Groupes

Exercice 11.

Il suffirait pour conclure d'écrire G comme une union de certains de ses sous-groupes finis...

Exercice 19.

1. Trouver n éléments engendrant $\mathbb{Z}^n$. Ensuite, à l'aide de ces éléments, expliquer comment une « quantité d'information finie » permet de connaître entièrement un morphisme de groupes $\varphi : \mathbb{Z}^n \to F$.
3. Montrer que $|\mathrm{Hom}(G, F)|$ est un *invariant d'isomorphisme*, c'est-à-dire que si G_1 et G_2 sont deux groupes isomorphes, alors $|\mathrm{Hom}(G_1, F)| = |\mathrm{Hom}(G_2, F)|$.

Exercice 24.

1. Pour la première question, on utilisera le théorème de Lagrange.
2. La première question traite tous les cardinaux sauf $n = 4$ et $n = 6$ mais, même dans ce cas, le théorème de Lagrange donne des contraintes.

   Dans le cas $n = 6$, on pourra par exemple montrer que si le groupe n'est pas cyclique, il existe un élément x d'ordre 3 et un élément y d'ordre 2 qui ne commutent pas. Dans ce cas, que vaut yxy^{-1} ?

Exercice 31.

Pour la première question, on pourra montrer que $\forall g \in G, A \cap \left\{ gb^{-1} \,\middle|\, b \in B \right\} \neq \varnothing$.

Exercice 32.

1. On notera que le théorème de Lagrange montre l'inégalité avec 4 remplacé par 2. Il s'agit donc d'améliorer un peu l'argument.
2. La première question et le théorème de Lagrange montrent qu'au moins trois quarts des éléments de G ne commute qu'avec une minorité (au sens large) des éléments de G...

Exercice 38.

On pourra montrer que si $f, g \in G$, alors le *commutateur* $f \circ g \circ f^{-1} \circ g^{-1}$ est une translation.

Autocorrection

Autocorrection A.

- Avant toute chose, il faut montrer que $\cdot$ reste une loi de composition interne sur $M^\times$, c'est-à-dire que $M^\times$ est stable par $\cdot$.

  Soit $x_1, x_2 \in M^\times$. On peut donc trouver $y_1, y_2 \in M$ tels que $x_1 y_1 = y_1 x_1 = x_2 y_2 = y_2 x_2 = 1_M$.

On a alors

$$(x_1x_2)(y_2y_1) = x_1 \underbrace{x_2y_2}_{=1_M} y_1 = x_1y_1 = 1_M$$
$$(y_2y_1)(x_1x_2) = y_2 \underbrace{y_1x_1}_{=1_M} x_2 = y_2x_2 = 1_M.$$

- Par ailleurs, l'associativité de $\cdot$:

  $$\forall x, y, z \in M, x(yz) = (xy)z$$

  donne *a fortiori*

  $$\forall x, y, z \in M^\times, x(yz) = (xy)z,$$

  ce qui montre l'associativité de $(M^\times, \cdot)$.
- On a $1_M1_M = 1_M$, donc $1_M \in M^\times$. Là encore, le fait que 1_M soit l'élément neutre de $(M, \cdot)$:

  $$\forall x \in M, 1_M\, x = x\, 1_M = x$$

  donne *a fortiori*

  $$\forall x \in M^\times, 1_M\, x = x\, 1_M = x,$$

  c'est-à-dire que 1_M est un élément neutre dans $(M^\times, \cdot)$.
- Enfin, montrons la présence d'inverses dans $M^\times$. Soit $x \in M^\times$.
  On peut donc trouver $y \in M$ tel que $xy = yx = 1_M$.
  Ces égalités montrent notamment que $y \in M^\times$.
  On a donc trouvé $y \in M^\times$ tel que $xy = yx = 1_M$, ce qui conclut.

Autocorrection B.

(i) On peut vérifier facilement qu'il s'agit d'un monoïde (dont la chaîne vide est l'élément neutre), et c'est d'ailleurs un exemple fondamental de monoïde.
Cependant, ce n'est pas un groupe : il n'existe par exemple pas de chaîne de caractères χ telle que "a" $+\chi =$ "", pour des raisons de longueur.

(ii) De même, il s'agit d'un monoïde, dont l'élément neutre est la matrice identité I_2.
Cependant, $\forall M \in M_2(\mathbb{Z}), M \times 0 \neq I_2$, ce qui montre que la matrice nulle n'a pas d'inverse, et donc que $(M_2(\mathbb{Z}), \cdot)$ n'est pas un groupe.

(iii)
- Soit $A, B \in SL_2(\mathbb{Z})$.
  - Pour tous $i, j \in [\![1, 2]\!]$, $[AB]_{i,j} = [A]_{i,1}[B]_{1,j} + [A]_{i,2}[B]_{2,j} \in \mathbb{Z}$.
  - On a $\det(AB) = \det(A)\det(B) = 1$.

