Exercices résolus sur les groupes

Exercice 1. Soit E une partie non vide de $\mathbb{R}$. Pour $x, y \in E$, on pose $x * y = \frac{x+y+|x-y|}{2}$. Montrer que $*$ définit une loi de composition interne sur E et étudier ses propriétés.

Solution. Remarquons que si $x \geq y$, alors $x*y = x$ et si $x \leq y$, alors $x*y = y$. Par conséquent $x*y = \sup(x, y)$.

Commutativité. $\forall x, y \in E$, $x * y = \sup(x, y) = \sup(y, x) = y * x$. La loi $*$ est donc commutative.

Associativité. $\forall x, y, z \in E$, on a :$(x * y) * z = \sup(\sup(x, y), z) = \sup(x, y, z) = \sup(x, \sup(y, z)) = x * (y * z)$. La loi $*$ est donc associative.

Elément neutre. Pour que $*$ admette un élément neutre, il faut qu'il existe $e \in E$, tel que $x * e = x$, $\forall x \in E$, i.e. $x \geq e$ $\forall x \in E$. Ce qui veut dire que e doit être le plus petit élément de E. Cette condition n'est pas toujours vérifiée c'est le cas par exemple si $E = \mathbb{R}$.

Eléments réguliers. Soit $a \in E$, alors a est régulier si $a * x = a * y \Rightarrow x = y$, $\forall x, y \in E$. En prenant $x < a$ et $y = a$, on a $a * x = a = a * a$, mais $x \neq a$. Donc dans ce cas là, a n'est pas régulier. Par conséquent, pour que a soit régulier, il faut que $a \leq x$, $\forall x \in E$, i.e. a doit être l'élément neutre de $*$.

Eléments symétrisables. On suppose que E possède un élément neutre e. Puisque $(E, *)$ est un monoïde, tout élément symétrisable es régulier. Comme e est le seul élément régulier de $(E, *)$, il en découle que e est le seul élément symétrisable.

Exercice 2. Sur $E = \mathbb{Q}^2$, on défini la loi $\perp$ par : $(a, b) \perp (a', b') = (aa', ba' + b')$. Citer les propriétés de cette loi. On étudiera en particulier les éléments symétrisables.

Solution.
Associativité. Soient $(a, b), (a', b'), (a'', b'') \in E$. On a :
$((a, b) \perp (a', b')) \perp (a'', b'') = (aa', ba' + b') \perp (a'', b'') = (aa'a'', (ba' + b')a'' + b'') = (aa'a'', ba'a'' + b'a'' + b'')$.
$(a, b) \perp ((a', b') \perp (a'', b'')) = (a, b) \perp (a'a'', b'a'' + b'') = (aa'a'', ba'a'' + b'a'' + b'')$.
Donc $((a, b) \perp (a', b')) \perp (a'', b'') = (a, b) \perp ((a', b') \perp (a'', b''))$, par conséquent, $\perp$ est associative.

Commutativité. On a $(a, b) \perp (a', b') = (aa', ba' + b')$ et $(a', b') \perp (a, b) = (a'a, b'a + b)$. Il est facile de voir que la loi $\perp$ n'est pas commutative. En effet, $(1, 1) \perp (0, 1) = (0, 1)$ alors que $(0.1) \perp (1, 1) = (0, 2)$.

Elément neutre. Soit $(e, e') \in E$ tel que $\forall (a, b) \in E$, on a : $(a, b) \perp (e, e') = (e, e') \perp (a, b) = (a, b)$. Alors $ae = ea = a$ et $be + e' = e'a + b = b$, $\forall a, b \in \mathbb{Q}$. Ainsi $e = 1$ et $e' = 0$. On vérifie ensuite que $(a, b) \perp (1, 0) = (1, 0) \perp (a, b) = (a, b)$. Donc $\perp$ possède un élément neutre qui est $(1, 0)$.

En conclusion $(E, \perp)$ est un monoïde non commutatif.

Eléments symétrisables. Soit $(a, b) \in E$ un élément symétrisable. Il existe alors $(a', b') \in E$ tel que $(a, b) \perp (a', b') = (a', b') \perp (a, b) = (1, 0)$. Par conséquent, $aa' = a'a = 1$ et $ba' + b' = b'a + b = 0$. Il en résulte que $a \neq 0$, $a' = a^{-1}$ et $b' = -b.a^{-1}$. Réciproquement, si $a \neq 0$, alors $(a, b) \perp (a^{-1}, -b.a^{-1}) = (a^{-1}, -b.a^{-1}) \perp (a, b) = (1, 0)$. En conclusion, (a, b) est symétrisable, si et seulement si, $a \neq 0$ et on a alors $(a, b)^{-1} = (a^{-1}, -b.a^{-1})$.

Eléments réguliers. Les éléments symétrisables sont réguliers.
Réciproquement, si (a, b) n'est pas symétrisable, on a $a = 0$ et $(a, b) = (0, b)$. Par ailleurs $(0, b) \perp (1, -b) = (0, 0) = (0, b) \perp (0, 0)$, alors que $(1, -b) \neq (0, 0)$. Ce qui veut dire que $(0, b)$ n'est pas régulier. Donc dans ce monoïde, nous avons tout élément régulier est symétrisable.

Exercice 3.
1 - Montrer que $\mathbb{Z}$ est un monoïde pour la loi $*$ définie par :

$$x * y = x + y - xy$$

2 - Trouver les éléments inversibles de $(\mathbb{Z}, *)$.
3 - Calculer pour la loi $*$, les puissances d'un élément $a \in \mathbb{Z}$.

Solution. 1 - *Associativité.* Soient $x, y, z \in \mathbb{Z}$, on a :
$(x * y) * z = (x + y - xy) * z = x + y - xy + z - xz - yz + xyz$ et
$x * (y * z) = x * (y + z - yz) = x + y + z - yz - xy - xz + xyz$. Donc $(x * y) * z = x * (y * z)$. $*$ est associative.
Commutativité. $\forall x, y \in \mathbb{Z}$, $x * y = x + y - xy = y + x - yx = y * x$. $*$ est commutative.
Elément neutre. Soit e tel que $x * e = x$, $\forall x \in \mathbb{Z}$. On a $x + e - ex = x$. Donc $ex = 0$, par suite $e = 0$. On vérifie alors que $x * 0 = 0 * x = x$. Ainsi 0 est l'élément neutre de $*$.
En conclusion, $(\mathbb{Z}, *)$ est un monoïde commutatif.
2 - Un élément x de $\mathbb{Z}$ est inversible pour $*$, s'il existe $x' \in \mathbb{Z}$ tel que $x * x' = x + x' - xx' = 0$. Ou encore, $1 - (1 - x)(1 - x') = 0$. Ce qui implique que $(1 - x)(1 - x') = 1$. Par conséquent $1 - x = 1$ ou $1 - x = -1$, $\Rightarrow x = 0$ ou $x = 2$. Les éléments inversibles de $(\mathbb{Z}, *)$ sont 0 et 2.
3 - En remarquant que $x*y = 1-(1-x)(1-y)$, montrons par récurrence que $x^{*n} = 1-(1-x)^n$. C'est vrai pour $n = 0$, $x^{*0} = 0$. Supposons la propriété vraie pour n. On a $x^{*(n+1)} = x*x^{*n} = 1-(1-x)(1-x)^n = 1-(1-x)^{n+1}$.

Exercice 4. Soit $(E, +)$ un monoïde commutatif d'élément neutre noté 0, dans lequel tout élément est régulier. Sur le monoïde produit $E \times E$, on définit une relation binaire $\mathcal{R}$ par :

$$\forall (x, y), (x', y') \in E \times E,\ (x, y)\mathcal{R}(x', y') \Leftrightarrow x + y' = y + x'$$

1 - Montrer que $\mathcal{R}$ est une relation d'équivalence compatible avec la loi de $E \times E$.
2 - On note $\overline{E}$ l'ensemble quotient $E \times E/\mathcal{R}$ et $\overline{+}$ la loi quotient définie sur $\overline{E}$. Montrer que $(\overline{E}, \overline{+})$ est un groupe abélien.
3 - Soit l'application $\phi : E \to \overline{E}$, définie par $\phi(x) = \overline{(x, 0)}$.
a - Montrer que ϕ est un morphisme injectif de monoïdes.
b - Soit G un groupe quelconque et $f : E \to G$ un morphisme de monoïdes. Montrer qu'il existe un morphisme de groupes $\overline{f} : \overline{E} \to G$ unique tel que $\overline{f} \circ \phi = f$.

Solution.
1 - *Reflexivité.* On a $x + y = y + x$ car $+$ est commutative. Donc $(x, y)\mathcal{R}(x, y)$, $\mathcal{R}$ est relexive.
Symétrie. Si $(x, y)\mathcal{R}(x', y')$, alors $x+y' = y+x'$. Par suite on a $x' + y = y' + x$, car le monoïde E est commutatif. D'où $(x', y')\mathcal{R}(x, y)$. $\mathcal{R}$ est symétrique.
Transitivité. Soient $(x, y), (x', y'), (x'', y'')$ dans $E \times E$. Si $(x, y)\mathcal{R}(x', y')$ et $(x', y')\mathcal{R}(x'', y'')$, alors $x' + y = y' + x$ et $x'' + y' = y'' + x'$. Donc $x' + y + x'' + y' = y' + x + y'' + x'$. Dans le monoïde E tout élément est régulier, donc on peut simplifier par x' et y'. Il en résulte que $y + x'' = y'' + x$. D'où $(x, y)\mathcal{R}(x'', y'')$. $\mathcal{R}$ est transitive.

En conclusion, $\mathcal{R}$ est une relation d'équivalence.

Compatibilité. Soient $(x, y), (x', y'), (a, b), (a', b')$ dans $E \times E$, tels que $(x, y)\mathcal{R}(x', y')$ et $(a, b)\mathcal{R}(a', b')$. On a $x + y' = y + x'$ et $a + b' = b + a'$. Donc $x + y' + a + b' = y + x' + b + a'$, ou encore $x + a + y' + b' = y + b + x' + a'$. Ceci exprime que $(x, y) + (a, b)\mathcal{R}(x', y') + (a', b')$. C'est la compatibilité de $\mathcal{R}$ avec la loi produit sur $E \times E$.

2 - D'après le cours, $(\overline{E}, \overline{+})$ est un monoïde commutatif d'élément neutre $\overline{(0, 0)}$ (l'associativité, la commutativité et l'élément neutre "passent" au quotient). Montrons que $(\overline{E}, \overline{+})$ est un groupe. Soit $\overline{(x, y)} \in \overline{E}$. On cherche $\overline{(a, b)}$ tel que $(x, y) + (a, b) = (x + a, y + b)\mathcal{R}(0, 0)$. i.e. $x + a = y + b$. Il suffit de prendre $a = y$ et $b = x$. Ainsi $\overline{(x, y)}\overline{+}\overline{(y, x)} = \overline{(x + y, x + y)} = \overline{(0, 0)}$
3 - a - $\phi(a + b) = \overline{(a + b, 0)} = \overline{(a, 0)}\overline{+}\overline{(b, 0)} = \phi(a)\overline{+}\phi(b)$.
D'autre part, on a $\phi(0) = \overline{(0, 0)}$. Donc ϕ est un morphisme de monoïdes.
Soit $a, b \in E$ tels que $\phi(a) = \phi(b)$. On a alors $\overline{(a, 0)} = \overline{(b, 0)}$. Donc $a = b$. ϕ est injectif.
b - Soit G un groupe quelconque et $f : E \to G$ un morphisme de monoïdes. Posons $\overline{f}(\overline{(x, y)}) = f(x)f(y)^{-1}$.
On montre que $\overline{f}$ ne dépend pas des représentants de la classe $\overline{(x, y)}$. En effet, si $\overline{(a, b)} = \overline{(x, y)}$, on a $a+y = x+b$. On applique f on obtient $f(a)f(y) = f(x)f(b)$. D'où $f(a)f(b)^{-1} = f(x)f(y)^{-1}$.

Montrons ensuite que $\overline{f}$ est un morphisme de groupes. Soient $\overline{(x, y)}, \overline{(x', y')} \in \overline{E}$. On a $\overline{f}(\overline{(x, y)} + \overline{(x', y')}) = \overline{f}(\overline{(x + x', y + y')}) = f(x + x')f(y + y')^{-1} = f(x)f(x')(f(y)f(y'))^{-1}$. Puisque $(\overline{E}, \overline{+})$ est abélien, on a : $\overline{f}(\overline{(x, y)} + \overline{(x', y')}) = f(x)f(y)^{-1}f(x')f(y')^{-1} = \overline{f}(\overline{(x, y)}) + \overline{f}(\overline{(x', y')})$.

Unicité de $\overline{f}$. Si $\overline{g} : \overline{E} \to G$ est un autre morphisme de groupes tel que $\overline{g} \circ \phi = f$, alors $\overline{g}(\overline{(x, y)}) = \overline{g}(\overline{(x, 0)}\overline{+}\overline{(0, y)}) = \overline{g}(\overline{(x, 0)}\overline{+}(-\overline{(y, 0)})) = (\overline{g} \circ \phi(x))(\overline{g} \circ \phi(y))^{-1} = f(x)f(y)^{-1} = \overline{f}(\overline{(x, y)})$. Donc $\overline{g} = \overline{f}$.

