Algèbre 2 – TD n°2
$\mathbb{Z}/n\mathbb{Z}$. Le théorème des restes chinois. Groupes.

Exercice 1 1. Donner la liste de tous les couples $(\lambda, \eta) \in \mathbb{Z}_{12} \times \mathbb{Z}_{12}$ tels que $\lambda \cdot \eta = [0]_{12}$.
2. Résoudre l'équation $x^2 - ([5]_{12})x + [6]_{12} = [0]_{12}$ dans $\mathbb{Z}_{12}$.

Exercice 2 Dresser la table de la multiplication sur $(\mathbb{Z}/30\mathbb{Z})^\times$.

Exercice 3 Trouver $[k] \in \mathbb{Z}_{330}$ tels que $k \equiv 2 \pmod 6$, $q \equiv 3 \pmod 5$, $q \equiv 10 \pmod{11}$.

Exercice 4 Parmi les exemples suivants, indiquer lesquels sont des groupes :

1. L'ensemble des nombres entiers pairs muni de l'addition.
2. L'ensemble des nombres entiers impairs muni de la multiplication.
3. L'ensemble $\mathbb{C}$ des nombres complexes muni de la soustraction
4. L'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ muni de l'addition.
5. L'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ muni de la multiplication.
6. L'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ muni de la composition.

Exercice 5 Montrer que le paires suivantes sont des groupes :

1. $(\{\pm 1\}, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ où $\cdot$ désigne la multiplication.
2. $(\mathbb{R}_n[X], +)$, $(\mathbb{R}[X], +)$, $(\mathbb{R}^n, +)$.
3. $(U, \cdot)$, où $U := \{z \in \mathbb{C} |\ |z| = 1\}$.
4. $(U_n, \cdot)$, où $U_n := \{z \in \mathbb{C} |\ z^n = 1\}$.
5. $(\mathfrak{S}(E), \circ)$, où E est un ensemble, $\mathfrak{S}(E) := \{f : E \to E |\ f \text{ est bijective}\}$, et $\circ$ désigne la composition.
6. $(\mathrm{Iso}(X), \circ)$, où (X, d) est un espace métrique, $\mathrm{Iso}(X) := \{f : X \to X |\ f \text{ est une isométrie bijective}\}$, et $\circ$ désigne la composition.
7. $(\mathrm{GL}(n, \mathbb{R}), \cdot)$, $(\mathrm{GL}(n, \mathbb{C}), \cdot)$ où $\mathrm{GL}(n, \mathbb{R}) := \{A \in M_{n,n}(\mathbb{R}) |\ \det(A) \neq 0\}$, $\mathrm{GL}(n, \mathbb{C}) := \{A \in M_{n,n}(\mathbb{C}) |\ \det(A) \neq 0\}$, et $\cdot$ désigne la multiplication matricielle.
8. $(\mathrm{SL}(n, \mathbb{R}), \cdot)$, $(\mathrm{SL}(n, \mathbb{C}), \cdot)$ où $\mathrm{SL}(n, \mathbb{R}) := \{A \in M_{n,n}(\mathbb{R}) |\ \det(A) = 1\}$, $\mathrm{SL}(n, \mathbb{C}) := \{A \in M_{n,n}(\mathbb{C}) |\ \det(A) = 1\}$, et $\cdot$ désigne la multiplication matricielle.
9. $(\mathcal{F}(X, G), *)$ où $(G, *)$ est un groupe, $\mathcal{F}(X, G) := \{f : X \to G\}$, et la loi $*$ sur $\mathcal{F}(X, G)$ est définie par $(f * g)(x) := f(x) * g(x)\ \forall x \in X$.

