Exercice 11. Montrer de façon la plus élémentaire possible que tout groupe d'ordre 4 est abélien. (*Indication : vous avez droit au théorème de Lagrange, mais guère plus*).

Corrigé :

Soit G un groupe d'ordre 4.

Par Lagrange, tout élément distinct du neutre dans G est d'ordre 2 ou 4.

Si G admet un élément d'ordre 4, alors il est cyclique donc abélien (car isomorphe à $\mathbb{Z}/4\mathbb{Z}$).

Si G admet seulement des éléments d'ordre 2 à part le neutre, montrons qu'il est abélien. Soit $a, b \in G$. Si $a = b$, $a = 1$ ou $b = 1$, clairement a et b commutent. Sinon ab est un élément de G distinct du neutre, donc lui aussi d'ordre 2, et l'égalité $1 = abab$ est équivalente à $ab = ba$ (car a, b d'ordre 2 implique $a = a^{-1}$, $b = b^{-1}$).

Exercice 12. Montrer qu'il existe exactement 20 groupes abéliens d'ordre $\leqslant 15$ à isomorphisme près. On donnera leur forme canonique successivement sous forme "facteurs invariants" et sous forme "facteurs élémentaires".

Corrigé :

Il y a déjà 15 groupes cycliques d'ordre $n \leqslant 15$. Pour chacun, la décomposition "facteurs invariants" consiste juste à écrire $\mathbb{Z}/n\mathbb{Z}$, et la décomposition "facteurs élémentaires" consiste à écrire la décomposition en facteurs premiers de n. Par exemple pour $n = 12 = 2^2 \cdot 3$, on a $\mathbb{Z}/12 = \mathbb{Z}/4 \times \mathbb{Z}/3$.

Intéressons nous maintenant aux groupes abéliens non cycliques d'ordre $n \geqslant 15$. Il en existe pour chaque n dont la décomposition en facteurs premiers admet au moins un exposant $\geqslant 2$: donc pour $n = 4, 8, 9, 12$.

Pour $n = 4, 8, 9$, comme n est une puissance d'un premier, les décompositions "facteurs invariants" et "facteurs élémentaires" coïncident pour les 4 groupes suivants :

$$\mathbb{Z}/2 \times \mathbb{Z}/2, \qquad \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2, \qquad \mathbb{Z}/4 \times \mathbb{Z}/2, \qquad \mathbb{Z}/3 \times \mathbb{Z}/3.$$

Enfin pour $n = 12$, on a le groupe non cyclique suivant, que l'on donne sous forme "facteurs invariants" puis "facteurs élémentaires" :

$$\mathbb{Z}/6 \times \mathbb{Z}/2 \simeq \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3$$

Au total on a donc bien 20 groupes abéliens d'ordre $\leqslant 15$.

Exercice 13. Soit $p > 2$ un nombre premier, et G un groupe non abélien d'ordre $2p$.

(1) Montrer qu'il existe $x, y \in G$ avec x d'ordre 2, y s'ordre p et $G = \langle x, y \rangle$.

(2) Montrer que $xyx = y^i$ pour un certain $2 \leqslant i \leqslant p-1$, puis montrer que $i^2 \equiv 1 \mod p$, et en déduire que $i = p - 1$.

(3) Montrer que G est isomorphe au groupe diédral D_p.

Corrigé :

(1) Le fait qu'il existe $x \in G$ d'ordre 2 et $y \in G$ d'ordre p découle du théorème de Cauchy vu en cours. Comme $\langle x \rangle \subsetneq \langle x, y \rangle$ et $\langle y \rangle \subsetneq \langle x, y \rangle$, par Lagrange l'ordre du sous-groupe $\langle x, y \rangle \subset G$ est un multiple strict de 2 et de p, et un diviseur de $2p$. On en déduit que cet ordre est égal à $2p$, et donc $\langle x, y \rangle = G$.