Commentaire. Ce procédé permet par exemple de construire le groupe $(\mathbb{Z}, +)$ à partir du monoïde $(\mathbb{N}, +)$.

Exercice 5. Dire si les ensembles suivants sont des monoïdes pour la multiplication des entiers.
1 - $E = \{x = a^2 + b^2 \in \mathbb{N} : a, b \in \mathbb{N}\}$.
2 - $F = \{x = a^2 + b^2 + c^2 \in \mathbb{N} : a, b, c \in \mathbb{N}\}$.

Solution.
1 - Soient $a, b, c, d \in \mathbb{N}$, on a : $(a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 = a^2c^2 + b^2d^2 + 2abcd + a^2d^2 + b^2c^2 - 2abcd = (ac + bd)^2 + (ad - bc)^2$.
On a $ac + bd, ad - bc \in \mathbb{N}$, donc $(a^2 + b^2)(c^2 + d^2) \in E$. E est stable par multiplication. Par ailleurs on a, $1 = 1^2 + 0^2$. Donc $1 \in E$. Puisque la multiplication des entiers est associative, $(E, .)$ est un monoïde.
2 - Nous allons montrer que F n'est pas stable par multiplication. On a $3 = 1^2 + 1^2 + 1^2$ et $5 = 2^2 + 1^2 + 0^2$. Donc 3 et $5 \in F$. Montrons que $15 = 3 \times 5$ n'est pas un élément de F. Sinon, $15 = a^2 + b^2 + c^2$. Nécessairement $a, b, c \leq 3$. D'autre part, un des entiers a, b, c est supérieur strictement à 2. Il en résulte qu'un des entiers, par exemple a, est égal à 3. On a alors $15 = 9 + b^2 + c^2$. Ce qui entraîne que $b^2 + c^2 = 6$. Ce qui est absurde. Donc $15 \notin F$.

Exercice 6. Soit X un ensemble non vide. On considère $(\mathcal{F}(X), \circ)$, le monoïde des applications de X dans lui-même. Soit $f \in \mathcal{F}(X)$. Montrer que :
1 - f est régulière à gauche $\Leftrightarrow$ f est injective $\Leftrightarrow$ f est inversible à gauche.
2 - f est régulière à droite $\Leftrightarrow$ f est surjective $\Leftrightarrow$ f est inversible à droite.
3 - f est bijective $\Leftrightarrow$ f est régulière $\Leftrightarrow$ f est inversible.

Solution.
1 - *f régulière à gauche $\Rightarrow$ f injective.* Supposons que f est régulière à gauche, soient $y, y' \in X$ tels que $f(y) = f(y')$. Montrons que $y = y'$. Considérons les applications constantes $g, h \in \mathcal{F}(X)$, telles que $\forall x \in X,\ g(x) = y$ et $h(x) = y'$. On a $\forall x \in X$. $f \circ g(x) = f(g(x)) = f(y) = f(y') = f(h(x)) = f \circ h(x)$. Donc $f \circ g = f \circ h$. Comme f est régulière à gauche, $g = h$. Donc $y = y'$. Par conséquent f est injective.

f injective $\Rightarrow$ f inversible à gauche. Supposons que f est injective. Pour tout $y \in x$, $f^{-1}\{y\}$ est un singleton ou vide. Fixons $a \in X$ et définissons $g \in \mathcal{F}(X)$ par : $g(y) = x$ si $f^{-1}\{y\} = \{x\}$, $g(y) = a$, si $f^{-1}\{y\} = \varnothing$. Alors $\forall x \in X$, on a : $g \circ f(x) = x, \forall x \in X$. Donc $g \circ f = I_X$.

f inversible à gauche $\Rightarrow$ f régulière à gauche. Cette implication est vraie dans tout monoïde.

2 - *f régulière à droite $\Rightarrow$ f surjective.* Par contraposition, supposons que f ne soit pas surjective. Il existe $y \in X$ tel que $y \notin f(X)$. Soient $a, b \in X$, $a \neq b$. On considère $g, h \in \mathcal{F}(X)$ définies par : g est l'application constante $g(x) = a$, $\forall x \in X$, h est définie par $h(x) = a$ si $x \in f(X)$, $h(x) = b$ sinon. On a $g \circ f(x) = h \circ f(x) = a$, $\forall x \in X$, mais $g \neq h$. Donc f n'est pas régulière à droite.

f surjective $\Rightarrow$ f inversible à droite. Supposons que f est surjective. Alors $\forall y \in X$, on a $f^{-1}\{y\}$ est non vide. Les ensembles $f^{-1}\{y\}$ forment une partition de X, on "choisit" dans chaque $f^{-1}\{y\}$ un élément z. On définit ainsi une application par $z = g(y)$. Alors $f \circ g = I_X$.
L'implication *f inversible à droite $\Rightarrow$ f régulière à droite* est vraie dans tout monoïde.
3 - Les équivalences f est bijective $\Leftrightarrow$ f est régulière $\Leftrightarrow$ f est inversible, sont une conséquence de 2 et 3.

Exercice 7.
1 - Soit n un entier naturel non nul. On note $\mathbb{U}_n$ le groupe des éléments inversibles du monoïde $(\mathbb{Z}/n\mathbb{Z}, \cdot)$. Pour $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$, montrer l'équivalence des assertions suivantes.
(i) $\bar{k} \in \mathbb{U}_n$.
(ii) k est premier avec n.
(iii) $\bar{k}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
On note $\phi(n)$ l'ordre du groupe $\mathbb{U}_n$. $\phi(n)$ est appelé l'indicateur d'Euler de n.
D'après le résultat précédent, $\phi(n) = card\{k : 1 \leq k \leq n,\ \text{et } k \wedge n = 1\}$
2 - Soit p un nombre premier et s un entier natuel non nul. Montrer que $\phi(p^s) = p^s - p^{s-1}$.
3 - Soient m et n deux entiers premiers entre eux. Montrer que l'application

$$\begin{array}{rcl} f : \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \bar{x}[mn] & \mapsto & (\bar{x}[m], \bar{x}[n]) \end{array}$$

est un isomorphisme des monoïdes multiplicatifs. (ici $\bar{x}[k]$ désigne la classe de x modulo k).
4 - Déduire de la question 3, que $card(\mathbb{U}_{mn}) = card(\mathbb{U}_m \times \mathbb{U}_n)$ et que $\phi(mn) = \phi(m)\phi(n)$.

5 - Soit $n = p_1^{k_1} \cdots p_s^{k_s}$ la factorisation de n en produit de nombres premiers p_i. Donner l'expression de $\phi(n)$ à l'aide des p_i et des k_i.

Solution.
1 - $(i) \Rightarrow (ii)$ Supposons que $\bar{k} \in \mathbb{U}_n$, il existe $m \in \mathbb{Z}$, tel que $\bar{k}\bar{m} = \bar{1}$. Donc $n \mid km - 1$, par conséquent, il existe $s \in \mathbb{Z}$, tel que $km - 1 = sn$, ou encore $km - sn = 1$, i.e. k et m sont premiers entre eux.
$(ii) \Rightarrow (iii)$. Supposons que $k \wedge n = 1$, d'après Bezout, il existe $m, s \in \mathbb{Z}$, tels que $km + sn = 1$. Donc $m\bar{k} = \bar{1}$. D'où, $\forall t \in \mathbb{Z}$, $\bar{t} = tm\bar{k}$, i.e. $\bar{k}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
$(iii) \Rightarrow (i)$. Supposons que $\bar{k}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$. En particulier, il existe $m \in \mathbb{Z}$, tel que $m\bar{k} = 1$. D'où $\bar{m}\bar{k} = \bar{1}$. i.e. $\bar{k}$ est inversible.
2 - D'après la question 1, pour déterminer $\phi(p^s)$, on calcule le nombre d'entiers k tels que $1 \leq k < p^s$ qui sont premiers avec p^s. Posons $E = \{1, 2, \ldots, p^s\}$, $F = \{k \in E : p \mid k\}$. On a $\phi(p^s) = card(E) - card(F) = p^s - card(F)$. Or $F = \{p, 2p, 3p, \ldots, p^s = p^{s-1}p\}$, donc $\text{card}(F) = p^{s-1}$. On en déduit que $\phi(p^s) = p^s - p^{s-1}$.
3 - Soient m et n deux entiers premiers entre eux. On considère l'application

$$\begin{array}{rcl} f : \mathbb{Z}/mn\mathbb{Z} & \rightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \bar{x}[mn] & \mapsto & (\bar{x}[m], \bar{x}[n]) \end{array}$$

Montrons d'abord que f est bien définie. Si $\bar{x}[mn] = \bar{y}[mn]$, alors $mn \mid x - y$. Comme m et n sont premiers entre eux, on a $m \mid x - y$ et $n \mid x - y$. Ou encore $\bar{x}[m] = \bar{y}[m]$ et $\bar{x}[n] = \bar{y}[n]$.
Montrons que f est un morphisme de monoïdes. $f(\bar{x}\bar{y}[mn]) = (\overline{xy}[m], \overline{xy}[n]) == (\bar{x}[m], \bar{x}[n])(\bar{y}[m], \bar{y}[n]) = f(\bar{x}[mn])f(\bar{y}[mn])$.
Montrons que f est injectif. Si $(\bar{x}[m], \bar{x}[n]) = (\bar{y}[m], \bar{y}[n])$, alors $m \mid x - y$ et $n \mid x - y$. Comme m et n sont premiers entre-eux, $mn \mid x - y$, ou encore $\bar{x}[mn] = \bar{y}[mn]$ 4 - Puisque f est un isomorphisme, on a $\bar{x} \in \mathbb{U}_{mn} \Leftrightarrow f(\bar{x}) \in \mathbb{U}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} = \mathbb{U}_m \times \mathbb{U}_n$ Par conséquent, $\phi(mn) = card(U_{mn} = card(U_m \times \mathbb{U}_n) = card(U_m)(\mathbb{U}_n) = \phi(m)\phi(n)$.
5 - Soit $n = p_1^{k_1} \cdots p_s^{k_s}$. Par récurrence, on montre que $\phi(n) = \prod_{i=1}^{s} \phi(p_i^{k_i}) = \prod_{i=1}^{s} (p_i^{k_i} - p_i^{k_i - 1})$.

Exercice 8. Soit $G_n = \{z \in \mathbb{C} \mid z^n = 1\}$.
1 - Montrer que G_n est un sous-groupe cyclique de $(\mathbb{C}^*, \cdot)$.
2 - Réciproquement, soit G un sous-groupe fini d'ordre n de $(\mathbb{C}^*, \cdot)$. Montrer que $G = G_n$ et que par conséquent G est cyclique.

Solution.
1 - D'abord on montre que G_n est un sous-groupe de $(\mathbb{C}^*, \times)$. On a $1 \in G_n$. Soient $u, v \in G_n$, on a $(uv^{-1})^n = u^n(v^n)^{-1} = 1$. Donc $uv^{-1} \in G_n$.
Tout élément de G_n est de la forme $z = exp(\frac{2k\pi i}{n}) = exp(\frac{2\pi i}{n})^k$. Donc $G_n = gr\langle\xi\rangle = \{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$, où $\xi = exp(\frac{2\pi i}{n})$.
Soit G un sous-groupe fini d'ordre n de $(\mathbb{C}^*, \times)$. D'après le théorème de lagrange, $\forall z \in G$, on a $z^n = 1$, donc $G \subset G_n$. Comme $|G| = |G_n|$, on a $G = G_n$.

Exercice 9. Soit $z = a + ib \in \mathbb{C}$, où $a, b \in \mathbb{R}$. On pose $\exp(z) = e^a(\cos b + i \sin b)$. Montrer que l'application $f : (\mathbb{C}, +) \rightarrow (\mathbb{C}^*, \times)$, définie par $f(z) = \exp(z)$, est un morphisme de groupes. Déterminer son noyau et son image.

Solution. Soient $u, v \in \mathbb{C}$, $u = a + bi$, et $v = c + di$ $a, b, c, d \in \mathbb{R}$. On a :
$\exp(u + v) = \exp(a + c)(\cos(b + d) + i \sin(b + d)) = \exp(a)\exp(c)[\cos(b)\cos(d) - \sin(b)\sin(d) + i \sin(b)\cos(d) + i \sin(d)\cos(b)]$
$\exp(u + v) = \exp(a)(\cos(b) + i \sin(b))\exp(c)(\cos(d) + i \sin(d)) = \exp(u)\exp(v)$.
exp est bien un morphisme $(\mathbb{C}, +) \rightarrow (\mathbb{C}^*, \times)$.
Soit $z = a + bi \in \mathbb{C}$, on a $u \in Kerf \Leftrightarrow \exp(z) = e^a(\cos(b) + i \sin(b) = 1$. Donc $e^a(\cos(b) = 1$ et $e^a(\sin(b) = 0$. Puisque $e^a > 0$, on a $\sin(b) = 0$ et $\cos(b) = 1$. D'où $a = 0$ et $b = 2k\pi$, où $k \in \mathbb{Z}$ est quelconque. D'où $Kerf \subset 2\pi i\mathbb{Z}$. Réciproquement, tout nombre complexe $z = 2k\pi i$, avec $k \in \mathbb{Z}$, vérifie $\exp(z) = 1$. Finalement, $Kerf = 2\pi i\mathbb{Z}$.
Soit $z = a + bi \in Imf$, puisque $z \neq 0$, posons $z = \rho e^{i\theta}$. Il existe $u = c + di$, tel que $\exp(u) = e^c e^{di} = \rho e^{i\theta}$. On a alors $c = \ln(\rho)$ et $d = \theta \pmod{2\pi}$. Il en résulte que z existe (mais n'est pas unique) $\forall u \in \mathbb{C}^*$. par conséquent, f est surjective et $\text{Im}f = \mathbb{C}^*$.