Exercice 6 Montrer que les lois suivantes munissent l'ensemble G indiqué d'une structure de groupe, et préciser s'il est abélien :

1. Sur $G := \mathcal{P}(X)$, l'ensemble des parties de X, la loi de différence symétrique, définie par :
$$A \Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)\ .$$
2. Sur $G :=]-1, 1[$ la loi $*$ définie par $x * y := \frac{x+y}{1+xy}$.
3. Sur $G = \mathbb{R}^2$ la loi $*$ définie par $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} * \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ x_2 e^{y_1} + y_2 e^{x_1} \end{pmatrix}$.
4. Sur $G := \{a, b, c, d\}$ la loi donnée par la table

$*$	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	b	a
d	c	d	a	b

Exercice 7 (Un groupe fini d'ordre 4). Soient les quatre applications de $\mathbb{C}^*$ dans $\mathbb{C}^*$:

$$f_1(z) = z \ , \ f_2(z) = \frac{1}{z} \ , \ f_3(z) = -z \ , \ f_4(z) = -\frac{1}{z} \ .$$

Montrer que $G = \{f_1, f_2, f_3, f_4\}$ est un groupe pour la loi $\circ$, et dresser sa table.

Exercice 8 (Groupe produit). Soit $(G, \cdot)$ et $(H, *)$ deux groupes. On définit sur $G \times H$ la loi $\circ$ définie par :

$$(x, y) \circ (x', y') = (x \cdot x', y * y') \ .$$

1. Montrer que $(G \times H, \circ)$ est un groupe,
2. Si G est un groupe d'ordre 2, dresser la table de $G \times G$.

Exercice 9 (Groupes d'isométries du plan). Soit $\triangle ABC$ un triangle équilatéral du plan.

1. Déterminer l'ensemble des rotations laissant globalement invariant l'ensemble $\{A, B, C\}$. Montrer que cet ensemble est un groupe pour la loi $\circ$.
2. Déterminer l'ensemble des reflexions laissant invariant $\{A, B, C\}$. Est-ce un groupe (par rapport à la composition des applications) ?
3. Montrer que l'ensemble formé des réflexions et rotations laissant invariant $\{A, B, C\}$ est un groupe.
4. Répondre aux questions précédentes pour pour un carré $ABCD$.

Exercice 10 (Exemples de sous-groupes). Soit $(G, \cdot)$ un groupe.

1. Montrer que le centre de G défini par $Z(G) := \{x \in G |\ \forall y \in G \ x \cdot y = y \cdot x\}$ est un sous-groupe abélien et distingué de G.
2. Soit H un sous-groupe de G et $a \in G$. Montrer que le conjugué de H définit par $aHa^{-1} := \{a \cdot h \cdot a^{-1} |\ h \in H\}$ est un sous-groupe de G (qui coïncide avec H si $a \in Z(G)$).

Exercice 11 (Exemples de sous-groupes). Revenir aux exemples de l'exercice 5 et mettre en évidence les inclusions de la forme $H \subset G$ où H est un sous-groupe de G. *Exemple :* $U_n \subset \mathbb{C}^*$.

Exercice 12 (Produit de deux sous-groupes). Soit $(G, \cdot)$ un groupe et A, B deux sous-groupes. On note

$$A \cdot B := \{a \cdot b |\ a \in A, \ b \in B\} \, .$$

1. Montrer que $A \cdot B$ est un sous-groupe de G si et seulement si $A \cdot B = B \cdot A$.
2. On suppose que $A \cap B = \{e\}$. Montrer que l'application $f : A \times B \to A \cdot B$ définie par $f(a, b) = ab$ est bijective. En déduire que, si A et B sont finis, alors $A \cdot B$ est fini et $|A \cdot B| = |A| \times |B|$.
3. Supposons que $(G, \cdot)$ est abélien (en particulier la condition $A \cdot B = B \cdot A$ est satisfaite, et $A \cdot B$ est un sous-groupe de G), et $A \cap B = \{e\}$. Définir un isomorphisme $f : A \times B \to A \cdot B$ (où $A \times B$ est muni de la lci produit).

Pour l'implication : AB est un sous-groupe implique $AB = BA$.

