule table possible est $\begin{bmatrix} * & a & b & c \\ a & a & b & c \\ b & b & c & a \\ c & c & a & b \end{bmatrix}$.

Synthèse :

— *Si $G = \{a\}$, on obtient le groupe trivial.*
— *Si $G = \{a, b\}$, on obtient des groupes abéliens isomorphes à $(\mathbb{Z}/2\mathbb{Z}, +)$.*
— *Si $G = \{a, b, c\}$, on obtient des groupes abéliens isomorphes à $(\mathbb{Z}/3\mathbb{Z}, +)$.*

Exercice 7. *(a) Il faut montrer l'équivalence entre les axiomes :*
{ $e \in H$, H stable par $*$, H stable par passage à l'inverse }
et les axiomes :
{ $H \neq \emptyset$, $\forall x, y \in H\colon x * y^{-1} \in H$ }.

Il est clair que le premier ensemble d'axiomes implique le second.

Réciproquement, soit $x, y \in H$ (un tel x existe puisque H est non-vide). Alors : $x * x^{-1} = e \in H$, puis : $e * x^{-1} = x^{-1} \in H$, puis : $x * (y^{-1})^{-1} = x * y \in H$.

(b) Si H est fini et stable par la loi, alors pour tout $x \in H$, l'ensemble $\{x^n, n \in \mathbb{N}\}$ est inclus dans H. Or il n'y a pas d'injection de $\mathbb{N}$ dans un ensemble fini. On en déduit qu'il existe $n > m$ tel que $x^n = x^m$. L'élément x du groupe G étant simplifiable, on obtient que $x^{n-m} = e$, ce qui prouve que x est inversible, d'inverse x^{n-m-1}. Si H est fini, stable par la loi et de plus non-vide, on vérifie donc les axiomes des sous-groupes de G.

(c) Le sous-ensemble $\mathbb{N} \subset \mathbb{Z}$ est non-vide et stable par $+$, mais ce n'est pas un sous-groupe.

Exercice 8. *On rappelle que l'ensemble S_X des permutations de X est l'ensemble des bijections $X \to X$. C'est un groupe pour la composition, de neutre* id.

(a) Il est clair que $\mathrm{id} \in H$. *Puisque $(g \circ h)(Y) = g(h(Y))$, H est stable par composition. Il reste à démontrer que H est stable par passage à l'inverse. Si $g(Y) \subseteq Y$, alors $Y \subseteq g^{-1}(Y)$. Si $Y \subseteq g(Y)$, par injectivité de g, on a $g^{-1}(Y) \subseteq Y$. Finalement on a bien $g^{-1}(Y) = Y$, ce qui finit de prouver que H est un sous-groupe.*

(b) Pour un ensemble Y fini, $f\colon Y \to Y$ est bijective si et seulement si elle est injective. Si $g(Y) \subseteq Y$, on peut définir la restriction $g\colon Y \to Y$, qui est injective puisque g l'est. Si l'ensemble Y est fini, alors g est bijective, et on a bien $g(Y) = Y$.

darondeau@imj-prg.fr

Exercice 9. *(a) L'application $N\colon \mathbb{C}^* \to \mathbb{R}^*$ donnée par $N(z) = |z|$ est un morphisme de groupes, de noyau $\mathbb{U}$.*

(b) Puisque $u\bar{u} = 1$, on a :

$$(r_u)^{-1} = r_{\bar{u}}$$

et :

$$(s_u)^{-1} = s_u.$$

(c) On a $r_1 = \mathrm{id}$, et $r_{uv}(z) = uvz = r_u \circ r_v(z)$. Donc $u \mapsto r_u$ est un morphisme de groupes.

Si $r_u = \mathrm{id}$, alors $r_u(1) = u = 1$, donc ce morphisme est injectif.

(d)

$$s_u = s_v \implies s_u(1) = s_v(1) \iff u = v.$$

L'application $u \mapsto s_u$ est injective.

(e) Le sous-ensemble G contient l'identité et est stable par inversion. De plus, on a

- $r_u \circ r_v = r_{uv}$;
- $r_u \circ s_v = s_{uv}$;
- $s_v \circ r_u = s_{\bar{u}v}$;
- $s_u \circ s_v = r_{u\bar{v}}$.

Le sous-ensemble G est donc stable par $\circ$. On obtient que G est un sous-groupe. Les identités ci-dessus montrent qu'il n'est pas abélien.

(f) Les applications $r_u\colon \mathbb{R}^2 \to \mathbb{R}^2$ et $s_u\colon \mathbb{R}^2 \to \mathbb{R}^2$ sont $\mathbb{R}$-linéaires. Si $u = a + ib$, elles ont pour matrices respectives dans la base canonique

$$\mathrm{Mat}(s_u) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

et

$$\mathrm{Mat}(r_u) = \begin{bmatrix} a & b \\ b & -a \end{bmatrix}.$$

On en déduit que $\det(s_u) = |u|^2 \geq 0$ et $\det(s_u) = -|u|^2 \leq 0$. Si $s_u = r_v$, on a donc $|u| = |v| = 0$, ce qui contredit $u, v \in \mathbb{C}^*$.

(g) Si pour un élément $z \in P_n$, $r_u(z) = uz \in P_n$, alors en multipliant par $z^{-1} \in P_n$, on obtient $u \in P_n$. Réciproquement si $u \in P_n$, pour tout $z \in P_n$, on a $uz \in P_n$.

Si pour un élément $z \in P_n$, $s_u(z) = u\bar{z} \in P_n$, alors en multipliant par $z = \bar{z}^{-1} \in P_n$, on obtient $u \in P_n$. Réciproquement si $u \in P_n$, pour tout $z \in P_n$, on a $u\bar{z} = uz^{-1} \in P_n$.

En conclusion :

$$H_n = \{r_u, u \in P_n\} \cup \{s_u, u \in P_n\}.$$

(h) Si $u = e^{i\theta}$, alors r_u est la rotation d'angle θ et s_u est la symétrie axiale par rapport à la droite de pente $\theta/2$.

P_n est constitué des sommets d'un polygone régulier à n côtés.

Montrons que le groupe H_n est le groupe des isométries de P_n (les isométries sont les bijections préservant les distances).

En effet, une isométrie préserve les diamètres donc les sommets sont envoyés sur les sommets. Une isométrie préserve les distances donc deux sommets voisins sont envoyés sur deux sommets voisins. Enfin une isométrie préserve les barycentres donc l'image des sommets détermine l'image de tous les points du polygone.

Il reste donc a étudier les permutations des sommets qui préserve les voisins. Une telle permutation est déterminé par l'image u du sommet 1 et par le sens de parcours du polygône.

Si le sens ne change pas, c'est la rotation r_u, si le sens change, c'est la symétrie axiale s_u.

darondeau@imj-prg.fr