Exercice 10. Soit E un monoïde d'élément neutre e.
1 - Montrer que tout élément inversible à gauche et régulier à droite est inversible.
2 - Donner un exemple d'un monoïde contenant un élément inversible à gauche non inversible à droite.
3 - Montrer que dans un monoïde fini tout élément régulier à gauche ou à droite est inversible.

Solution.
1 - Soit $x \in E$ inversible à gauche et régulier à droite. Il existe $x' \in E$ tel que $x'x = e$. On a $(xx')x = x(x'x) = xe = x = ex$. Puisque x est régulier à droite, on a : $xx' = e$. Donc x est inversible.
2 - En utilisant l'exercice 6, il suffit de considérer $\mathcal{F}(X)$ avec X infini et une application injective non surjective. Par exemple $X = \mathbb{N}$ et $f : \mathbb{N} \to \mathbb{N}$, définie par $f(n) = n + 1$.
3 - On suppose que E est fini et $a \in E$ régulier à droite. Soit l'application $\rho_a : E \to E$, définie par $\rho_a(x) = xa$. Puisque a est régulier à droite, ρ_a est injective. Or E et fini, donc ρ_a est bijective. Il existe $a' \in E$ tel que : $a'a = e$. Donc a est inversible à gauche et régulier à droite. On applique alors 1.

Par la même méthode on démontre que régulier à gauche $\Rightarrow$ inversible.

Autre méthode. On considère l'application $\phi : \mathbb{N} \to E$ définie par $\phi(n) = a^n$. Puisque E et fini, ϕ ne peut pas être injective. Donc il existe $m > n$ tels que $a^n = a^m$. Donc, puisque a est régulier à gauche ou à droite, il en est de même de a^n. Donc $a^{m-n} = e$. Ou encore $a.a^{m-n-1} = a^{m-n-1}.a = e$. Donc a est inversible.

Exercice 11. Soit E l'intervalle ouvert $]-1, 1[$. Pour $x, y \in E$, on pose $x * y = \frac{x+y}{1+xy}$. Montrer que $*$ définit une l.c.i. sur E et que $(E, *)$ est un groupe abélien isomorphe à $(\mathbb{R}, +)$.

Solution.

$*$ *est une l.c.i.* D'abord si $x, y \in E$ on a $-1 < xy < 1$ et $0 < 1 + xy < 2$. D'où $x + y + 1 + xy = (x + 1)(y + 1) > 0$. Donc $\frac{x+y}{1+xy} > -1$. De même $x + y - 1 - xy = (x - 1)(1 - y) < 0$. Donc $\frac{x+y}{1+xy} < 1$. D'où $x * y \in]-1, 1[$.

Associativité . Soient $x, y, z \in E$. On a :

$(x * y) * z = \frac{x+y}{1+xy} * z = \frac{x+y+z+xyz}{1+xy+xz+yz}$.

$x * (y * z) = x * \frac{y+z}{1+yz} = \frac{x+y+z+xyz}{1+yz+xy+xz}$.

Donc $(x * y) * z = x * (y * z)$. La loi $*$ est associative.

Commutativité. On a $x * y = \frac{x+y}{1+xy} = \frac{y+x}{1+yx} = y * x$, $\forall x, y \in E$.
Donc $*$ est commutative.

Elément neutre. On a $x * 0 = 0 * x = x$, donc 0 est l'élément neutre de la loi $*$.

Eléments symétrisables. Pour tout $x \in E$ on a $-x \in E$ et $x * (-x) = (-x) * x = 0$.

En conclusion, $(E, *)$ est un groupe abélien.

On cherche une application bijective $f : \mathbb{R} \to]-1, 1[$, telle que $f(x + y) = f(x) * f(y) = \frac{f(x)+f(y)}{1+f(x)f(y)}$. Une application qui répond à cette propriété est $\mathrm{th}(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$ (la tangente hyperbolique).

Exercice 12. On appelle application affine de $\mathbb{R}$, toute application de la forme $f_{a,b} : \mathbb{R} \to \mathbb{R}$, $x \mapsto ax + b$.
1 - Montrer que l'ensemble $\mathrm{Aff}(\mathbb{R})$, des applications affines est un monoïde pour la composition des applications.
2 - Soit $f_{a,b}$ une application affine. Montrer que $f_{a,b}$ est bijective, si et seulement si, $a \neq 0$. On a alors $f_{a,b}^{-1} = f_{a^{-1},-a^{-1}b}$.
3 - Montrer que l'ensemble des bijections affines, $\mathrm{GA}(\mathbb{R})$, muni de la composition des applications est un groupe.

Solution.
1 - On a $I = f_{1,0}$ est une application affine. Si $f_{a,b}, f_{c,d}$ sont des applications affines, on a : $\forall x \in \mathbb{R}$, $f_{a,b} \circ f_{c,d}(x) = a(cx + d) + b = acx + ad + b = f_{ac,ad+b}(x)$. Donc $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$. $\mathrm{Aff}(\mathbb{R})$ est donc stable par La loi $\circ$ et contient I. La loi $\circ$ étant associative, $(\mathrm{Aff}(\mathbb{R}), \circ)$ est un monoïde.
2 - Soit $f_{a,b}$ une application affine. Si $a \neq 0$, on a, d'après 1, $f_{a,b} \circ f_{a^{-1},-a^{-1}b} = f_{a^{-1},-a^{-1}b} \circ f_{a,b} = f_{1,0} = I$,

donc $f_{a,b}$ est inversible.
Réciproquement, si $a = 0$, on a $f_{0,b}(0) = f_{0,b}(1) = b$, donc $f_{0,b}$ n'est pas bijective.
3 - Puisque la réciproque d'une bijection affine est une bijection affine, $\mathrm{GA}(\mathbb{R})$ est le groupe des éléments inversibles du monoïde $\mathrm{Aff}(\mathbb{R})$.

Exercice 13.
Soit $(E, \cdot)$ un ensemble muni d'une loi de composition interne. Pour tout $a \in E$, on définit les applications $G_a, D_a : E \to E$, par $G_a(x) = ax$ et $D_a(x) = xa$, pour tout $x \in E$.
1 - Montrer que a est régulier à gauche (resp. à droite), si et seulemnt si, G_a (resp.D_a) est injective.
2 - Soit $(E, \cdot)$ un ensemble fini muni d'une loi associative pour laquelle tout élément de E est régulier (à droite et à gauche). Montrer que $(E, \cdot)$ est un groupe.
(Indication : Montrer que pour tout $a \in E$, les applications G_a et D_a sont bijectives).
3 - Soit $(G, \cdot)$ un groupe et H un sous-ensemble fini de G stable par la loi $\cdot$. Montrer que H est un sous-groupe de G.
4 -On reprend la question 2 en supposant seulement la régularité d'un seul côté. Peut-on conclure que $(E, \cdot)$ est un groupe ?

Solution.
1 - Supposons que a est régulier à gauche, soient $x, y \in E$, tels que $G_a(x) = G_a(y)$. Alors $ax = ay$. Comme a est régulier à gauche, on a $x = y$. D'où G_a est injective.
Réciproquement, supposons que G_a est injectve. Soient $x, y \in E$ tels que $ax = ay$. On a $G_a(x) = G_a(y)$, donc $x = y$, puisque G_a est injective.
On a montré que a régulier à gauche, si et seulement si, G_a est injective.
Même démonstration pour l'équivalence a régulier à droite, si et seulement si, D_a est injective.
2 - Nous allons montrer d'abord que $(E, \cdot)$ possède un élément neutre. Soit $a \in E$ fixé. Puisque a est régulier, d'après la question 1, G_a et D_a sont injectives. Comme E est fini, elles sont bijectives. Donc $\exists e \in E$ tel que $ae = G_a(e) = a$. Soit $x \in E$. Comme D_a est bijective, il existe $x' \in E$ tel que $x = x'a$. On a $xe = (x'a)e = x'(ae) = x'a = x$. De même on a $a(ex) = (ae)x = ax$, donc par régularité de a on a $ex = x$. D'où, $\forall x \in E, xe = ex = x$. Par conséquent, $(E, \cdot)$ possède un élément neutre e.
$(E, \cdot)$ est donc un monoïde d'élément neutre e. Soit $x \in E$, il existe $x', x'' \in E$, tels que $G_x(x') = xx' = e$ et $x''x = D_x(x'') = e$ Donc tout élément de E et inversible. En conclusion $(E, \cdot)$ est un groupe.
3 - Soit $(G, \cdot)$ un groupe et H un sous-ensemble fini de G stable par la loi $\cdot$. Donc $(H, .)$ est un ensemble fini muni d'une loi associative pour laquelle tout élément est régulier. Donc H est un sous-groupe de G.
4 - Soit E un ensemble fini de cardinal ≥ 2. on définit sur E la loi $*$ par $x * y = y$. $*$ est associative et tout élément de E est régulier à gauche car $a * x = a * y \Rightarrow x = y$. Mais $(E, *)$ n'est pas un groupe (il ne possède pas d'élément neutre).

Exercice 14. Une table d'une l.c.i sur un ensemble fini E est dite carré latin si dans chaque ligne et dans chaque colonne, tout élément de E figure une et une seule fois.
Montrer que la table d'un groupe fini est un carré latin et étudier la réciproque.

Solution. Une table d'une l.c.i $*$ est un carré latin $\Leftrightarrow$, tout élément est régulier pour $*$. Ceci est vraie pour un groupe. la réciproque est fausse, il suffit de considérer la table :

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

Ce n'est pas la table d'un groupe, l'associativité est en défaut car $a(bc) = aa = b$, mais $(ab)c = ac = c$.

Exercice 15. Soit G un groupe, H et K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe de G, si et seulement si, $H \subset K$ ou $K \subset H$.

Solution. Montrons que, si $H \cup K$ est un sous-groupe, alors $H \subset K$ ou $K \subset H$. Par contraposition. Supposons que $H \not\subseteq K$ et $K \not\subseteq H$, alors il existe $x \in H$ $x \notin K$ et $y \in K$, $y \notin H$. Montrons que $xy^{-1} \notin H \cup K$. Sinon, $xy^{-1} \in H$ ou $xy^{-1} \in K$. Si $xy^{-1} \in H$ on a $x^{-1}xy^{-1} \in H$, ce qui entraîne $y^{-1} \in H$. Absurde. De même, $xy^{-1} \in K$ entraîne $x = xy^{-1}y \in K$ c'est encore une absurdité. Donc $xy^{-1} \notin H \cup K$. Par suite $H \cup K$ n'est pas un groupe.

La réciproque est évidente.

Exercice 16. Soit G un groupe, H, K deux sous-groupes. On suppose qu'il existe $x, y \in G$ tels que $xH = yK$. Montrer que $H = K$.

Solution.

D'abord on a $y^{-1}xH = K$. Donc $y^{-1}xe = y^{-1}x \in K$. Soit $h \in H$, on a $y^{-1}xh \in K$. Donc $y^{-1}xh = k \in K$. D'où $h = x^{-1}yk$. Or $x^{-1}y = (y^{-1}x)^{-1} \in K$ car K est un sous-groupe de G. Donc $h \in K$. D'où $H \subset K$. De façon symétrique on a $K \subset H$. Par conséquent $H = K$.

Exercice 17. Soit G un groupe, H et K deux sous-groupes de G.
1 - Montrer qu'il existe une bijection entre $(H/H \cap K)_g$ et $(KH/K)_g$. (Bien que KH n'est pas nécessairement un sous-groupe de G).
2 - Montrer que si H et K sont finis, alors on a $\text{card}(KH) = \dfrac{|K||H|}{|H \cap K|}$.
3 - Montrer que si H, K sont d'indices finis de G, alors $[H : H \cap K] \leq [G : K]$, que $H \cap K$ est d'indice fini dans G et :

$$[G : H \cap K] \leq [G : H][G : K]$$

4 - Montrer que si $[G : H]$ et $[G : K]$ sont finis et premiers enre eux, alors $G = KH$.

Solution.

1 - Pour tout $x(H \cap K) \in (H/H \cap K)_g$, posons $\phi(x(H \cap K)x) = xK$. Montrons que ϕ est une application injective de $(H/H \cap K)_g$ dans $(G/K)_g$ dont l'image est $(KH/K)_g$.

ϕ est bien définie. En effet, si $x(H \cap K) = y(H \cap K)$, on a $y^{-1}x \in H \cap K$. Donc $y^{-1}x \in K$. i.e. $xK = yK$. Par conséquent, ϕ ne dépend pas du représentant choisi.