Attention, nous savons seulement que AB est un sous-groupe, aucune information sur BA !

Supposons que AB est un sous-groupe. Soit $x \in BA$, donc il existe $(a, b) \in A \times B$ t.q. $x = ba$; il en résulte $a^{-1}b^{-1} \in AB$, qui est un sous-groupe par hypothèse, donc $(a^{-1}b^{-1})^{-1} \in AB$. Mais $(a^{-1}b^{-1})^{-1} = ba$, donc $x = ba \in AB$. Donc $BA \subset AB$. Réciproquement, soit $x =\in AB$, donc il existe $(a, b) \in A \times B$ t.q. $x = ab$. Il en résulte $x^{-1} = b^{-1}a^{-1} \in BA \subset AB$, donc il existe $\alpha \in A$, $\beta \in B$ tels que $b^{-1}a^{-1} = \alpha\beta$. Donc $x = ab = \beta^{-1}\alpha^{-1} \in BA$. Donc $AB \subset BA$.

Exercice 13 Soit G un groupe d'élément neutre e, tel que $x^2 = e$ pour tout $x \in G$.

1. Montrer que G est abélien.
2. Soit H un sous-groupe de G distinct de G, et soit $a \in G \setminus H$.
   (a) Montrer que $H \cap aH = \emptyset$.
   (b) Montrer que $H \cup aH$ est un sous-groupe de G, et ce sous-groupe est isomorphe à $H \times \mathbb{Z}_2$, en particulier $|H \cup aH| = 2|H|$.

3. En déduire que si G est d'ordre fini, alors il existe $k \in \mathbb{N}$ tel que $G \simeq \mathbb{Z}_2^k$, en particulier $|G| = 2^k$.
   Indication : Recurrence par rapport à $n := |G|$. Supposons $|G| > 1$, et soit $m \in \mathbb{N}$ maximal tel que G admet un sous-groupe $H \subsetneq G$ d'ordre m. Choisir $a \in G \setminus H$ et montrer que $G = H \cup aH$.

Exercice 14 Déterminer $\mathbb{Z}_{10}^\times$ et écrire la table de ce groupe. Démontrer que $(\mathbb{Z}_{10}^\times, \cdot)$ est un groupe cyclique, et en déduire que $(\mathbb{Z}_{10}^\times, \cdot) \simeq (\mathbb{Z}_4, +)$. Est-ce que le groupe $(\mathbb{Z}_{30}^\times, \cdot)$ est cyclique ?

Exercice 15 (Image réciproque, image directe de sous-groupe). Soient $(G, \cdot)$ et $(\tilde{G}, *)$ groupes, $f : G \to \tilde{G}$ un morphisme.

1. Montrer que si $\tilde{H}$ est un sous-groupe de $\tilde{G}$, alors $f^{-1}(\tilde{H})$ est un sous-groupe de G, qui sera normal si $\tilde{H}$ est normal.
2. Montrer que si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de $\tilde{G}$. Montrer que $f(H)$ est normal si H est normal et f est surjective.

Exercice 16 (Un endomorphisme) Soit l'application $\varphi : \mathcal{F}(\mathbb{R}, \mathbb{R}) \to \mathcal{F}(\mathbb{R}, \mathbb{R})$ qui à une fonction $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ associe la fonction $\varphi(f) : \mathbb{R} \to \mathbb{R}$ donnée par $x \mapsto f(x) + f(-x)$.

1. Montrer que φ est un endomorphisme de $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +)$.
2. Décrire le noyau et l'image de φ. (Reconnaitre des espaces de fonctions aux propriétés connues)

Exercice 17 * (Endomorphismes des groupes de nombres). Un endomorphisme d'un groupe $(G, *)$ est un morphisme de groupes $f : G \to G$. L'ensemble des endomorphismes de $(G, *)$ est noté $\mathrm{End}(G, *)$. Si G est abélien, alors $\mathrm{End}(G)$ est un sous-groupe de $\mathcal{F}(G, G)$ (voir l'exo 5 Q9), en particulier un groupe. Un automorphisme de $(G, *)$ est un isomorphisme $G \to G$. L'ensemble $\mathrm{Aut}(G, *)$ des automorphismes de G, muni de la composition des automorphismes, est un groupe.

