Exercice 1

1) Théorème de Lagrange

Soit G un groupe d'ordre fini n, $H<G$ un sous-groupe d'ordre m.
On considère la relation de congruence modulo H :

$$\forall g_1, g_2 \in G \qquad g_1 \equiv g_2 \bmod H \iff \exists h \in H \text{ tq } g_1 = g_2 h.$$

C'est une relation d'équivalence :

i) pour $g \in G$, $g = g \cdot 1$, donc $g \equiv g \bmod H$;

ii) soit $g_1, g_2 \in G$ tq $g_1 \equiv g_2 \bmod H$: il existe $h \in H$ tq $g_1 = g_2 h$;
on a donc $g_2 = g_1 h^{-1}$, et ainsi $g_2 \equiv g_1 \bmod H$ puisque $h^{-1} \in H$;

iii) soit $g_1, g_2, g_3 \in G$ tq $g_1 \equiv g_2 \bmod H$ et $g_2 \equiv g_3 \bmod H$:
il existe $h_1, h_2 \in H$ tq $g_1 = g_2 h_1$ et $g_2 = g_3 h_2$.
Ainsi $g_1 = g_3(h_2 h_1)$ et $g_1 \equiv g_3 \bmod H$ puisque $h_2 h_1 \in H$.

On en déduit que G est partitionné selon les classes de congruence modulo H.
Ces classes sont toutes de cardinal m : en effet, l'application

$$h \in H \longmapsto gh \in \overline{g}$$

(étant donné $g \in G$, et notant $\overline{g}$ sa classe)
~~est~~ surjective par définition, et injective car si $gh = gh'$ alors $h = h'$
puisque g est inversible.

On en déduit $n = \begin{pmatrix}\text{nombre de classes} \\ \text{modulo } H\end{pmatrix} \times m$ et en particulier $m \mid n$. $\square$

2) Groupe quotient

Pour $g_1, g_2 \in G$, on veut poser $\overline{g_1} \cdot \overline{g_2} = \overline{g_1 g_2}$.
Vérifions que c'est indépendant du choix des représentants des classes :
soit $k_1, k_2 \in K$; on va montrer que $\overline{g_1 k_1 g_2 k_2} = \overline{g_1 g_2}$;
on a $g_1 k_1 g_2 k_2 = g_1 g_2\, g_2^{-1} k_1 g_2 k_2$, et $g_2^{-1} k_1 g_2 \in K$ puisque
K est distingué, donc $g_2^{-1} k_1 g_2 k_2 \in K$ et $g_1 k_1 g_2 k_2 \equiv g_1 g_2 \bmod K$
comme il fallait démontrer.

On a donc muni G/K d'une opération interne.
On vérifie sans peine que les axiomes en faisant une loi de groupe sont satisfaits, en utilisant ces axiomes pour l'opération interne sur G.

Montrons que $\pi : x \in G \longmapsto \bar{x} \in G/K$ est un morphisme de groupes.
Par définition de la multiplication sur G/K, si $x_1, x_2 \in G$:

$$\pi(x_1 x_2) = \overline{x_1 x_2} = \overline{x_1} \cdot \overline{x_2} = \pi(x_1) \cdot \pi(x_2)$$

donc c'est bon.
π est surjectif puisque toute classe modulo K possède un représentant.

3) On considère $\phi : G \longrightarrow H$ tq $\phi(K) = 1$.

On veut poser pour tout $g \in G$, $\bar{\Phi}(\bar{g}) = \phi(g)$. Pour cela, il faut vérifier que pour tout $k \in K$: $\phi(gk) = \phi(g)$.
Or $\phi(gk) = \phi(g)\,\phi(k)$ puisque ϕ morphisme
$= \phi(g) \cdot 1$ par hypothèse.
Donc notre définition est bien valide, et visiblement $\bar{\Phi}$ est un morphisme de groupes ; par définition on a $\phi = \bar{\Phi} \circ \pi$.

Pour tout morphisme $\psi : G/K \longrightarrow H$, la condition $\phi = \psi \circ \pi$ impose pour tout $g \in G$: $\psi(\bar{g}) = \phi(g)$.
Donc notre définition pour $\bar{\Phi}$ est la seule possible, et l'unicité est démontrée.