  Cela montre $AB \in SL_2(\mathbb{Z})$: le produit matriciel est donc une loi de composition interne sur $SL_2(\mathbb{Z})$, et celle-ci est nécessairement associative.
- La matrice I_2 appartient clairement à $SL_2(\mathbb{Z})$, et est élément neutre pour la multiplication.
- Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. On a alors $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in SL_2(\mathbb{Z})$, donc

  $$\forall M \in SL_2(\mathbb{Z}), \exists N \in SL_2(\mathbb{Z}) : MN = NM = I_2.$$

  Tout cela montre que $SL_2(\mathbb{Z})$ est un groupe multiplicatif.

- ▶ Les calculs $\begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -2 \\ 1/2 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix} = \begin{pmatrix} 0 & -1/2 \\ 2 & 0 \end{pmatrix}$ montrent par exemple que $\mathrm{SL}_2(\mathbb{Z})$ n'est pas abélien.

(iv) ▶ Il s'agit d'une partie de $\mathrm{GL}_2(\mathbb{R})$, donc il suffit de montrer que cela en est un sous-groupe. Comme la partie est clairement non vide, il suffit même de montrer qu'elle est stable par l'opération $(M, N) \mapsto MN^{-1}$.

Or, si $M = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ et $N = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$, on a $N^{-1} = \begin{pmatrix} 1 & -y \\ 0 & 1 \end{pmatrix}$, donc

$$MN^{-1} = \begin{pmatrix} 1 & x-y \\ 0 & 1 \end{pmatrix}.$$

Cela conclut.

- ▶ On a $\forall x, y \in \mathbb{R}$, $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$, ce qui montre que le groupe est commutatif (essentiellement, cette formule montre même que le groupe est isomorphe à $\mathbb{R}$).

(v) Le magma $(\mathbb{R}, \vee)$ ne possède pas d'élément neutre.
En effet, quel que soit $x \in \mathbb{R}$, on a $x \vee (x-1) = x \neq x-1$, donc x n'est pas neutre.
Ce n'est donc pas un groupe (l'associativité est vérifiée, et la présence d'inverse n'a pas de sens en l'absence d'élément neutre).

(vi) On va montrer que $\mathbb{U}_\infty$ est un sous-groupe multiplicatif de $\mathbb{C}^*$ (à ce titre, il héritera de la commutativité du produit des complexes et sera donc abélien).
Encore une fois, comme $\mathbb{U}_\infty$ n'est pas vide, il suffit de vérifier que cet ensemble est stable par l'opération $(x, y) \mapsto xy^{-1}$.
Soit donc $x, y \in \mathbb{U}_\infty$. On peut donc trouver $n, m \in \mathbb{N}^*$ tels que $x^n = y^m = 1$.
On a alors

$$(xy^{-1})^{nm} = x^{nm}y^{-nm} = (x^n)^m(y^m)^{-n} = 1^m 1^{-n} = 1,$$

ce qui montre $xy^{-1} \in \mathbb{U}_\infty$, et conclut.

Autocorrection C.

- ▶ Montrons déjà que $\bigcup_{n\in\mathbb{N}} H_n$ est stable par produit : soit $x_0, x_1 \in \bigcup_{n\in\mathbb{N}} H_n$.
On peut donc trouver $n_0, n_1 \in \mathbb{N}$ tels que $x_0 \in H_{n_0}$ et $x_{n_1} \in H_{n_1}$.
Posons $N = \max(n_0, n_1)$. Par croissance de la suite $(H_n)_{n\in\mathbb{N}}$, on a donc $x_0, x_1 \in H_N$.
Comme H_N est un sous-groupe de G, on en déduit $x_0x_1 \in H_N$ et donc $x_0x_1 \in \bigcup_{n\in\mathbb{N}} H_n$.

- ▶ On a $1_G \in H_0$ (car H_0 est un sous-groupe de G), donc $1_G \in \bigcup_{n\in\mathbb{N}} H_n$.

- ▶ Montrons maintenant que $\bigcup_{n\in\mathbb{N}} H_n$ est stable par inversion : soit $x \in \bigcup_{n\in\mathbb{N}} H_n$.
On peut donc trouver $n_0 \in \mathbb{N}$ tel que $x \in H_{n_0}$.
Comme H_{n_0} est un sous-groupe de G, on en déduit $x^{-1} \in H_{n_0}$ et donc $x \in \bigcup_{n\in\mathbb{N}} H_n$.

Ces trois points montrent que $\bigcup_{n\in\mathbb{N}} H_n$ est un sous-groupe de G.

Autocorrection D.

1. (a) ▶ Clairement, $1_G\, g = g\, 1_G = g$, donc $1_G \in C_G(g)$.
   ▶ Soit $x, y \in C_G(g)$. On a alors $gxy = xgy = xyg$, donc $xy \in C_G(g)$.
   ▶ Soit enfin $x \in G$. On a alors $gx = xg$.
   En multipliant à gauche et à droite par x^{-1}, on obtient $x^{-1}g = gx^{-1}$, donc $x^{-1} \in C_G(g)$.
   Cela montre $x^{-1} \in C_G(g)$.