Montrons que ϕ est injective. Si $\phi(x(H \cap K)) = \phi(y(H \cap K))$, on a : $xK = yK$. Donc $y^{-1}x \in K$. Comme $x, y \in H$, on a : $y^{-1}x \in H \cap K$. Donc $x(H \cap K) = y(H \cap K)$, ϕ est injective.

Pour $x \in H$, on a $\phi(x(H \cap K)) = xK \in (KH/K)_g$. D'autre part, si $xK \in (KH/K)_g$, $x \in H$, et $\phi(x(H \cap K)) = xK$. Donc $\phi((H/H \cap K)_g = (HK/K)_g$. Il en résulte une bijection entre $(H/H \cap K)_g = (KH/K)_g$.

2 - Si H et K sont finis, les ensembles $(H/H \cap K)_g, (KH/K)_g$ sont finis et ont même cardinal. Par suite $|H|/|H \cap K| = \text{card}(HK)/|K|$.

3 - On suppose que H et K sont d'indices finis. On a $(G/K)_g$ est fini. Donc, d'après 1, $(H/H \cap K)_g$ est fini et card $(H/H \cap K)_g = [H : H \cap K] \leq \text{Card}(G/K)_g = [G : K]$.

On a $[H : H \cap K]$ et $[G : H]$ sont finis. Donc $[G : H \cap K]$ est fini, et $[G : H \cap K] = [G : H][H : H \cap K]$ (multiplicativité des indices). Or $[H : H \cap K] \leq [G : K]$. D'où $[G : H \cap K] \leq [G : H][G : K]$.

4 - On a $[G : H][H : H \cap K] = [G : K][K : H \cap K]$. Par conséquent, $[G : K] | [G : H][H : H \cap K]$. Comme $[G : K] \wedge [G : H] = 1$, on a $[G : K] | [H : H \cap K]$. mais, d'après 1, on a $[H : H \cap K] \leq [G : K]$. Il en résulte que $[G : K] = [H : H \cap K]$. Ou encore $[G : K] = [KH : K]$. Finalement, $G = KH$.

Exercice 18. Soit G le groupe des isométries qui laissent fixe un triangle équilatéral. Donner la liste de tous les sous-groupes G en précisant ceux qui sont distingués.

Solution. Le groupe G des isométries laissant fixe un triangle equilatéral est constitué les éléments : $\imath$ l'identité, trois symétries s_1, s_2, s_3 et deux rotations $r_1, r_2 = r_1^2$. La table de ce groupe est la suivante :

$\circ$	I	r_1	r_2	s_1	s_2	s_3
I	I	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	I	s_3	s_1	s_2
r_2	r_2	I	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	I	r_1	r_2
s_2	s_2	s_3	s_1	r_2	I	r_1
s_3	s_3	s_1	s_2	r_1	r_2	I

On a $|G| = 6$. Si H est un sous-groupe de G alors $|H||6$. Donc $|H| \in \{1, 2, 3, 6\}$. Il est alors facile de voir que les sous-groupes de G sont $\{I\}$, $\{I, s_1\}$, $\{I, s_2\}$, $\{I, s_3\}$, $\{I, r_1, r_2\}$, et G.
Sont distingués les sous-groupes $\{I\}$, $\{I, r_1, r_2\}$, et G.

Exercice 19. Soit G un groupe et H un sous-groupe d'indice 2 de G.
1 - Montrer que H est distingué dans G.
2 - Montrer que $\forall g \in G$ on a : $g^2 \in H$.

Solution.
1 - Il suffit de montrer que $a^{-1}Ha \subset H$ pour tout $a \in G$. C'est vrai si $a \in H$. Soit maintenant $a \notin H$. Comme $[G : H] = 2$, l'ensemble quotient à gauche modulo H est $(G/H)_g = \{H, Ha\}$. De même, l'ensemble quotient à droite modulo H est $(G/H)_d = \{H, aH\}$. On a donc $G = H \cup Ha = H \cup aH$. Il en résulte que $Ha = G \backslash H = aH$. D'où $a^{-1}Ha \subset H$.

2 - Soit $g \in G$. Si $g \in H$, on a : $g^2 \in H$. Si $g \notin H$. Supposons que $g^2 \notin H$. On a $g^2 \in Hg$ (puisque $G = H \cup Hg$). Donc $g^2 = hg$ avec $h \in H$. Ce qui entraîne que $g = h \in H$ absurde. Donc $g^2 \in H$.

Exercice 20. Soit G un groupe et H un sous-groupe de G.
1 - Pour tout $g \in G$, montrer que gHg^{-1} est un sous-groupe de G et que si H est fini, alors $|gHg^{-1}| = |H|$.
2 - On suppose que G possède un seul sous-groupe H d'ordre m. Montrer que H est distingué dans G.

Solution.
1 - Pour tout $g \in G$, Considérons l'automorphisme intérieur $\gamma_g : G \to G$, définie par $\gamma_g(x) = gxg^{-1}$. On a $gHg^{-1} = \gamma_g(H)$. C'est l'image par un morphisme d'un sous-groupe donc c'est un sous-groupe. Si H est fini, comme γ_g est bijectif, on a : $|gHg^{-1}| = |\gamma_g(H)| = |H|$.
2 - Si G possède un seul sous-groupe H d'ordre m, alors pour tout $g \in G$, on a $|gHg^{-1}| = |H| = m$. Donc $gHg^{-1} = H$. D'où $H \lhd G$

Exercice 21. Soit G un groupe. On définit sur G une loi $*$ par $x * y = yx$. Montrer que $(G, *)$ est un groupe isomorphe à G.

Solution. En écrivant : $x * y = yx = (x^{-1}y^{-1})^{-1}$, on déduit que $(x * y)^{-1} = x^{-1}y^{-1}$. Donc l'application $(G, *) \to (G, \cdot)$, $x \mapsto x^{-1}$, est un isomorphisme.

Exercice 22. Montrer que les groupes $(\mathbb{Q}^*_+, \times)$ et $(\mathbb{Q}, +)$ ne sont pas isomorphes.

Solution. Supposons qu'il existe un isomorphisme $f : (\mathbb{Q}, +) \to (\mathbb{Q}^*_+, \times)$. Il existe $\alpha \in \mathbb{Q}$, tel que $f(\alpha) = 2$. On a $2 = f(\alpha) = f(\frac{\alpha}{2} + \frac{\alpha}{2}) = f(\frac{\alpha}{2})^2$. Donc $f(\frac{\alpha}{2}) = \sqrt{2}$. Absurde, car $\sqrt{2} \notin \mathbb{Q}$.

Exercice 23. Soit $G = \{e, a, b, c\}$ groupe non cyclique d'ordre 4 d'élément neutre e.
1 - Montrer que $a^2 = b^2 = c^2 = e$, $ab = ba = c$, $ac = ca = b$, $bc = cb = a$. En déduire que G est abélien.
2 - Montrer que G est un groupe de Klein.
3 - Donner la liste, à un isomorphisme près, de tous les groupes d'ordre ≤ 5.

Solution.
1 - Soit $x \in G$. On a $o(x) \,|\, |G| = 4$. Donc $o(x) \in \{1, 2, 4\}$. Puisque G n'est pas cyclique, on a $o(x) = 1 \,\text{ou}\, 2$. Par suite, $x^2 = e$.

Par ailleurs on a ab et $ba \neq a, b$ donc $ab = ba = c$ De même $ac = ca = b$ et $bc = cb = a$. En particulier, G est abélien.

2 - Posons $H = \{e, a\}$, $K = \{e, b\}$. On a $HK = G$, $H \cap K = \{e\}$ et $H, K \triangleleft G$ (car G est abélien). Donc (voir cours) $G \cong H \times K$. C'est le produit direct de deux groupes cycliques d'ordre 2, c'est un groupe de Klein.

En conclusion, tout groupe non cyclique d'ordre 4 est de Klein.

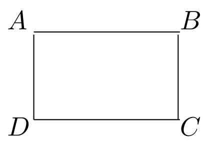
3 - Soit G un groupe d'ordre ≤ 5. Alors :

• Si $|G| = 1$, il est isomorphe à $\{e\}$.

• Si $|G = |p = 2, 3, 5$, il est isomorphe à $(\mathbb{Z}/p\mathbb{Z}, +)$, car p est premier .

• Si $|G| = 4$, il est alors soit cyclique, isomorphe à $(\mathbb{Z}/4\mathbb{Z}, +)$, soit de Klein, isomorphe à $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$.

Exercice 24. Soit $R = ABCD$ un rectangle qui n'est pas un carré.



Trouver son groupe de symétries.

Solution.

On a $\| \overrightarrow{AB} \| = \| \overrightarrow{CD} \|$, $\| \overrightarrow{BC} \| = \| \overrightarrow{AD} \|$, et $\| \overrightarrow{AB} \| > \| \overrightarrow{AD} \|$

Les isométries qui laissent fixe ce rectangle sont, en plus de l'identité I :

- la symétrie par rapport à l'axe passant par les milieux des côtés AD et BC : $\sigma_1 = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$.

- La symétrie par rapport à l'axe passant par les milieux des côtés AB et CD : $\sigma_2 = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$.

- La rotation d'angle π, $\sigma_3 = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$

$G = \{I, \sigma_1, \sigma_2, \sigma_3\}$, tous ses éléments sont d'ordre 1 ou 2. Il n'est pas cyclique, donc isomorphe au groupe de Klein.

Exercice 25. Dans $\mathrm{GL}_2(\mathbb{R})$ on considère les matrices $A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Trouver les ordres de A, B et AB.

Solution.

On a $A^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$, et $A^3 = I$. Donc $o(A) = 3$. De même $B^2 = -I$, $B^3 = -B$, $B^4 = I$. Donc $o(B) = 4$.

$AB = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$, $AB = I + N$, avec $N = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}$. On a $(AB)^k = (I + N)^k = I + kN \neq I$, $\forall k \in \mathbb{N}^*$. Donc AB n'est pas d'ordre fini.

Exercice 26.
1 - Soit $f : G \to G'$ un morphisme de groupes. Si $x \in G$ est d'ordre fini, montrer que l'ordre de $f(x)$ divise l'ordre de x, avec égalité si f est injectif.
2 - Soit G un groupe, $x, y \in G$, montrer que les éléments xy et yx sont conjugués et en déduire qu'ils ont le même ordre.
Montrer le même résultat pour xyz, yzx, zxy.

Solution.
1 - Soit $n = o(x)$. On a $f(x)^n = f(x^n) = f(e) = e'$. Donc $o(f(x))|n$.
Supposons que f est injectif, soit $k \in \mathbb{N}$ tel que $f(x)^k = e'$. On a : $f(x^k) = e'$. Comme f est injectif, $x^k = e$. d'où $n|k$. Il en résulte que $o(f(x)) = n$.
2 - Il suffit de remarquer que $xy = xyxx^{-1} = \gamma_x(yx)$. Où γ_x est l'automorphisme intérieur associé à x. Donc, d'après 1, $o(xy) = o(\gamma_x(yx)) = o(yx)$.
De même $xyz = xyzxx^{-1} = z^{-1}zxyz$.

Exercice 27. Soit G un groupe fini d'ordre n et k un entier naturel. On considère l'application $f : G \to G$, définie par $f(x) = x^k, \ \forall x \in G$.
1 - f est-elle un endomorphisme ? Justifier.
2 - On suppose que k est premier avec n.
a - Montrer que f est bijective.
b - Montrer qu'il existe un entier m tel que $f^{-1}(x) = x^m, \ \forall x \in G$.

Solution.
1 - En général, f n'est pas un endomorphisme. Par exemple, on prend $G = \mathcal{S}_3$, $k = 2$, $x = (12), y = (23)$. On a $(xy)^2 = (123)^2 = (132)$, alors que $x^2y^2 = I$.
2 - On suppose $k \wedge n = 1$.
a - D'après Bézout, il existe $u, v \in \mathbb{Z} : uk + vn = 1$. Soit $x \in G$. Posons $z = x^u$. On a $z^k = x^{uk} = x^{1-vn} = x.x^{-vn} = x$. Donc x admet un antécédent. Par conséquent, f est surjective. Comme G est fini, f est bijective.
b - La question a, montre qu'il suffit de prendre $m = u$, puisque $(x^k)^m = x$.

Exercice 28. (Théorème de Cauchy pour les groupes abéliens) Soit G un groupe abélien fini et p un nombre premier divisant l'ordre de G. Montrer que G contient un élément d'ordre p.

Solution. Posons $|G| = pm$ et raisonnons par récurrence sur m. Si $m = 1$, $|G| = p$, $G \cong \mathbb{Z}/p.\mathbb{Z}$, le résultat est vrai.
Supposons que $m > 1$ et que le résultat soit vrai pour tous les entiers $< m$. Si G est un groupe d'ordre pm, considérons un élément $g \neq e$ de G et $H = \mathrm{gr} < g >$. On a $H \neq \{e\}$.

• Si $H = G$, G est cyclique et l'élément g^m est d'ordre p.

• Si $H \neq G$, on a $p \mid |G| = [G : H].|H|$.

- Si $p \mid |H|$, comme on a $|H| < |G|$, on applique l'hypothèse de récurernce qui nous donne un élément x d'ordre p dans H donc dans G.