Exercice 2

1) Sous-groupes de $(\mathbb{Z},+)$

Soit H un tel sous-groupe. Si $H=\{0\}$ il est monogène, sinon considérons
$$a = \operatorname{Min}\{h\in H,\ h>0\}.$$
On va montrer que $H=a\mathbb{Z}$. Puisque $a\mathbb{Z}=\langle a\rangle$ et $a\in H$, on a $a\mathbb{Z}\subseteq H$.
Réciproquement soit $h\in H$. On écrit sa division euclidienne par a:
$$h = aq+r \quad \text{avec } q,r\in\mathbb{Z},\ 0\leq r<a.$$
Puisque $r = h+q(-a)$, $r\in H$. Donc comme $0\leq r<a$, on a nécessairement $r=0$ et ainsi $h\in a\mathbb{Z}$. □

2) Sous-groupes de $(\mathbb{Z}/n,+)$

Soit H un tel sous-groupe.
On regarde $\pi : a\in\mathbb{Z}\longmapsto \bar{a}\in\mathbb{Z}/n$ morphisme de groupes surjectifs.
$\pi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$, donc il existe $d\in\mathbb{Z}$ tq
$$\pi^{-1}(H) = d\mathbb{Z}$$
d'après 1). On va voir que $\pi(d)$ est un générateur de H: déjà $\pi(d)\in H$ donc $\langle\pi(d)\rangle\subseteq H$.
Réciproquement, pour $h\in H$ il existe $a\in\mathbb{Z}$ tq $\pi(a)=h$ par surjectivité de π; $a\in\pi^{-1}(H)$ donc il existe $k\in\mathbb{Z}$ tq $a=dk$.
Alors $h=\pi(a)=\pi(k.d)=k.\pi(d)\in\langle\pi(d)\rangle$. □

3) Ordre de $\overline{114}$

On a $114 = 2\times3\times19$ et $252=2^2\times3^2\times7$
donc pgcd$(114,252)=6$.
On sait donc que $\langle\overline{114}\rangle=\langle\bar{6}\rangle$ et on en déduit
$$\text{ordre}(\overline{114}) = \text{ordre}(\bar{6}) = \frac{252}{6} = 6\times7=42.$$

4) $(\mathbb{Q},+)$ pas de type fini

~~Supposons par l'absurde qu'il existe~~ Soit $a_1,\dots,a_n\in\mathbb{Z}$, $b_1,\dots,b_n\in\mathbb{Z}^*$ ~~tq~~ et $q\in\left\langle \frac{a_1}{b_1},\dots,\frac{a_n}{b_n}\right\rangle$ ~~$=(\mathbb{Q},+)$~~.

Il existe des entiers $u_1,\dots,u_n$ tq

$$q=u_1\frac{a_1}{b_1}+\dots+u_n\frac{a_n}{b_n}=\sum_{i=1}^{n}\frac{u_ia_i\prod_{j\neq i}b_j}{b_1\cdots b_n}$$

donc $(b_1\cdots b_n)\,q\in\mathbb{Z}$.

Or $b_1\cdots b_n\cdot\dfrac{1}{b_1\cdots b_n+1}\notin\mathbb{Z}$ donc $\left\langle \frac{a_1}{b_1},\dots,\frac{a_n}{b_n}\right\rangle\subsetneq\mathbb{Q}$

et $\mathbb{Q}$ ne peut pas être engendré par un nombre fini d'éléments. $\square$

5) On utilise de façon répétée le théorème d'isomorphisme chinois:

a) $$\mathbb{Z}/14\times\mathbb{Z}/18=(\mathbb{Z}/2\times\mathbb{Z}/7)\times(\mathbb{Z}/2\times\mathbb{Z}/9)$$

$$=(\mathbb{Z}/2\times\mathbb{Z}/7\times\mathbb{Z}/9)\times\mathbb{Z}/2=\mathbb{Z}/2\times\mathbb{Z}/126$$

b) $\mathbb{Z}/28\times\mathbb{Z}/9=\mathbb{Z}/252$ puisque $3\nmid 28$ donc $9\wedge 28=1$.

On conclut avec le théorème de structure des groupes abéliens de type fini que les deux groupes a) et b) ne sont __pas__ isomorphes.