   (b) **Inclusion directe.** Soit $y \in \varphi[C_G(g)]$. On peut donc trouver $x \in C_G(g)$ tel que $y = \varphi(x)$. On a alors
   $$y\varphi(g) = \varphi(x)\varphi(g) = \varphi(xg) = \varphi(xg) = \varphi(x)\varphi(g) = y\varphi(g),$$
   ce qui montre $y \in C_G(\varphi(g))$.

   Inclusion réciproque. Soit $y \in C_G(\varphi(g))$. On a alors
   $$\varphi^{-1}(y)g = \varphi^{-1}(y)\varphi^{-1}(\varphi(g)) = \varphi^{-1}(y\varphi(g)) = \varphi^{-1}(\varphi(g)y) = \varphi^{-1}(\varphi(g))\varphi^{-1}(y) = g\varphi^{-1}(y),$$
   donc $\varphi^{-1}(y) \in C_G(g)$. On a donc $y = \varphi(\varphi^{-1}(y)) \in \varphi[C_G(g)]$.
   Cela conclut.

2. (a) On peut le montrer « à la main », comme dans la question précédente, mais il est possible d'utiliser la première question.
   En effet, un élément $h \in G$ appartient au centre $Z(G)$ si et seulement s'il commute avec tous les éléments de G. Cela montre
   $$Z(G) = \bigcap_{g \in G} C_G(g).$$
   Intersection de sous-groupes, $Z(G)$ est donc lui-même un sous-groupe de G.

   (b) Il est ici plus commode de donner une démonstration « à la main » (notamment parce que l'on n'a pas en général égalité entre $\bigcap_{i\in I} f[X_i]$ et $f\left[\bigcap_{i\in I} X_i\right]$, même si on peut montrer que cela est vrai quand l'application f est surjective, ce qui serait utile ici).

   Inclusion directe. Soit $y \in \varphi[Z(G)]$. On peut donc trouver $x \in Z(G)$ tel que $y = \varphi(x)$.
   Soit $g \in G$. Comme φ est surjective, on peut trouver $\widetilde{g} \in G$ tel que $g = \varphi(\widetilde{g})$. On a alors
   $$y\, g = \varphi(x)\, \varphi(\widetilde{g}) = \varphi(x\, \widetilde{g}) = \varphi(\widetilde{g}\, x) = \varphi(\widetilde{g})\, \varphi(x) = g\, y,$$
   ce qui montre $y \in Z(G)$.

   Inclusion réciproque. Soit $y \in Z(G)$. Comme φ est un automorphisme, on peut écrire $y = \varphi(\varphi^{-1}(y))$.
   En appliquant le premier point à l'automorphisme φ^{-1}, on obtient que $\varphi^{-1}(y) \in Z(G)$, et on en tire $y = \varphi(\varphi^{-1}(y)) \in \varphi[Z(G)]$, ce qui conclut.

Autocorrection E.

On va montrer qu'il s'agit de $\mathbb{U}_{12}$.

- Déjà, $i^{12} = j^{12} = 1$, donc $i, j \in \mathbb{U}_{12}$.
  Le sous-groupe engendré étant le plus petit sous-groupe de $\mathbb{C}^*$ contenant i et j, on a $\langle i, j\rangle \subseteq \mathbb{U}_{12}$.
- Réciproquement, on vérifie facilement que

$$\zeta_{12} = \exp\left(i\,2\pi\,\frac{1}{12}\right) = \exp\left(i\,2\pi\,\left(\frac{1}{3} - \frac{1}{4}\right)\right) = \exp\left(i\,2\pi\,\frac{1}{3}\right)\exp\left(i\,2\pi\,\frac{1}{4}\right)^{-1} = j\,i^{-1} \in \langle i, j\rangle.$$

  Le sous-groupe $\langle i, j\rangle$ va alors contenir toutes les puissances de ζ_{12}, ce qui montre l'inclusion réciproque $\mathbb{U}_{12} = \langle\zeta_{12}\rangle \subseteq \mathbb{C}^*$.

Autocorrection F.

1. Par les règles sur les puissances, on a, pour tout $k \in \mathbb{Z}$, $\left(x^{-1}\right)^k = x^{-k} = \left(x^k\right)^{-1}$.

   En particulier, pour tout $k \in \mathbb{Z}$, x^k et $\left(x^{-1}\right)^k$ sont inverses l'un de l'autre, ce qui montre notamment que l'un est égal à l'élément neutre si et seulement si l'autre l'est.
   Cela montre que l'un est d'ordre fini si et seulement si l'autre l'est, et que, dans ce cas, les ordres sont les mêmes.
2. De même, on a $\forall k \in \mathbb{Z}$, $\left(yxy^{-1}\right)^k = yx^ky^{-1}$.

   Pour tout $k \in \mathbb{Z}$, les éléments x^k et $\left(yxy^{-1}\right)^k$ sont conjugués, donc l'un est l'élément neutre si et seulement si l'autre l'est.
   On conclut alors de la même façon.
3. Il suffit de remarquer que $yx = y(xy)y^{-1}$ et d'appliquer la question précédente !