- Si $p \nmid |H|$ on a $p \mid [G : H]$. Comme G est abélien, $H \lhd G$, et $|G/H| = [G : H] < |G|$, on applique alors l'hypothèse de récurence à G/H : il existe $\bar{x} \in G/H$, tel que $o(\bar{x}) = p$. Donc $x^p \in H$. Posons $|H| = k$ et $y = x^k$. Montrons que $o(y) = p$. D'après Bézout, il existe $\alpha, \beta \in \mathbb{Z} : \alpha p + \beta k = 1$. On a $x = x^{\alpha p + \beta k} = (x^p)^\alpha.y^\beta$, forcèment $y \neq e$, car sinon on aura $x \in H$. Par ailleurs, $y^p = (x^k)^p = e$, par conséquent $o(y) = p$.

Exercice 29. Soit G un groupe d'élément neutre e tel que $\forall x \in G$ on a $x^2 = e$.
1 - Montrer que G est abélien.
2 - On suppose que G est fini. Montrer que son ordre est une puissance de 2.

Solution.
1 - Pour $x, y \in G$, on a : $e = (xy)^2 = xyxy$. Donc $xy = x^2yxy^2 = yx$. G est abélien.
2 - Soit p un nombre premier tel que $p \mid |G|$. D'après le théorème de Cauchy pour les groupes abéliens, il existe dans G un élément x d'ordre p. On a $x^p = e$ ce qui entraîne que $2|p$, par conséquent $p = 2$. Ainsi 2 est le seul nombre premier divisant $|G|$. Il en résulte que $|G|$ est une puissance de 2.

Exercice 30. Soit G un groupe cyclique d'ordre n engendré par un élément g.
Si k un diviseur de n. Montrer que G possède un seul sous-groupe d'ordre k.

Solution. Considérons l'ensemble $H = \{g \in G : g^k = e\}$. Montrons que H est un sous-groupe d'ordre k de G. On a $e^k = e$, donc $e \in H$. Si $x, y \in H$, alors $(xy^{-1})^k = x^k(y^k)^{-1}$ car G est abélien. Donc $(xy^{-1})^k = e$. Par suite $xy^{-1} \in H$. H est un sous-groupe de G.

H est cyclique comme sous-groupe d'un groupe cyclique. Posons $H = \text{gr}\langle h\rangle$. Comme $h^k = e$, on a $o(h) = |H| \le k$. Montrons que $|H| \ge k$. Soit $x = g^{\frac{n}{k}}$. Il est clair que $o(x) = k$. Donc $x \in H$. Par suite $k \le |H|$. Finalement $|H| = k$.
Soit H' un autre sous-groupe d'ordre k de G. On a $\forall x \in H'$, $x^k = e$. Donc $H' \subset H$. Comme $|H| = |H'| = k$, on a $H' = H$.

Exercice 31. Soit $(G, \cdot)$ un groupe d'élément neutre e.
1 - Si g est un élément d'ordre n de G. Montrer que l'ordre de g^k est égal à $\frac{n}{n\wedge k}$, où $n \wedge k$ désigne le PGCD de n et k. En déduire que g^k engendre $\text{gr}<g>$, si et seulement si, k est premier avec n.
2 - Soit $x \in G$ tel que $o(x) = n$. Pour $k|n$, montrer que $o(x^{\frac{n}{k}}) = k$.
3 - Soient $a, b \in G$ d'ordres finis tels que $ab = ba$ et $o(a) \wedge o(b) = 1$. Montrer que $\text{gr}<a>\cap \text{gr} <b>= \{e\}$ et que $o(ab) = o(a)o(b)$.
4 - Déterminer le groupe des éléments inversibles du monoïde $(\mathbb{Z}/36\mathbb{Z}, \cdot)$. Calculer l'ordre de chacun de ses éléments. Est-il cyclique ?

Solution.
1 - Posons $m = \frac{n}{n\wedge k}$. On a $(g^k)^m = g^{km}$. Or $km = n\frac{k}{n\wedge k}$, $n|km$. Donc $(g^k)^m = e$. Par conséquent, $o(g^k)|m$. Réciproquement, Posons $d = n \wedge k$. On a $n = m.d$ et $k = k'.d$ avec $m \wedge k' = 1$. Si $(g^k)^s = e$, on a $n|ks$. Donc $md|k'ds$. i.e. $m|k's$. Comme $m \wedge k' = 1$, on a $m|s$.
g^k engendre $\text{gr}<g>$, si et seulement si, $o(g^k) = n$. Donc si et seulement si, $\frac{n}{n\wedge k} = n$. C'est à dire $n \wedge k = 1$.
2 - $o(x^{\frac{n}{k}}) = \frac{n}{n\wedge d}$, avec $d = \frac{n}{k}$. Donc $o(x^{\frac{n}{k}}) = \frac{n}{d} = k$.
3 - Soit $x \in \text{gr} <a>\cap \text{gr} <b>$. D'après le théorème de Lagrange, on a $o(x)|o(a)$ et $o(x)|o(b)$. Comme $o(a) \wedge o(b) = 1$, on a $o(x) = 1$, i.e $x = e$.

Posons $n = o(a)o(b)$. Puisque $ab = ba$, on a $(ab)^n = a^n b^n = e$. Soit maintenant m un entier tel que $(ab)^m = e$. On a $a^m b^m = e$ Donc $a^m = b^{-m} \in \text{gr} <a>\cap \text{gr} <b>$. Donc $a^m = e$ et $b^m = e$. Par conséquent, $o(a)|m$ et $o(b)|m$. Comme $o(a) \wedge o(b) = 1$, on a $o(a)o(b) = n|m$. En conclusion, $o(ab) = o(a)o(b)$.

Posons $\mathbb{U}_n$ le groupe des inversibles du monoïde $(\mathbb{Z}/n\mathbb{Z}, .)$. On sait d'après l'exercice **??**, que $\mathbb{U}_n = \{\overline{k} \in \mathbb{Z}/n\mathbb{Z} : k \wedge n = 1\}$.

$\mathbb{U}_{36} = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{29}, \overline{31}, \overline{35}\}$. est un groupe d'ordre 12.

• gr$<\overline{5}>= \{\overline{1}, \overline{5}, \overline{25}, \overline{17}, \overline{13}, \overline{29}\}$.

$o(\overline{1}) = 1$, $o(\overline{5}) = 6$, $o(\overline{25}) = o(\overline{5}^2) = 3$, $o(\overline{17}) = o(\overline{5}^3) = 2$, $o(\overline{13}) = o(\overline{5}^4) = 3$, $o(\overline{29}) = o(\overline{5}^5) = 6$.

• gr$<\overline{7}>= \{\overline{1}, \overline{7}, \overline{13}, \overline{19}, \overline{25}, \overline{31}\}$.

$o(\overline{7}) = 6$, $o(\overline{19}) = o(\overline{7}^3) = 2$, $o(\overline{31}) = o(\overline{7}^5) = 6$, $o(\overline{35}) = \overline{-1} = 2$.

• gr$<\overline{11}>= \{\overline{1}, \overline{11}, \overline{13}, \overline{13}, \overline{35}, \overline{25}, \overline{23}\}$.

$o(\overline{11}) = 6$, $o(\overline{23}) = o(\overline{11}^5) = 6$.

$\mathbb{U}_{36}$ n'est pas cyclique car il ne contient aucun élément d'ordre 12.

Exercice 32. Soit un groupe G tel que l'application $x \mapsto x^{-1}$ soit un endomorphisme de G. Montrer que G est abélien.

Solution. On a $\forall x, y \in G$, $(xy)^{-1} = y^{-1}x^{-1} = (yx)^{-1}$. Donc $xy = yx$. G est abélien.

Exercice 33. Dans cet exercice, G désigne un groupe fini d'ordre $2p$, où p est un nombre premier impair.
1 - Montrer que $\forall x \in G$, on a $o(x) \in \{1, 2, p, 2p\}$.
2 - Montrer que G contient un élément a d'ordre p.
Dans la suite on notera N le sous-groupe engendré par a.
3 - Montrer que N est distingué dans G.
4 - Montrer que $\forall x \in G$, si $o(x) = p$ alors $x \in N$.
5 - Montrer que G contient un élément b d'ordre 2 et que $bab = a^k$, où $k = 1$ ou $p-1$.

6 - On suppose que $k = 1$. Montrer que G est cyclique.
7 - On suppose que $k = p-1$. Montrer que G est diédral.

Solution.

1 - D'après le Théorème de Lagrange, $\forall x \in G$, $o(x) \mid |G| = 2p$. Donc $o(x) \in \{1, 2, p, 2p\}$.
2 - Si $\forall x \in G \backslash \{e\}, o(x) = 2$, on aura , d'après l'exercice 29, $|G|$ est une puissance de 2, ce qui est faux. Donc il existe un élément $x \in G\backslash\{e\} : o(x) \neq 2$. i.e. $x^2 \neq e$. Posons $a = x^2$, alors puisque $|G| = 2p$, on a $a^p = (x^2)^p = x^{2p} = e$. Ce qui entraîne que $o(a) = p$.
3 - On a $|N| = p$, donc $[G : N] = 2$. D'après l'exercice 19, $N \lhd G$.
4 - Soit $x \in G$ tel que $o(x) = p$, on a $x^2 \in N$. D'après Bézout, il existe $u, v \in \mathbb{Z} : 2u + pv = 1$. Donc $x = x^1 = (x^2)^u.(x^p)^v = (x^2)^u \in N$.
5 - Supposons que $\forall x \in G$, on a $x^p = e$. On aura alors, d'après 4, $x \in N$. Ce qui entraîne $G \subset N$, ce qui est absurde. Par suite, il existe $x \in G : x^p \neq e$. Posons $b = x^p$. On a $b^2 = e$. b est donc un élément d'ordre 2.

Puisque $N \lhd G$, on a $bab = bab^{-1} = a^k \in N$, et $a = bbabb = ba^kb = (bab)^k = (a^k)^k = a^{k^2}$. Ce qui implique que $a^{k^2-1} = e$. D'où $p \mid k^2 - 1 = (k-1)(k+1)$. Ou encore, puisque p est premier, $p \mid k-1$ ou $p \mid k+1$. Comme $k \in \{0, 1, 2 \ldots p-1\}$, on a : $k = 1$ ou $k = p-1$.
6 - Si $k = 1$, $ab = ba$, montrons que $o(ab) = 2p$. On a $(ab)^{2p} = e$. Soit $n \in \mathbb{Z}$ tel que $(ab)^n = e$. Puisque $ab = ba$, on a : $(ab)^n = a^nb^n = e$. Ou encore $a^n = b^{-n}$. En élevant à la puissance p on obtient : $e = a^{np} = b^{-np}$. Il en résulte que $2 \mid np$. D'où $2 \mid n$, car p est impair. Par conséquent, $a^n = e$, il s'ensuit que $p \mid n$. Finalement, $2p \mid n$. En conclusion, $o(ab) = 2p$, ce qui entraîne que G est cyclique engendré par ab.
7 - Si $k = p-1$, et puisque $[G : N] = 2$, on a : $G = N \cup Nb$. Donc tout élément de G est de la forme a^kb^m, ce qui entraîne que G est engendré par a et b. Par ailleurs, $o(a) = p$, $o(b) = 2$, $abab = e$, donc $o(ab) = 2$. Finalement G est diédral.

Conclusion finale : Tout groupe fini d'ordre $2p$, avec p premier impair, est ou bien cyclique ou bien diédral. Cela s'applique, par exemple, pour les groupes d'ordres 6, 10, 14, etc..

Exercice 34. Soit $(M, +)$ un groupe abélien noté additivement, d'élément neutre noté 0. Pour $n \in \mathbb{N}$, On pose $T_n(M) = \{x \in M : nx = 0\}$.
1 - Montrer que $T_n(M)$ est un sous-groupe de M.
2 - Exprimer $T_n(M)$ pour $M = \mathbb{Z}/m\mathbb{Z}$.

Solution.
1 - On a $0 \in T_n(M)$ et si $x, y \in T_n(M)$, on a : $nx = ny = 0$. Donc $n(x-y) = 0$. Ce qui entraîne que $x-y \in T_n(M)$.

2 - D'après la caractérisation des sous-groupes de $M = \mathbb{Z}/m\mathbb{Z}$, $T_n(\mathbb{Z}/m\mathbb{Z}) = H/m\mathbb{Z}$, où H est le sous-groupe de $\mathbb{Z}$: $H = \{k \in \mathbb{Z} : \overline{kn} = \bar{0}\} = \{k \in \mathbb{Z} : m \mid kn\}$.

Soit $k \in H$. On a $m \mid kn$. i.e. $kn = \alpha m$, avec $\alpha \in \mathbb{Z}$. Posons $d = \mathrm{PGCD}(m, n)$, alors : $m = du$ et $n = dv$ avec u, v premiers entre eux. $kn = kdv = \alpha m = \alpha du \Rightarrow kv = \alpha u$. Comme u, v sont premiers entre eux, $u \mid k$, i.e $k = \beta \frac{m}{d}$.

Réciproquement, si $k = \alpha \frac{m}{d}$, alors $kn = \alpha \frac{nm}{d} = \alpha m \frac{n}{d}$, est divisible par m.

Conclusion : $H = \frac{m}{d}\mathbb{Z}$ et $T_n(\mathbb{Z}/m\mathbb{Z}) = \frac{m}{d}\mathbb{Z}/m\mathbb{Z}$.