6) On effectue des multiplications à gauche et à droite par des matrices de $GL_3(\mathbb{Z})$ pour écrire une suite de matrices équivalentes sur $\mathbb{Z}$:

$$\begin{pmatrix}1&6&6\\4&1&6\\6&4&0\end{pmatrix}\sim\begin{array}{c}\\ L_2-4L_1\\ L_3-6L_1\end{array}\begin{pmatrix}1&6&6\\0&-23&-18\\0&-32&-36\end{pmatrix}$$

$$\sim\begin{array}{ccc}&C_2-6C_1&C_3-6C_1\\ \end{array}\begin{pmatrix}1&0&0\\0&-23&-18\\0&-32&-36\end{pmatrix}$$

$$\sim \begin{array}{l} -7L_2+5L_3 \\ 32L_2-23L_3 \end{array} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & * \\ 0 & 0 & 252 \end{pmatrix}$$

autorisé car $\begin{vmatrix} -7 & 5 \\ 32 & -23 \end{vmatrix} = 161 - 160 = +1$

$$\begin{array}{c} C_3 - *C_2 \\ \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 252 \end{pmatrix}. \end{array}$$

On en déduit un isomorphisme de groupes

$$\mathbb{Z}^3/N \simeq \mathbb{Z}^3/\mathbb{Z}\times\mathbb{Z}\times 252\mathbb{Z} \simeq \mathbb{Z}/252\mathbb{Z}$$

donc $\mathbb{Z}^3/N$ est isomorphe à $\mathbb{Z}/_{28}\times\mathbb{Z}/_9$ mais pas à $\mathbb{Z}/_{14}\times\mathbb{Z}/_{18}$

7) On sait qu'il existe des entiers d_1, d_2, d_3 tq les matrices

$$\begin{pmatrix} 1 & 1 & 1 \\ 7 & 8 & 4 \\ 7 & 5 & 0 \\ 7 & 5 & 9 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \\ 0 & 0 & 0 \end{pmatrix}$$

sont équivalentes sur $\mathbb{Z}$. Ainsi

$$\mathbb{Z}^4/N \simeq \mathbb{Z}/_{d_1}\times\mathbb{Z}/_{d_2}\times\mathbb{Z}/_{d_3}\times\mathbb{Z}$$

et $(0,0,0,1)$ est un élément d'ordre ∞ dans le groupe de droite.

<u>NB</u> Gauss est né en 1777 et mort en 1855.

Exercice 3

1) On écrit σ comme produit de cycles à supports disjoints :

$$\sigma = (1\ 4\ 3\ 8)(2\ 7)(5\ 11\ 9\ 10).$$

On en déduit que σ est d'ordre 4.

Or $2019 \equiv 19 \equiv -1 \mod 4$.

Donc $\sigma^{2019} = \sigma^{-1} = (8\ 3\ 4\ 1)(2\ 7)(10\ 9\ 11\ 5)$.

2) Deux permutations sont conjuguées ssi leurs décompositions en produits de cycles à supports disjoints sont du même type.

Ainsi, tout $\sigma \in \mathfrak{S}_5$ est conjugué à une et une seule des permutations suivantes :

i) id ; 1 élément

ii) $(1\ 2)$; $\binom{5}{2} = 10$ éléments

iii) $(1\ 2\ 3)$; $\frac{5 \times 4 \times 3}{3} = 20$ éléments (choix d'un (a, b, c) avec a, b, c 2 à 2 $\neq$; chaque 3-cycle apparaît 3 fois)

iv) $(1\ 2\ 3\ 4)$; $\frac{5 \times 4 \times 3 \times 2}{4} = 30$ éléments (idem)

v) $(1\ 2\ 3\ 4\ 5)$; $\frac{5!}{5} = 24$ éléments (idem)

vi) $(1\ 2)(3\ 4)$; $\frac{1}{2} \times \binom{5}{2}\binom{3}{2} = \frac{10 \times 3}{2} = 15$ éléments

(choix de $\{a, b\}$ et $\{c, d\}$ avec a, b, c, d 2 à 2 $\neq$; chaque double-transposition apparaît 2 fois)

vii) $(1\ 2\ 3)(4\ 5)$; $2 \times \binom{5}{2} = 20$ éléments

(pour chaque choix de support de la transposition, une seule transposition et deux 3-cycles possibles).

