Géométrie et Arithmétique 2 – TD n°2 : Sous-groupes, Homorphismes, Groupes quotients, le groupe $\mathbb{Z}_n$, le théorème de Lagrange et le théorème des restes chinois

Exercice 1 Soit $H \subset \mathbb{Z}$ un sous-groupe non-trivial (i.e. $H \neq \{0\}$).

1. Montrer que $H \cap \mathbb{N}^* \neq \emptyset$,
2. En utilisant le théorème de division euclidienne montrer que $H = d\mathbb{Z}$, où $d := \min(H \cap \mathbb{N}^*)$. En déduire que *tout sous-groupe de $\mathbb{Z}$ est un sous-groupe cyclique*.

Exercice 2

1. Soit $(G, \cdot)$ un groupe et $H, H' \subset G$ deux sous-groupes. Montrer que $H \cap H'$ est un sous-groupe de G.
2. Soit $(A, +)$ un groupe abélien, et $H, H' \subset A$ deux sous-groupes. Montrer que

$$H + H' := \{x + x' | \, x \in H, \; x' \in H'\}$$

est un sous-groupe de A. Montrer par un exemple que l'affirmation n'est pas vraie dans la cas non-abélien.

Exercice 3 Soient $m, n \in \mathbb{N}^*$. Rappeler la définition de $\text{pgcd}(m,n)$, $\text{ppcm}(m,n)$. Montrer que

1. $m\mathbb{Z} + n\mathbb{Z} = \text{pgcd}(m,n)\mathbb{Z}$,
2. $m\mathbb{Z} \cap n\mathbb{Z} = \text{ppcm}(m,n)\mathbb{Z}$,
3. $m\mathbb{Z} \subset n\mathbb{Z}$ si et seulement si m est un multiple de n, et si c'est le cas, alors a un isomorphisme $n\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_d$, où $d := m/n$.

Exercice 4 Soit $n \in \mathbb{N}^*$.

1. Montrer que tout sous-groupe de $\mathbb{Z}_n$ est cyclique.
2. Soit $x = [k] \in \mathbb{Z}_n$.
   (a) Montrer que $\langle x \rangle = \langle \text{pgcd}(k,n) \rangle$, et $\langle x \rangle \simeq \mathbb{Z}_l$, où $l := \dfrac{n}{\text{pgcd}(k,n)}$.
   (b) Construire un isomorphisme $\mathbb{Z}_n \big/ \langle x \rangle \xrightarrow{\simeq} \mathbb{Z}_d$, où $d := \text{pgcd}(k,n)$.

Exercice 5 Pour $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$ on va désigner par $[k]_n$ la classe de congruence de k modulo n. Soit $m, n \in \mathbb{N}^*$.

1. Montrer que la formule $g([k]_{mn}) = ([k]_m, [k]_n)$ définit un homomorphisme de groupes $g : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$.
2. Préciser $\ker(g)$, $\text{im}(g)$.
3. Étudier le cas où m, n sont premiers entre eux (i.e. où $\text{pgcd}(m,n) = 1$).
4. Généraliser ces résultats pour un système $(n_1, \dots n_k) \in (\mathbb{N}^*)^k$ (ou $k \geq 2$).

Exercice 6 Classifier les sous-groupes et les sous-groupes distingués des groupes suivants :

1. $\mathbb{Z}_6$, $\mathfrak{S}_3$.
2. Le groupe diédral D_4 (le groupe d'isométries d'un carré). *Indication : Soit $D_4^0 \simeq \mathrm{U}_4$ le sous-groupe formé par les rotations qui laissent invariant le carré. Classifier d'abord les sous-groupes de D_4^0, puis les sous-groupes d'ordre 2 engendrés par une reflexion. Montrer que D_4 a aussi deux sous-groupes d'ordre 4 non-cycliques (donc isomorphes à $\mathbb{Z}_2 \times \mathbb{Z}_2$), chacun de ces sous-groupes contenant deux reflexions par rapport à deux axes perpendiculaires.*

Exercice 7 Montrer que tout sous-groupe d'indice 2 est distingué.

Exercice 8 Pour tout nombre complexe $z = a + ib$ non nul (avec a et b réels), posons $M(z) := \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

1. Vérifier que $M(z)$ est inversible pour tout $z \in \mathbb{C}^*$,
2. Prouver que l'application $M : \mathbb{C}^* \to \mathrm{GL}(2, \mathbb{R})$ donnée par $z \mapsto M(z)$ est un homomorphisme de groupes. Cet homomorphisme est-il injectif ? Est-il surjectif ?

Exercice 9 Rappelons qu'un isomorphisme $f : G \to G$ s'appelle automorphisme de G. Montrer que l'application $\mathrm{GL}(n,\mathbb{R}) \to \mathrm{GL}(n,\mathbb{R})$ donnée par $A \mapsto {}^t(A^{-1})$ est un automorphisme de $\mathrm{GL}(n,\mathbb{R})$.

Exercice 10 Soient G, G' et G'' trois groupes et $f : G \to G'$, $g : G' \to G''$ deux applications.

1. Supposer : f et g des homomorphismes. Déduire : $g \circ f$ est un homomorphisme.
2. Supposer : $g \circ f$ et g des homomorphismes et g injectif. Déduire : f est un homomorphisme.
3. Supposer : $g \circ f$ et f des homomorphismes et f surjectif. Déduire : g est un homomorphisme.
4. Donner un exemple où f et g ne sont pas des homomorphismes tandis que $g \circ f$ est un homomorphisme.