Exercice 35. Soient N et M deux groupes abéliens notés additivement. On note $\mathrm{Hom}(N, M)$ l'ensemble des homomorphismes de N dans M.
Pour $f, g \in \mathrm{Hom}(N, M)$ on considère l'application $f + g$ définie par :

$$f + g(x) = f(x) + g(x) \quad \forall x \in N$$

1 - Montrer $f + g \in \mathrm{Hom}(N, M)$.
2 - Montrer $(\mathrm{Hom}(N, M), +)$ est un groupe abélien.
3 - On prend $N = \mathbb{Z}/n\mathbb{Z}$ et on considère l'application $\phi : \mathrm{Hom}(N, M) \to M$, définie par $\phi(f) = f(\bar{1})$.

a - Montrer que ϕ est un homomorphisme de groupes.
b - Montrer qu'on a l'isomorphisme $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, M) \cong T_n(M)$.
c - Identifier $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$.

Solution.
1 - Montrons que $f + g \in \mathrm{Hom}(N, M)$. Posons $h = f + g$. On a $\forall x, y \in N$, $h(x + y) = (f + g)(x + y) = f(x + y) + g(x + y) = f(x) + f(y) + g(x) + g(y) = f(x) + g(x) + f(y) + g(y)$.

Donc $h(x + y) = (f + g)(x) + (f + g)(y) = h(x) + h(y)$, $h = f + g \in \mathrm{Hom}(N, M)$.

2 - Il suffit de montrer que $\mathrm{Hom}(N, M)$ est un sous-groupe du groupe des applications $N \to M$. En effet, il est non vide, car contient l'application nulle. Stable par $+$ d'après 1, et si $f \in \mathrm{Hom}(N, M)$, alors $-f \in \mathrm{Hom}(N, M)$.

3 - a - Soient $f, g \in \mathrm{Hom}(N, M)$, on a : $\phi(f + g) = (f + g)(\bar{1}) = (f)(\bar{1}) + (g)(\bar{1})$. L'application ϕ est donc un morphisme de groupes.

b - Montrons que $\mathrm{Im}\phi = T_n(M)$. Si $x \in \mathrm{Im}\phi$, il existe $f \in \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, M)$, tel que $f(\bar{1}) = x$. On a $nx = f(\bar{n}) = f(\bar{0}) = 0$. Donc $x \in T_n(M)$. Réciproquement, si $x \in T_n(M)$. Soit $g : \mathbb{Z} \to M$, définie par $g(k) = kx$. g est un homomorphisme et $g(n\mathbb{Z}) = \{0\}$. D'après la décomposition canonique, il existe $f : \mathbb{Z}/n\mathbb{Z} \to M$, telle que $f(\bar{k}) = g(k)$, et on a$\phi(f) = f(\bar{1}) = g(1) = x$. Par conséquent, $x \in \mathrm{Im}\phi$.

Montrons que ϕ est injectif. Soit $f \in \mathrm{Ker}\phi$. On a $\phi(f) = f(\bar{1}) = 0$. Par suite, $\forall \bar{k} \in \mathbb{Z}/n\mathbb{Z}$, $f(\bar{k}) = kf(\bar{1}) = 0$. D'où $f = 0$. ϕ est injectif. En conséquence, $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, M) \cong \mathrm{Im}\phi = T_n(M)$.

c - $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong T_n(\mathbb{Z}/m\mathbb{Z}) = \omega Z/m\mathbb{Z}$, où $\omega = \frac{m}{d}$, d étant le PGCD de m et n. Par conséquent, $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$.

Exercice 36. Soit p un nombre premier différent de 2, G un un groupe fini d'ordre $p + 1$ et d'élément neutre e. On suppose que G possède un automorphisme σ d'ordre p. On pose $E = G\backslash\{e\}$, et on note α la restriction de σ à E.
1 - Soit $\Gamma = \{I, \sigma, \sigma^2, \ldots \sigma^{p-1}\}$. Montrer que, pour tout $a \in G$, l'ensemble $H_a = \{\phi \in \Gamma : \phi(a) = a\}$ est un sous-groupe de Γ.
2 - Montrer qu'il existe $a \in E$ tel que $G = \{e, a, \sigma(a), \sigma^2(a), \ldots, \sigma^{p-1}(a)\}$.
3 - Montrer que $a^2 = e$. (Raisonner par l'absurde en supposant que $a^2 \neq e$. Montrer alors qu'il existe $1 \leq k \leq p - 1$, tel que $a^{-1} = \sigma^k(a)$ et conclure à une contradiction).
4 - Montrer que $\forall x \in G$, on a : $x^2 = e$ et en déduire que G est abélien d'ordre une puissance de 2.
5 - Donner un exemple d'un tel groupe et un tel automorphisme.

Solution. 1 - Soit $H_a = \{\phi \in \Gamma : \phi(a) = a\}$. Montrons que H_a est un sous-groupe de Γ. L'ensemble H_a contient évidemment l'application identique I. De plus, si ϕ et ϕ' sont dans H_a, alors $\phi \circ \phi'(a) = \phi(\phi'(a)) = \phi(a) = a$. Par ailleurs, $\phi^{-1}(a) = \phi^{-1}(\phi(a)) = a$. En conclusion, H_a es un sous-groupe de G.
2 - Comme H_a est un sous-groupe de Γ qui es d'ordre p premier, on a, d'après le Théorème de Lagrange, $|H_a| = 1,$ou p. Donc $H_a = \Gamma$, ou $H_a = \{I\}$. Montrons qu'il existe $a \in G$ tel que $H_a = \{I\}$. Sinon, $\forall a \in G$, on aura $H_a = \Gamma$, ce qui impliqueralt que $\forall a \in G$, $\sigma(a) = a$ et que $\sigma = I$, absurde. Soit donc $a \in G$ tel que $H_a = \{I\}$. On a $F = \{a, \sigma(a), \sigma^2(a), \ldots, \sigma^{p-1}(a)\} \subset E$. Mais card $F = p$, car $\sigma^k(a) \neq \sigma^m(a)$, $\forall k \neq m = 0, 1 \ldots p-1$. Donc $F = E$. D'où $G = E \cup \{e\} = \{e, a, \sigma(a), \sigma^2(a), \ldots, \sigma^{p-1}(a)\}$.

3 - Par l'absurde, supposons que $a^2 \neq e$, alors $a^{-1} \neq a$. Par suite, existe un entier k tel que $1 \leq k \leq p - 1$, et $a^{-1} = \sigma^k(a)$. Appliquons σ^{p-k}, on obtient : $\sigma^{p-k}(a^{-1}) = \sigma^{p-k}(\sigma^k(a)) = \sigma^p(a) = a$. D'où $a^{-1} = \sigma^{p-k}(a)$. Par suite $\sigma^{p-k}(a) = \sigma^k(a)$. D'après le choix de a, on a $p-k = k$, ce qui entraîne que $p = 2k$, absurde. Donc $a^2 \neq e$.

4 - On a $\forall g \in G\backslash\{e\}$, il existe k tel que $g = \sigma^k(a)$. Alors, $g^2 = \sigma^k(a^2) = \sigma^k(e) = e$. Il en résulte que G est abélien d'ordre une puissance de 2 d'après Exercice 3.

5 - En cherchant un exemple, on note d'abord que $x^2 = e$ pour tout élément de G. On a un exemple de ce type de groupe : c'est le groupe de Klein $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On considère l'endomorphisme σ défini par : $\sigma(x, y) = (x + y, x)$. $\sigma^2(x, y) = (y, x + y)$, $\sigma^3(x, y) = (x, y)$. Donc σ est un automorphisme d'ordre $3 = 4 - 1$.

Exercice 37. Soient les matrices complexes : $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$; $K = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$; $L = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

On pose $H = \{I, -I, J, -J, K, -K, L, -L\}$.
1 - Montrer que H est un groupe non commutatif pour la multiplication des matrices. (H est appelé groupe des quaternions).
2 - Montrer que tout sous-groupe de H est distingué.
3 - Montrer que H n'est pas diédral. (On montrera que le groupe diédral d'ordre 8 contient un sous-groupe d'ordre 2 non distingué).
4 - Soit G un groupe engendré par deux éléments a, b tels que $o(a) = 4$, $a^2 = b^2$, et $aba = b$. On pose $N = \text{gr} < a >$.
a - Montrer que $bN \subset Nb$.
b - Soit $K = N \cup Nb$. montrer que K est un sous-groupe de G et en déduire qu $K = G$.
c - Montrer que $|G| = 8$ et que tous les éléments de G s'écrivent $a^k b^m$, avec $k = 0, 1, 2, 3$ et $m = 0, 1$.
d - Montrer que G est isomorphe au groupe des quaternions.

Solution.
1 - Il suffit de montrer que H est stable par produit matriciel et que l'inverse d'un élément de H est un élément de H. On a : $I \in H$ et $JK = -KJ = L$, $KL = -LK = J$, $LJ = -JL = K$, $J^2 = K^2 = L^2 = -I$. Ceci implique aussi que $J^{-1} = -J, K^{-1} = -K, L^{-1} = -L$.

2 - Si N est un sous-groupe de H, alors $o(H) \in \{1, 2, 4, 8\}$. Par ailleurs, on a $o(I) = 1$, $o(-I) = 2$, les $o(\pm J) = o(\pm K) = o(\pm L) = 4$.
- Les sous-groupes triviaux $\{I\}$ et H sont évidemment distingués.
- Un seul sous-groupe d'ordre 2 qui est $\{I, -I\}$ il est distingué.
- Les sous-groupe d'ordre 4 sont évidemment distingués car ils sont d'indice 2.
3 - Le groupe diédral $\Delta_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, possède un sous-groupe d'ordre 2, $\{e, b\}$ qui est non distingué car $aba^{-1} = a^2b \notin \{e, b\}$. Donc, d'après 2, H n'est pas diédral.

4 - a - Montrons que $bN \subset Nb$, c'est à dire $bNb^{-1} \subset N$. On a : $ba^kb^{-1} = (bab^{-1})^k = (a^3)^k = a^{3k} \in N$.
b - Montrons que $K = N \cup Nb$ est un sous-groupe de G.

On a $K \neq \varnothing$, car $e \in K$. Soient $g, h \in K$.

- Si $g, h \in N$ on a $gh \in N$ car N est un sous-groupe de G.

- Si $g \in N$ et $h \in Hb$, on a $gh \in Nb$.

- Si $g \in Nb$ et $h \in N$, on a $gh \in NbN \subset N.Nb \subset Nb$.

- Si $g, h \in Nb$, on a $gh \in NbNb \subset N.Nb^2 \subset N$, car $b^2 = a^2 \in N$.

Dans tous les cas on a $gh \in K$.

- Soit $g \in k$, si $g \in N$, $g^{-1} \in N$, si $g \in Nb$, $g^{-1} \in b^{-1}N = b^3N = b.b^2N \subset bN \subset Nb$.

En conclusion, K est un sos-groupe de G. Comme $a, b \in K$, on a $G \subset K$. Par conséquent, $G = K = N \cup Nb$.
c - On a $|G| = |N|.[G : N] = 4.2 = 8$. Comme $G = N \cup Nb$, tout élément de G est de la forme a^kb^m.
d - Considérons le J, K les éléments du groupe des quaternions H de la question 1. Posons $\phi(a^mb^n) = J^mK^n$. Si $a^mb^n = a^{m'}b^{n'}$, on a $J^mK^n = J^{m'}K^{n'}$. ϕ définit ainsi une application de G dans H. ϕ est un morphisme in jectif. Comme $o(G) = |H|$, c'est un isomorphisme.

Exercice 38. Soit G un groupe non abélien d'ordre 8 d'élément neutre e.
1 - Montrer que G contient un sous-groupe cyclique H d'ordre 4 et que H est distingué.
Dans la suite, on notera $H = \{e, a, a^2, a^3\}$.
2 - Soit $b \in G \backslash H$. Montrer $G = H \cup Ha$ et en déduire que H est engendré par a, b.
3 - Montrer que $bab^{-1} = a^3$.
4 - On suppose que b est d'ordre 2. Montrer que G est diédral.
5 - On suppose que b est d'ordre 4. Montrer que G est quaternionien.

Solution.
1 - Soit $x \in G$, on a $o(x)|8$, donc $o(x) \in \{1, 2, 4, 8\}$.
Si $x^2 = e \forall x \in G$, alors G est abélien ce qui est absurde. Donc il existe $a \in G$ tel que $o(a) = 4$.
Soit $H = \text{gr} < a >$, alors $[G : H] = 2$. Donc $H \lhd G$.
2 - Comme $[G : H] = 2$, et $b \notin H$, on a $(G/H)_d = \{H, Hb\}$. Donc $G = H \cup Hb$. Tout élément de G est alors de la forme $a^k b^j$. Donc $G = \text{gr} < a, b >$.
3 - Comme H est distingué, on a $bab^{-1} \in H$ et $o(bab^{-1}) = o(a)$. Par conséquent bab^{-1}, engendre H. Il en résulte que $bab^{-1} = a$ ou a^3. Si $bab^{-1} = a$, alors $ab = ba$. Or G est engendré par a et b donc il sera abélien ce qui est absurde. Par conséquent $bab^{-1} = a^3$.
4 - Si $o(b) = 2$, on a $o(a) = 4$, $abab = a.a^3 = e$. Donc $o(ab) = 2$. G est alors diédral.
5 - Si $o(b) = 4$, on a $b^2 \in H$, comme b^2 est d'ordre 2, il s'ensuit que $b^2 = a^2$. G est quaternionien.