On vérifie que

$$1 + 10 + 20 + 30 + 24 + 15 + 20 = 120 = |\mathfrak{S}_5| = 5!$$

11 31 61 85 100

3) 3-cycles dans $\mathfrak{A}_5$

- On a $(1\ 2\ 3) =$

$$= (2\,3)\,(1\ 3\ 2)\,(2\,3)^{-1}$$

- Soit κ un 3-cycle. Tous les 3-cycles sont conjugués dans $\mathfrak{S}_5$, donc il existe $\sigma \in \mathfrak{S}_5$ tq

$$\kappa = \sigma\,(1\ 2\ 3)\,\sigma^{-1}.$$

Si $\varepsilon(\sigma) = +1$, alors κ est conjugué à $(1\ 2\ 3)$ dans $\mathfrak{A}_5$.

Si $\varepsilon(\sigma) = -1$, alors $\quad \varepsilon(\sigma(2\,3)) = +1$

$$\text{et} \quad \kappa = \sigma\,(2\,3)\,(1\ 3\ 2)\,(2\ 3)^{-1}\,\sigma^{-1}$$

donc κ est conjugué à $(1\ 3\ 2)$ dans $\mathfrak{A}_5$.

- On a $\quad (1\ 2\ 3) = (2\,3)(4\,5)\cdot(1\ 3\ 2)\,\big((2\,3)(4\,5)\big)^{-1}$

donc $(1\ 2\ 3)$ et $(1\ 3\ 2)$ sont conjugués dans $\mathfrak{A}_5$.

Puisque tout 3-cycle est conjugué ou à $(1\ 2\ 3)$ ou à $(1\ 3\ 2)$, on en déduit que tous les 3-cycles sont conjugués dans $\mathfrak{A}_5$. $\square$

4)

On a $\quad \mathrm{Stab}_G(h) = \{ g \in G,\ ghg^{-1} = h \}$

donc $\quad \mathrm{Stab}_G(h) \cap H = \{ g \in H :\ ghg^{-1} = h \}$

$$= \mathrm{Stab}_H(h). \qquad \square$$

5)

a) Notons $\omega_{\mathfrak{S}}$ l'orbite de κ sous l'action de $\mathfrak{S}_5$.

D'après 2) : $\quad |\omega_{\mathfrak{S}}| = 24$

On sait que $\quad |\omega_{\mathfrak{S}}| = \dfrac{|\mathfrak{S}_5|}{|\mathrm{Stab}_{\mathfrak{S}_5}(\kappa)|} \quad$ donc $\left| \mathrm{Stab}_{\mathfrak{S}_5}(\kappa) \right| = \dfrac{120}{24} = 5.$

Or clairement $\langle \kappa \rangle \subset \mathrm{Stab}_{\mathfrak{S}_5}(\kappa)$ et $\langle \kappa \rangle \cong \mathbb{Z}/5$ est d'ordre 5.
On en conclut que $\mathrm{Stab}_{\mathfrak{S}_5}(\kappa) = \langle \kappa \rangle$. $\square$

b) D'après 4) et 5a), on a :

$$\mathrm{Stab}_{\mathfrak{A}_5}(\kappa) = \mathrm{Stab}_{\mathfrak{S}_5}(\kappa) \cap \mathfrak{A}_5 = \langle \kappa \rangle \cap \mathfrak{A}_5 = \langle \kappa \rangle. \quad \square$$

c) Notons $\omega_{\mathfrak{A}_5}$ l'orbite de κ sous l'action de $\mathfrak{A}_5$.
On a
$$|\omega_{\mathfrak{A}_5}| = \frac{|\mathfrak{A}_5|}{|\mathrm{Stab}_{\mathfrak{A}_5}(\kappa)|} = \frac{60}{5} = 12.$$

Le même raisonnement prouve que toute classe de conjugaison de 5-cycle dans $\mathfrak{A}_5$ contient 12 éléments.
Puisqu'il y a 24 5-cycles en tout, il y a donc 2 classes de conjugaison de 5-cycles dans $\mathfrak{A}_5$.

d) On a $(1\ 2\ 3\ 5\ 4) = (4\ 5)(1\ 2\ 3\ 4\ 5)(4\ 5)^{-1}$
donc si $(1\ 2\ 3\ 5\ 4)$ et $(1\ 2\ 3\ 4\ 5)$ étaient conjugués dans $\mathfrak{A}_5$, tous les 5-cycles seraient conjugués dans $\mathfrak{A}_5$ par le même raisonnement qu'en 3), une contradiction.
Donc $(1\ 2\ 3\ 5\ 4)$ et $(1\ 2\ 3\ 4\ 5)$ ne sont pas conjugués dans $\mathfrak{A}_5$.