Exercice 11 Soit G un groupe. Rappelons qu'un isomorphisme $f : G \to G$ s'appelle automorphisme de G. A tout élément a de G on associe une application $f_a : G \to G$ par

$$f_a(x) = axa^{-1}.$$

1. Montrer que f_a est un automorphisme de G (on dit que c'est un *automorphisme intérieur*).
2. Montrer que $f_a = \mathrm{id}_G$ si et seulement si $a \in Z(G) = \{z \in G \mid \forall g \in G, gz = zg\}$ (le centre de G).
3. Montrer que l'ensemble $\mathrm{Aut}(G)$ des automorphismes de G est un groupe (avec l'opération de composition d'applications).
4. Montrer que l'ensemble des automorphismes intérieurs $\mathrm{Int}(G)$ est un sous-groupe du groupe $\mathrm{Aut}(G)$. Ce sous-groupe est-il distingué dans $\mathrm{Aut}(G)$?
5. Montrer que l'application $\phi : G \to \mathrm{Int}(G)$, définie par $\phi(a) = f_a$, est un homomorphisme.
6. Déterminer le noyau de ϕ.
7. Soit $H \subset G$ un sous-groupe de G. Montrer que pour tout $a \in G$ l'image $f_a(H)$ de H par f_a est un sous-groupe de G isomorphe à H, et que H est distingué si et seulement si $\forall a \in G,\ f_a(H) = H$.

Exercice 12 En utilisant le premier théorème d'isomorphisme construire des isomorphismes

1. $\mathbb{R}/\mathbb{Z} \xrightarrow{\simeq} U$, où $U := \{z \in \mathbb{C} \mid |z| = 1\}$,
2. $\mathbb{C}^*/U \simeq \mathbb{R}_+^*$, $\mathbb{C}^*/\mathbb{R}_+^* \simeq U$,
3. $\mathbb{R}^*/\mathbb{R}_+^* \xrightarrow{\simeq} \{\pm 1\}$,
4. $\mathbb{Z}_n \xrightarrow{\simeq} U_n$, où $n \in \mathbb{N}^*$ et $U_n := \{z \in \mathbb{C} \mid z^n = 1\}$,
5. $\mathrm{GL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{R}) \xrightarrow{\simeq} \mathbb{R}^*$, $\mathrm{GL}(n,\mathbb{C})/\mathrm{SL}(n,\mathbb{C}) \xrightarrow{\simeq} \mathbb{C}^*$.

Exercice 13 Trouver $[m], [n], [p], [q] \in \mathbb{Z}_{330}$ tels que

1. $m \equiv 1 \pmod 6$, $m \equiv 0 \pmod 5$, $m \equiv 0 \pmod{11}$.
2. $n \equiv 0 \pmod 6$, $n \equiv 1 \pmod 5$, $n \equiv 0 \pmod{11}$.
3. $p \equiv 0 \pmod 6$, $p \equiv 0 \pmod 5$, $p \equiv 1 \pmod{11}$.
4. $q \equiv 2 \pmod 6$, $q \equiv 3 \pmod 5$, $q \equiv 10 \pmod{11}$.

Exercice 14 Un corps (commutatif) est un triplet $(K, +, \cdot)$, où $+, \cdot$ sont deux lois de composition internes sur K telles que

(1) $(K, +)$ est un groupe abélien, dont l'élément neutre sera noté 0_K.

(2) $(K \setminus \{0_K\}, \cdot)$ est un groupe abélien, dont l'élément neutre sera noté 1_K.

(3) la lci $\cdot$ est distributive par rapport à la lci $+$, i.e. pour tout $(x, y, z) \in K \times K \times K$ on a $x \cdot (y + z) = x \cdot y + x \cdot z$.

1. Soit $n \in \mathbb{N}^*$. Montrer que sont équivalentes :
   (a) $(\mathbb{Z}_n, +, \cdot)$ est un corps.
   (b) n est un nombre premier.

   Pour un nombre premier p, le corps $(\mathbb{Z}_p, +, \cdot)$ sera noté $\mathbb{F}_p$. Noter que ce corps est fini.
2. Combien de droites vectorielles il y a-t-il dans l'espace vectoriel $\mathbb{F}_p^n$?

Exercice 15 Démontrer la version multiplicative du lemme chinois : [la version multiplicative du lemme chinois] Soit $(n_1,\dots,n_k) \in (\mathbb{N}^*)^k$ une famille de k nombres premiers entre eux deux à deux, et soit $n := \prod_{i=1}^k n_i$ leur produit. Alors la formule

$$h([x]_n) := ([x]_{n_1},\dots,[x]_{n_k})$$

définit un isomorphisme de groupes $h : \mathbb{Z}_n^\times \xrightarrow{\simeq} \bigtimes_{i=1}^k \mathbb{Z}_{n_i}^\times$.

Application : Définir un isomorphisme $(\mathbb{Z}_4 \times \mathbb{Z}_6, +) \to (\mathbb{Z}_{35}^\times, \cdot)$, et montrer que $\mathbb{Z}_{35}^\times$ n'est pas un groupe cyclique.

Remarque : En utilisant la théorie des anneaux on peut démontrer que pour tout nombre *premier* $p \in \mathbb{N}^*$, le groupe des unités $\mathbb{Z}_p^\times = \mathbb{Z}_p^*$ est un groupe cyclique d'ordre $p-1$. En plus, si $p \neq 2$, alors $\mathbb{Z}_{p^r}^\times$ est aussi cyclique pour tout $r \geq 2$. $\mathbb{Z}_4^\times$ est aussi cyclique. Par contre, pour $r > 2$ le groupe $\mathbb{Z}_{2^r}^\times$ n'est pas cyclique ; il est isomorphe au produit $\mathbb{Z}_2 \times \mathbb{Z}_{2^{r-2}}$. En utilisant ces remarques montrer que $\mathbb{Z}_n^\times$ est cyclique si et seulement si $n = 4$, ou une puissance d'un premier impair, ou le double d'une telle puissance.