(2) Le groupe $\langle y\rangle$ est d'indice 2 dans G, donc est distingué. On en déduit que $xyx^{-1} = xyx \in \langle y\rangle$, ce qui revient à dire qu'il existe $1 \leqslant i \leqslant p-1$ tel que $xyx = y^i$. Enfin $i \neq 1$, car sinon x et y commutent, et comme ils engendrent G le groupe G serait abélien, en contradiction avec l'hypothèse.

Puisque $x^2 = 1$, on a

$$y = x^2yx^2 = x(xyx)x = xy^ix = (xyx)^i = (y^i)^i = y^{i^2},$$

d'où $i^2 = 1 \mod p$ puisque y est d'ordre p.

L'équation $x^2 = 1$ a deux solutions sur le corps $\mathbb{Z}/p\mathbb{Z}$: $x = \bar{1}$ et $x = -\bar{1}$. Mais comme on a $i \geqslant 2$, on en déduit que $\bar{i} = -\bar{1}$ et $i = p-1$.

(3) Le groupe diédral D_p est engendré par une rotation r d'ordre p et une symétrie axiale s : on peut prendre r la rotation d'angle $\frac{2\pi}{p}$, et s la symétrie par rapport à l'axe des abscisses. On a alors

$$D_p = \{1, s, r, rs, r^2, r^2s, \ldots, r^{p-1}, r^{p-1}s\}$$

et la loi de groupe sur D_p se déduit des relations $s^2 = 1$, $r^p = 1$ et $srs = r^{-1}$.

Par les questions précédentes, tout groupe G non abélien d'ordre $2p$ peut s'écrire

$$G = \{1, x, y, yx, y^2, y^2x, \ldots, y^{p-1}, y^{p-1}x\}$$

avec $x^2 = 1$, $y^p = 1$ et $xyx = y^{-1}$. On en déduit que G est isomorphe à D_p, via l'isomorphisme qui envoie x sur s et y sur r.

Exercice 14. Soit G un groupe non abélien d'ordre 8.

(1) Montrer que G contient un élément x d'ordre 4, puis montrer que le groupe $\langle x\rangle$ est distingué dans G.

(2) Supposons que $y \in G$ soit un élément d'ordre 2 distinct de x^2. Montrer que $yxy = x^3$, puis que $G = \langle x, y\rangle$ est isomorphe au groupe diédral D_4.

(3) Supposons que x^2 est le seul élément d'ordre 2 dans G. Montrer que pour tout choix de $z \in G\setminus\langle x\rangle$, on a $xz = zx^{-1}$, puis que $G = \langle x, z\rangle$ est isomorphe au groupe quaternonique $\mathbb{H}_8$.

(4) Conclure qu'il existe exactement cinq groupes d'ordre 8 à isomorphisme près, et en faire la liste.

Corrigé :

(1) Par Lagrange tout élément distinct du neutre dans G est d'ordre 2,4 ou 8. Si G contient un élément d'ordre 8, il est cyclique donc abélien, contradiction. Si G ne contient que des éléments d'ordre 2 à part le neutre, alors il est abélien (voir argument dans corrigé exo 11), contradiction à nouveau. On en déduit que G contient au moins un élément x d'ordre 4, et comme le groupe $\langle x\rangle$ est alors d'indice 2 dans G, il est distingué.

(2) Si y est d'ordre 2 et est distinct de x^2, alors le groupe $\langle x, y\rangle$ contient strictement $\langle x\rangle$ et donc par Lagrange doit être d'ordre 8, c'est-à-dire $\langle x, y\rangle = G$.

Comme on a vu que $\langle x\rangle$ est distingué dans G, on a $yxy = yxy^{-1} = x^i$ pour un certain exposant $0 \leqslant i \leqslant 3$. Comme yxy doit être d'ordre 4 (la conjugaison préserve l'ordre), on a $i = 1$ ou $i = 3$. Le cas $i = 1$ impliquerait que x et y commutent, et donc que G est abélien : contradiction. Donc $i = 3$.