1. Trouver tous les endomorphismes et les automorphismes du groupe $(\mathbb{Z}, +)$.
2. Trouver tous les endomorphismes du groupe $(\mathbb{Q}, +)$.
3. Trouver tous les endomorphismes continus du groupe $(\mathbb{R}, +)$.

Exercice 18 (L'application d'inversion) Soit $(G, \cdot)$ un groupe, et l'application $\iota : G \to G$ définie par $\iota(x) = x^{-1}$.

1. Montrer que ι est un morphisme de groupes si et seulement si G est abélien.
2. Dans ce cas, montrer que ι est un isomorphisme.
3. Déterminer le sous-groupe engendré par ι dans le groupe $(\mathrm{Aut}(G), \circ)$. Faire attention au cas où G est un groupe avec la propriété $x^2 = e$ pour tout $x \in G$ (voir l'exercice 13).

Exercice 19 (exemples de groupes isomorphes).

1. Montrer que $(\mathbb{R}_+^*, \cdot)$ est isomorphe à $(\mathbb{R}, +)$.
2. Montrer que le groupe $\mathrm{U}_n \subset \mathbb{C}^*$ des racines n-ièmes de l'unité est isomorphe à $\mathbb{Z}_n$.
3. Montrer que le groupe des isométries qui préservent un rectangle (non carré) est isomorphe à $\mathbb{Z}_2^2$.
4. Construire des isomorphismes $(\mathbb{Z}_2, +) \xrightarrow{\simeq} (\mathbb{Z}_6^\times, \cdot)$, $(\mathbb{Z}_4, +) \xrightarrow{\simeq} (\mathbb{Z}_5^\times, \cdot)$, $(\mathbb{Z}_2 \times \mathbb{Z}_4, +) \xrightarrow{\simeq} (\mathbb{Z}_{30}^\times, \cdot)$.
5. Montrer que le groupe $(\{f_1, f_2, f_3, f_4\}, \circ)$ de l'exercice 7, et le groupe $(\{a, b, c, d\}, *)$ de l'exercice 6 (4) sont isomorphes à $\mathbb{Z}_2 \times \mathbb{Z}_2$.
6. Montrer que le groupe $(\mathcal{P}(X), \Delta)$ introduit dans l'exercice 6 est isomorphe au groupe $(\mathcal{F}(X, \mathbb{Z}_2), +)$ des applications $X \to \mathbb{Z}_2$ muni de la lci définie par $(f + g)(x) = f(x) + g(x)$.

Exercice 20 (Groupes d'endomorphismes, groupes d'automorphismes). Soit $n \in \mathbb{N}^*$, $n \geq 2$. Définir des isomorphismes $\mathbb{Z}_n \to \mathrm{End}(\mathbb{Z}_n, +)$, $\mathbb{Z}_n^\times \to \mathrm{Aut}(\mathbb{Z}_n, +)$.

Exercice 21 Montrer que tout groupe d'ordre 4 est isomorphe soit à $\mathbb{Z}_4$ soit à $\mathbb{Z}_2 \times \mathbb{Z}_2$. Donner des exemples de sous-groupes de $\mathrm{Iso}(\mathbb{R}^2)$ (où $\mathbb{R}^2$ est regardé comme espace métrique muni de la distance standard d_2) qui sont isomorphes à ces deux groupes.

Exercice 22 Soient p, q nombres premiers distincts. Montrer que tout groupe *abélien* d'ordre pq est cyclique, donc isomorphe à $\mathbb{Z}_{pq}$. *Indication : Utiliser l'exercice 12.*