Exercice 39. Dans le groupe affine $G = \text{GA}(\mathbb{R})$, on note $N = \{f_{1,b} : b \in \mathbb{R}\}$. Montrer que N est un sous-groupe distingué de $\text{Aff}_1(\mathbb{R})$ et que $\text{GA}(\mathbb{R})/N \cong (\mathbb{R}_+^*, \times)$.

Solution. Soit l'application $\phi : G \to (\mathbb{R}_+^*, \times)$, définie par $\phi(f_{a,b}) = a$. Alors $\phi(f_{a,b} \circ f_{c,d}) = \phi(f_{ac,ad+b}) = ac = \phi(a)\phi(c)$. Donc ϕ est un morphisme de groupes. On vérifie facilement qu'il est surjectif et que $\text{Ker}\phi = N$. Le premier théorème des isomorphismes permet alors d'écrire $\text{GA}(\mathbb{R})/N \cong (\mathbb{R}_+^*, \times)$.

Exercice 40. Soit G un groupe. Pour tout $g \in G$, on considère l'application $\gamma_g : G \to G$, définie par $\gamma_g(x) = gxg^{-1}$, $\forall x \in G$.
1 - Montrer que γ_g est un automorphisme de G appelé automorphisme intérieur associé à g.
2 - Montrer que $\gamma_{gh} = \gamma_g \circ \gamma_h$. et que $(\gamma_g)^{-1} = \gamma_{g^{-1}}$.
3 - On note $\text{Aut}(G)$, le groupe des automorphismes de G. $\text{Int}(G)$ l'ensemble des automorphismes intérieurs de G.
a - Montrer que $\text{Int}(G)$ est un sous-groupe distingué de $\text{Aut}(G)$.
b - Etablir l'isomorphisme $\text{Int}(G) \cong G/Z(G)$, où $Z(G)$ désigne le centre de G.

Solution.
1 - On a $\forall x, y \in G$, $\gamma_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \gamma_g(x)\gamma_g(y)$. Donc γ_g est un endomorphisme.
On a $\gamma_g \circ \gamma_{g^{-1}} = \gamma_{g^{-1}} \circ \gamma_g = I_G$. Donc γ_g est bijectif. C'est un automorphisme.
2 - $\forall x \in G$, on a : $\gamma_{gh}(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = \gamma_g(\gamma_h(x)) = \gamma_g \circ \gamma_h(x)$. Par conséquent, $\gamma_{gh} = \gamma_g \circ \gamma_h$.
On a $\gamma_g \circ \gamma_{g^{-1}} = \gamma_e = I_G$. Donc $\gamma_{g^{-1}} = (\gamma_g)^{-1}$.
3 - a - $I_G \in \text{Int}(G)$. Si $\gamma_g, \gamma_h^{-1} \in \text{Int}(G)$, on a : $\gamma_g \circ \gamma_h^{-1} = \gamma_{gh^{-1}} \in \text{Int}(G)$. Donc $\text{Int}(G)$ est un sous-groupe de $\text{Aut}(G)$.
Montrons qu'il est distingué. Soit $\sigma \in \text{Aut}(G)$. On a $\forall x \in G$, $\sigma \circ \gamma_g \circ \sigma^{-1}(x) = \sigma(g\sigma^{-1}(x)g^{-1}) = \sigma(g)x\sigma(g^{-1}) = \gamma_{\sigma(g)}(x)$. Par suite, $\sigma \circ \gamma_g \circ \sigma^{-1} == \gamma_{\sigma(g)} \in \text{Int}(G)$. En conclusion, $\text{Int}(G)$ est un sous-groupe distingué de $\text{Aut}(G)$.
b - Soit l'application $\phi : G \to \text{Int}(G)$, $\phi(g) = \gamma_g$. On a $\phi(gh) = \gamma_{gh} = \gamma_g \circ \gamma_h = \phi(g) \circ \phi(h)$. ϕ est un morphisme surjectif de groupes. D'après le premier théorème d'isomorphisme, on a $G/\text{Ker}\phi \cong \text{Int}(G)$. Soit $g \in G$, alors $g \in \text{Ker}\phi \Leftrightarrow \gamma_g = I_G \Leftrightarrow \forall x \in G, gxg^{-1} = x \Leftrightarrow \forall x \in G, gx = gx \Leftrightarrow g \in Z(G)$.

Exercice 41. Soient G_1 et G_2 deux groupes Si $H_1 \lhd G_1$ et $H_2 \lhd G_2$. Montrer que l'on a : $H_1 \times H_2 \lhd G_1 \times G_2$ et

$$\frac{G_1 \times G_2}{H_1 \times H_2} \cong \frac{G_1}{H_1} \times \frac{G_2}{H_2}$$

Solution. On a un morphisme surjectif de groupes $\psi : G_1 \times G_2 \to\cong \frac{G_1}{H_1} \times \frac{G_2}{H_2}$, défini par $\psi(x_1, x_2) = (\pi_1(x_1), \pi_2(x_2))$, où π_i sont les surjections canoniques correspondantes. Par ailleurs, $(x_1, x_2) \in \text{Ker}\psi \Leftrightarrow x_1 \in H_1 \,\text{et}\, x_2 \in H_2$. Par conséquent, $\text{Ker}\psi = H_1 \times H_2$. Il en résulte que $H_1 \times H_2 \lhd G_1 \times G_2$ et d'après le premier théorème des isomorphismes

$$\frac{G_1 \times G_2}{H_1 \times H_2} \cong \frac{G_1}{H_1} \times \frac{G_2}{H_2}$$

Exercice 42. Soit G un groupe fini d'élément neutre e possèdant un automorphisme σ tel que $\forall x \in g$, $\sigma(x) = x \Rightarrow x = e$. On considère l'application $f : G \to G$; définie par : $f(x) = x^{-1}\sigma(x)$.
1 - Montrer que f est une bijection.
2 - On suppose que $\sigma^2 = I$. Montrer que $\forall x \in G$ on a : $\sigma(x) = x^{-1}$, et en déduire que G est abélien d'ordre impair.

Solution.
1 - Montrons que f est injective. Soient $x, y \in G$ tels que $f(x) = x^{-1}\sigma(x) = f(y) = y^{-1}\sigma(y)$, alors $\sigma(y)\sigma(x)^{-1} = yx^{-1}$. Donc $\sigma(yx^{-1}) = yx^{-1}$. Par hypothèse, e est le seul élment fixé par σ, par conséquent, $yx^{-1} = e$. D'où $x = y$. f est injective. Comme G est fini, f est bijective.
2 - Soit $x \in G$, comme f est bijective, il existe $a \in G$ tel que $x = a^{-1}\sigma a$. On a $\sigma(x) = \sigma(a^{-1})\sigma^2(a) = \sigma(a)^{-1}a = (a^{-1}\sigma(a))^{-1} = x^{-1}$. Donc σ est l'inversion $x \to x^{-1}$. Il en résulte que G est abélien. Par ailleurs $\forall x \in G$, $x \neq e \Rightarrow \sigma(x) = x^{-1} \neq x$. i.e $x^2 \neq e$. par conséquent, G ne possède pas d'élément d'ordre 2. Ce qui entraîne que l'ordre de G est impair.

Exercice 43. Soient les matrices $u = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $v = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ de $\mathrm{GL}_2(\mathbb{R})$.
1 - Déterminer les ordres de u, v et uv.
2 - Soit G le sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ engendré par les éléments u et v. Montrer que G est diédral d'ordre 8.
3 - Soit $w = u^2$. On note $Z(G)$ le centre du groupe G. Montrer que $Z(G) = \{I, w\}$.
4 - Quelle est la nature du groupe quotient $G/Z(G)$?

Solution.
1 - On a $u^2 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$; $u^3 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, ; $u^4 = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = I$. Donc $o(u) = 4$.
$v^2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = I$. Donc $o(v) = 2$.

$uv = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $(uv)^2 = I$. Donc $o(uv) = 2$.
2 - G est engendré par u, v, tels que $o(u) = 4$, $o(v) = 2$, $o(uv) = 2$. Par conséquent, G est un groupe diédral d'ordre 8.
3 - Il suffit de montrer que w commute avec les générateurs de G. Soit $w = u^2$. On a $uw = wu$ et $vwv^{-1} = vwv = vu^2v = vuvvuv = u^{-1}u^{-1} = u^{-2} = u^2 = w$. Donc $vw = wv$. Par conséquent, $w \in Z(G)$.

D'abord tout élément g de G s'écrit $g = u^k v^i$, avec $k = 0, 1, 2, 3$ $m = 0, 1$. Soit $g = u^k v^i \in Z(G)$. Montrons d'abord que $i = 0$. Si $g = u^k v$. On a $ug = u^{k+1}v$ et $gu = u^k vu = u^k u^3 v = u^{k+3}v$. Donc $gu \neq ug$. Par conséquent, $Z(G) \subset \mathrm{gr} < u >$. Soit donc $g = u^k \in Z(G)$. On a $vu^k = u^{4-k}v = u^k v$. Par conséquent $u^{4-2k} = e$, ce qui implique que $4 | 4 - 2k$. Donc $k = 0 \,\mathrm{ou}\, 2$. Finalement, $Z(G) = \{e, u^2\}$.
4 - On a $o(G/Z(G)) = 4$, et $\forall g \in G$, on a : $g^2 \in Z(G)$. Par suite $\bar{g}^2 = \bar{e}$. Par conséquent $G/Z(G)$ est de Klein.

Exercice 44. m et n deux entiers premiers entre-eux.
1 - Montrer que $\mathbb{Z}/n.\mathbb{Z} \times \mathbb{Z}/m.\mathbb{Z} \cong \mathbb{Z}/nm.\mathbb{Z}$.
2 - Montrer que le produit direct de deux groupes cycliques d'ordres premiers entre eux est un groupe cyclique.

Solution. 1 - Soit $\phi : \mathbb{Z} \to \mathbb{Z}/n.\mathbb{Z} \times \mathbb{Z}/m.\mathbb{Z}$, définie par $\phi(x) = (\pi_1(x), \pi_2(x))$, où $\pi_1(x)$ (resp.$\pi_2(x)$ est la classe de x modulo n (res. m). On a ϕ est un morphisme de groupes.

Soit $x \in \mathbb{Z}$. On a $x \in \mathrm{Ker}(\phi) \Leftrightarrow n|x \,\mathrm{et}\, m|x \Leftrightarrow mn|x$, car m et n sont premiers entre eux. Par conséquent, $\mathrm{Ker}\phi = nm\mathbb{Z}$. D'après le premier théorème des isomorphismes on a $\mathbb{Z}/\mathrm{Ker}\phi = \mathbb{Z}/nm\mathbb{Z} \cong \mathrm{Im}\phi$. Or $o(\mathrm{Im}\phi) = o(\mathbb{Z}/nm\mathbb{Z}) = mn = o(\mathbb{Z}/n.\mathbb{Z} \times \mathbb{Z}/m.\mathbb{Z})$. Donc $\mathrm{Im}\phi = \mathbb{Z}/n.\mathbb{Z} \times \mathbb{Z}/m.\mathbb{Z}$.

En conclusion on a l'isomorphisme $\mathbb{Z}/n.\mathbb{Z} \times \mathbb{Z}/m.\mathbb{Z} \cong \mathbb{Z}/nm.\mathbb{Z}$.

2 - Si G_1 et G_2 sont deux groupes cyclique d'ordre respectifs n et m premiers entre eux, on a $G_1 \times G_2 \cong \mathbb{Z}/n.\mathbb{Z} \times \mathbb{Z}/m.\mathbb{Z} \cong \mathbb{Z}/nm.\mathbb{Z}$. Donc $G_1 \times G_2$ est cyclique.

Exercice 45. Soit $(G, \cdot)$ un groupe noté mutiplicativement d'élément neutre noté e. On note $\mathrm{Aut}(G)$ le groupe des automorphismes de G. Un sous-groupe H de G est dit caractéristique dans G, si pour tout automorphisme u de G on a $u(H) \subset H$.
1 - Montrer que tout sous-groupe caractéristique de G est distingué dans G.
2 - Montrer que le centre de G est un sous-groupe caractéristique de G.
3 - On suppose que G possède un seul sous-groupe H d'ordre m. Montrer que H est un sous-groupe caractéristique de G.
4 - On suppose que G est cyclique. Montrer que tout sous-groupe de G est caractéristique.
5 - (Transitivité) Soit N un sous-groupe caractéristique de G et H un sous-groupe caractéristique de N. Montrer

que H est un sous-groupe caractéristique de G.
6 - Soit E un groupe non trivial d'élément neutre e. On considère le groupe produit direct $G = E \times E$. Montrer que $N = E \times \{e\}$ est un sous-groupe distingué dans G mais n'est pas caractéristique.