Comme dans le corrigé de l'exo 13, on montre que les relations $x^4 = 1$, $y^2 = 1$ et $yxy = x^{-1}$ caractérise le groupe diédral, donc $G \simeq D_4$.

(3) Si x^2 est l'unique élément d'ordre 2 de G, tout élément $z \in G \setminus \langle x \rangle$ est d'ordre 4. Par Lagrange à nouveau on déduit $G = \langle x, z \rangle$, et comme $xz \neq zx$ et que $z^{-1}xz$ est un élément d'ordre 4, on obtient $xz = zx^{-1}$. Les relations $x^4 = 1$, $z^4 = 1$, $x^2 = z^2$, $xz = zx^{-1}$ caractérisent la loi de groupe sur G, dont on peut écrire les éléments sous la forme

$$G = \{1, x, x^2, x^3, z, xz, x^2z, x^3z\}$$

Comme ces mêmes relations sont satisfaites par les éléments I, J du groupe quaternionique $\mathbb{H}_8$, le groupe G lui est isomorphe (l'isomorphisme étant déterminé en posant $\varphi(x) = I$, $\varphi(z) = J$).

Rappel : On appelle groupe quaternionique le groupe d'ordre 8

$$\mathbb{H}_8 = \{\pm \mathrm{id}, \pm I, \pm J, \pm K\} \subset \mathrm{SL}_2(\mathbb{C})$$

où

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \text{ et } K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Noter que $IJ = K$, et $I^2 = J^2 = K^2 = -\mathrm{id}$, donc on peut écrire

$$\mathbb{H}_8 = \{\mathrm{id}, I, I^2, I^3, J, IJ, I^2J, I^3J\}$$

(4) En conclusion, il existe cinq groupes d'ordre 8 à isomorphisme près :

- Trois sont abéliens : $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;
- Deux sont non abéliens : le groupe diédral D_4 et le groupe quaternionique $\mathbb{H}_8$.

Exercice 15.

(1) Montrer que le sous-groupe $\mathbb{H}_{12}$ de $\mathrm{SL}_2(\mathbb{C})$ engendré par les matrices $I = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ et $K = \left(\begin{smallmatrix} j & 0 \\ 0 & j^2 \end{smallmatrix}\right)$ est d'ordre 12 (où on a noté $j = e^{2i\pi/3}$).

(2) Montrer que les groupes d'ordre 12 suivants sont deux à deux non isomorphes : $\mathbb{H}_{12}$, A_4 (groupe alterné) et D_6 (groupe diédral).

Corrigé :

(1) On vérifie que la matrice I est d'ordre 4 et la matrice K d'ordre 3. De plus $IK = K^2I$:

$$IK = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} j & 0 \\ 0 & j^2 \end{pmatrix} = \begin{pmatrix} 0 & j^2 \\ -j & 0 \end{pmatrix} = \begin{pmatrix} j^2 & 0 \\ 0 & j \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = K^2I.$$

On en déduit que le groupe $\mathbb{H}_{12} = \langle I, K \rangle$ est constitué des 12 matrices suivantes :

$$\mathbb{H}_{12} = \{\mathrm{id}, I, I^2, I^3, K, KI, KI^2, KI^3, K^{-1}, K^{-1}I, K^{-1}I^2, K^{-1}I^3\}$$

(2) L'élément $KI^2 = \left(\begin{smallmatrix} -j & 0 \\ 0 & -j^2 \end{smallmatrix}\right)$ est d'ordre 6 dans $\mathbb{H}_{12}$, alors que A_4 ne contient aucun élément d'ordre 6, donc $\mathbb{H}_{12}$ et A_4 ne sont pas isomorphes.

D_6 contient 7 éléments d'ordre 2 (6 symétries axiales et la rotation d'angle π), alors que A_4 n'en contient que 3 (les doubles transpositions), donc D_6 et A_4 ne sont pas isomorphes.

L'élément I est d'ordre 4 dans $\mathbb{H}_{12}$, alors que D_6 ne contient aucun élément d'ordre 4, donc $\mathbb{H}_{12}$ et D_6 ne sont pas isomorphes.

Exercice 16. On admet que l'exercice précédent donne la liste complète des groupes non abéliens d'ordre 12. En déduire qu'il existe exactement huit groupes non abéliens d'ordre $\leqslant 15$, et en donner la liste.

Corrigé :

On sait que sont abéliens les groupes d'ordre n suivant :

- $n = 1$: trivial !
- $n = p$ premier : cela règle le cas de $n = 2, 3, 5, 7, 11, 13$.
- $n = p^2$ carré d'un nombre premier cela règle le cas de $n = 4, 9$. (résultat vu en cours, pour $n = 4$ l'exo 11 proposait une méthode élémentaire).

On a vu dans l'exo 13 que pour $n = 6, 10, 14$, l'unique groupe non abélien d'ordre n est le groupe diédral. Cela nous laisse avec les cas $n = 8$ (vu dans l'exo 14), $n = 12$ (vu dans l'exo 15) et enfin $n = 15$.

Si G est un groupe d'ordre 15, par le théorème de Sylow G admet un unique 3-Sylow S_3 et un unique 5-Sylow S_5. On en déduit que G est le produit direct de S_3 et S_5, et par le théorème des restes chinois G est donc cyclique :

$$G = S_3 \times S_5 \simeq \mathbb{Z}/3 \times \mathbb{Z}/15 \simeq \mathbb{Z}/15.$$

Bilan : les huits groupes non abéliens d'ordre $n \leqslant 15$ sont à isomorphismes près :

$$D_3, D_4, \mathbb{H}_8, D_5, D_6, A_4, \mathbb{H}_{12}, D_7.$$

Exercice 17. Notons $T \subset \mathrm{GL}_3(\mathbb{Z}/3\mathbb{Z})$ le sous-groupe des matrices de la forme

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, a, b, c \in \mathbb{Z}/3.$$

(1) Montrer que tout élément non trivial de T est d'ordre 3.

(2) Le groupe T est-il isomorphe à $\mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/3$?

(3) En quoi cet exemple est-il intéressant ?

Corrigé :

(1) On peut utiliser le fait que sur n'importe quel corps $\mathbf{k}$, toute matrice de la forme

$$N = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}$$

est nilpotente d'indice 3, c'est-à-dire $N^3 = 0$ (plutôt que de le vérifier en faisant le produit matriciel, on peut juste constater que les vecteurs e_1, e_2, e_3 de la base satisfont $Ne_1 = 0$, $N^2e_2 = Nae_1 = 0$ et $N^3e_3 = N^2(be_1+ce_2) = 0$). Donc une matrice de la forme $I + N$ vérifie

$$(I + N)^3 = I + 3N + 3N^2.$$

Si maintenant le corps est de caractéristique 3 (comme ici $\mathbb{Z}/3$), alors $(I + N)^3 = I$ et donc tout élément non trivial de T est d'ordre 3.

(2) Le groupe T n'est pas isomorphe à $\mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/3$, car T n'est pas abélien. En effet par exemple :

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

(3) Cet exercice devrait vous convaincre que le raisonnement suivant, vu dans d'innombrables copies par le passé, n'est pas correct :

"Montrons que S_3 et Isom(T) sont isomorphes. S_3 contient le neutre, 3 éléments d'ordre 2 (les transpositions) et 2 éléments d'ordre 3 (les 3-cycles). De même, Isom(T) contient le neutre, 3 éléments d'ordre 2 (les symétries axiales) et 2 rotations d'ordre 3. Comme ces groupes ont des éléments deux à deux du même ordre ils sont isomorphes."