Solution. 1 - Soit H un sous-groupe caractéristique de G. Pour tout $g \in G$, on a $\gamma_g(H) \subset H$, où γ_g est l'automorphisme intérieur $x \mapsto gxg^{-1}$. Donc $gHg^{-1} \subset H$. Le sous-groupe H est donc distingué dans G.

2 - Soit $z \in Z(G)$ et $u \in \mathrm{Aut}(G)$. Il faut montrer que $u(z) \in Z(G)$. On a : $\forall y \in G, \exists x \in G : y = u(x)$, car u est bijectif. D'où $yu(z) = u(x)u(z) = u(xz)$, car u est un automorphisme. Mais $u(xz) = u(zx)$, car $z \in Z(G)$. Donc $yu(z) = u(zx) = u(z)u(x) = u(z)y$. Par conséquent, $u(z) \in Z(G)$.

3 - Soit H l'unique sous-groupe d'ordre m de G. Pour $u \in \mathrm{Aut}(G)$, $o(u(H)) = o(H) = m$, car u est un automorphisme. Donc $u(H) = H$.

4 - On suppose que G est cyclique engendré par g. Soit H un sous-groupe de G. H est donc engendré par g^k. Pour tout $u \in \mathrm{Aut}(G)$, on a $u(g) = g^m$ car G est cyclique. Il en résulte que pour tout $x = g^{ks} \in H$, on a : $u(x) = u(g^{ks}) = u(g)^{ks} = (g^m)^{ks} = g^{mks} = (g^k)^{ms} \in H$.

5 - Soit N un sous-groupe caractéristique de G et H un sous-groupe caractéristique de N. On a $\forall u \in \mathrm{Aut}(G)$, $u(N) \subset N$. On a aussi $u^{-1}(N) \subset N$. Donc $u(N) = N$. Ainsi la restriction de u à N, $u\mid_N$, est un automorphisme de N. Comme H est un sous-groupe caractéristique de N, on a $u\mid_N (H) = u(H) \subset H$.

6 - Soit E un groupe non trivial d'élément neutre e, et $G = E \times E$ le groupe produit direct.

Montrons que $N = E \times \{e\}$ est un sous-groupe distingué dans G. On a $(e, e) \in N$, et si $(x, e), (y, e) \in N$, on a $(x, e).(y, e)^{-1} = (x, e).(y^{-1}, e) = (xy^{-1}, e) \in N$. Donc N est un sous-groupe de G.

$\forall (a, b) \in G$, $\forall (x, e) \in N$, on a : $(a, b)(x, e)(a, b)^{-1}{=}(a, b)(x, e)(a^{-1}{,}b^{-1})$
$= (axa^{-1}, aea^{-1}) = (axa^{-1}, e) \in N$. Donc N est un sous-groupe distingué de G.

Montrons que N n'est pas caractéristique. Il suffit de prendre $u : G \to G$; $u(x, y) = (y, x)$. u est bien un automorphisme de G. On a $u(N) = \{e\} \times E \not\subset N$.

Exercice 46. 1 - Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 8 & 6 & 4 & 1 & 3 & 7 \end{pmatrix} \in \mathcal{S}_8$. Décomposer σ en produit de cycles disjoints et calculer son ordre et sa signature.

2 - Soit $\phi = (34)(45)(23)(12)(56)(23)(45)(34)(23) \in \mathcal{S}_6$. Calculer ϕ et déterminer son ordre et sa signature.

3 - Soit $\sigma = (1384) \circ (268) \circ (532) \in \mathcal{S}_8$. Décomposer σ en produit de cycles disjoints et calculer son ordre.

4 - Soit $n \in \mathbb{N}^*$. On considère la permutation $\sigma \in \mathcal{S}_n$ définie par $\sigma(k) = n + 1 - k$, $\forall k = 1, \ldots, n$. Calculer la signature de σ.

Solution.
1 - On a $\sigma = (12546)(387)$. Son ordre est le PPCM des longueurs des cycles disjoints qui la composent. Donc $o(\sigma) = \mathrm{PPCM}(5, 3) = 15$.

On a $\sigma = (12)(25)(54)(46)(38)(87)$ est composée d'un nombre pair de transpositions. Donc $\epsilon(\sigma) = 1$.
2 - Soit $\phi = (34)(45)(23)(12)(56)(23)(45)(34)(23) \in \mathcal{S}_6$.

On a $\phi(1) = 4$, $\phi(2) = 6$, $\phi(3) = 2$, $\phi(4) = 1$, $\phi(5) = 5$, $\phi(6) = 3$.

Donc $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 1 & 5 & 3 \end{pmatrix}$
ϕ est le produit d'un nombre impair de transpositions, par suite sa signature est -1.

D'autre part, la décomposition de ϕ en cycles disjoints donne $\phi = (14)(263)$. Il en résulte que $o(\phi) = \text{PPCM}(2,3) = 6$.

3 - Soit $\sigma = (1384) \circ (268) \circ (532) \in \mathcal{S}_8$.

• $\sigma(1) = 3$, $\sigma(3) = 6$, $\sigma(6) = 4$, $\sigma(4) = 1$, Donc σ contient dans sa décomposition le cycle (1364).

• $\sigma(2) = 5$, $\sigma(5) = 8$, $\sigma(8) = 2$. Donc σ contient le cycle (258).

• $\sigma(7) = 7$, 7 est fixe par σ.

Par conséquent, $\sigma = (1364) \circ (258)$. Son ordre est donc 12.

4 - $\sigma \in \mathcal{S}_n$ est définie par $\sigma(k) = n+1-k$, $\forall k = 1, \ldots, n$. On a :

• Si $n = 2k$ est pair, $\sigma = (1\, n)(2\, n-1) \ldots (k\, k+1)$, donc $\epsilon(\sigma) = (-1)^k$.

• Si $n = 2k+1$ est impair, $\sigma = (1\, n)(2\, n-1) \ldots (k\, k+2)$, donc $\epsilon(\sigma) = (-1)^k$. (Noter que dans ce cas là, $k+1$ est fixé par σ)

Ainsi,
– si $n \equiv 0$ ou $1 \pmod 4$, σ est paire,
– si $n \equiv 2$ ou $3 \pmod 4$, σ est impaire.

Exercice 47. Soit $\sigma \in \mathcal{S}_n$ d'ordre un nombre premier $p \nmid n$. Montrer que σ possède au moins un point fixe.

Solution. Nous allons montrer que si σ ne possède pas de point fixe, alors $p \mid n$. Soient $\Omega_1, \ldots, \Omega_k$, les orbites suivant σ. L'ordre de σ est le PPCM des longueurs (cardinaux) de ses orbites. On a $\sum_{i=1}^{k} \text{card}(\Omega_i) = n$, car les orbites forment une partition de l'ensemble $\{1, \ldots, n\}$. Supposons que σ ne possède pas de point fixe. Cela veut dire que toutes les orbites ont un cardinal > 1. Comme le cardinal de l'orbite divise $o(\sigma) = p$, par conséquent, $\text{card}\Omega_i = p$, $\forall i = 1, \ldots, k$. Il s'ensuit que $n = kp$. i.e $p \mid n$.

Exercice 48. Déterminer les différents ordres que peut avoir une permutation de $\mathcal{S}_8$. Quel est l'ordre maximal d'une telle permutation ?

Solution. Une permutation σ se decompose en produit $c_1 c_2 \ldots c_k$ de cycles deux à deux disjoints. L'ordre de σ est le PPCM des longueurs de ces cycles qui sont comprises entre 2 et 8. Donc $k \leq 4$. Notons $(l_1, l_2, \ldots, l_k)$, $k \leq 4$, les longueurs des cycles qui composent σ. On peut supposer que $l_1 \geq l_2 \geq \ldots_k \geq 2$. On a $l_1 + \ldots + l_k \leq 8$. Les différentes possiblités sont alors :

Forme de la décomposition $(l_1, l_2 \dots, l_k)$	ordre $=$ PPCM$(l_1, l_2 \dots, l_k)$
(8)	8
(7)	7
$(6,2)$	6
(6)	6
$(5,3)$	15
$(5,2)$	10
(5)	5
$(4,4)$	4
$(4,3)$	12
$(4,2,2)$	4
$(4,2)$	4
$(3,3,2)$	3
$(3,3)$	3
$(3,2,2)$	6
$(3,2)$	6
$(2,2,2,2)$	2
$(2,2,2)$	2
$(2,2)$	2
(2)	2

Les différents ordres possibles d'un élément de $\mathcal{S}_8$ sont 1,2,3,4,5,6,7,8,10,
12,15. Le maximum est donc 15.

Exercice 49. Soient $n \in \mathbb{N}^*$, $\sigma \in \mathcal{S}_n$ et $c = (i_1 i_2 \dots i_k)$ un k-cycle de $\mathcal{S}_n$.
1 - Montrer que $\sigma \circ c \circ \sigma^{-1} = (\sigma(i_1)\sigma(i_2)\dots\sigma(i_k))$.
2 - Soit $\tau = (jm)$ une transposition. Calculer $\sigma \circ \tau \circ \sigma^{-1}$
3 - On note $C_\tau = \{\sigma \in \mathcal{S}_n : \sigma \circ \tau = \tau \circ \sigma\}$, le centralisateur de la transposition $\tau = (jm)$ dans $\mathcal{S}_n$. Montrer que $C_\tau = \{\sigma \in \mathcal{S}_n : \{\sigma(j), \sigma(m)\} = \{j\ , m\}\}$.
4 - Déduire de la question 3, que pour $n \geq 3$, le centre de $\mathcal{S}_n$ est réduit à $\{I\}$.

Solution.
1 - Montrons que $\sigma \circ c \circ \sigma^{-1}$ est égale au cycle $(\sigma(i_1)\sigma(i_2)\dots\sigma(i_k))$. Posons $\rho = \sigma \circ c \circ \sigma^{-1}$. Pour $s = 1, 2, \dots, k-1$, on a : $\rho(\sigma(i_s)) = \sigma \circ c \circ \sigma^{-1}(\sigma(i_s)) = \sigma \circ c(i_s) = \sigma(i_{s+1})$. De même, $\rho(\sigma(i_k)) = \sigma \circ c(i_k) = \sigma(i_1)$. Par ailleurs, si $m \notin \{\sigma(i_1)\sigma(i_2)\dots\sigma(i_k)\}$, on a $\sigma^{-1}(m) \notin \{i_1, i_2, \dots, i_k\}$. Par conséquent, $c(\sigma^{-1}(m)) = \sigma^{-1}(m)$ et $\sigma \circ c \circ \sigma^{-1}(m) = \sigma(\sigma^{-1}(m)) = m$. En conclusion, $\sigma \circ c \circ \sigma^{-1}$ est le cycle $(\sigma(i_1)\sigma(i_2)\dots\sigma(i_k))$.
2 - En utilisant 1, on a : $\sigma \circ (jm) \circ \sigma^{-1} = (\sigma(j)\sigma(m))$.
3 - On a : $C_\tau = \{\sigma \in \mathcal{S}_n : \sigma \circ \tau = \tau \circ \sigma\} = C_\tau = \{\sigma \in \mathcal{S}_n : \sigma \circ \tau \circ \sigma^{-1} = \tau\} = \{\sigma \in \mathcal{S}_n : (\sigma(j)\sigma(m)) = (jm)\} = \{\sigma \in \mathcal{S}_n : \{\sigma(j), \sigma(m)\} = \{j, m\}\}$.
4 - On a I est un élément du centre de $\mathcal{S}_n$. Nous allons montrer que I est le seul élément du centre $Z(\mathcal{S}_n)$ de $\mathcal{S}_n$. Soit $\sigma \neq I$. Montrons que $\sigma \notin Z(\mathcal{S}_n)$. Comme $\sigma \neq I$, il existe $i \in \{1, 2, \dots n\}$, tel que $\sigma(i) = j \neq i$. Puisque $n \geq 3$, il existe $m \in \{1, 2, \dots n\}$, tel que $m \neq i$ et $m \neq j$. Notons τ la transposition (im), on a $\{\sigma(i), \sigma(m))\} = \{j, \sigma(m)\} \neq \{i, m\}$, car $j \neq i$ et $j \neq m$. Par conséquent, $\sigma \notin C_\tau$ (d'après 3). D'où $\sigma \notin \mathrm{Z}(\mathcal{S}_n)$.

Exercice 50. Soit n un entier naturel ≥ 3.
1 - Montrer que le produit de deux transpositions de $\mathcal{S}_n$ est un 3-cycle ou un produit de deux 3-cycles. En déduire que $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles.
2 - Calculer $(12i)(2jk)(12i)^{-1}$, $(12j)(12k)(12j)^{-1}$. En déduire que $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles de la forme $(123), (124), \dots (12n)$.
3 - Soit H un sous-groupe distingué de $\mathcal{A}_n$. Montrer que si H contient un 3-cycle, alors $H = \mathcal{A}_n$.
4 - Dans la suite on prend $n = 4$.
4.1. On note E l'ensemble des 3-cycles de $\mathcal{A}_4$, déterminer E et vérifier que card$(E) = 8$.
4.2. On suppose que $\mathcal{A}_4$ contient un sous-groupe H d'ordre 6, Montrer que H est distingué dans $\mathcal{A}_4$ et que H contient contient tous les 3-cycles de $\mathcal{A}_4$. Conclure à une contradiction et que $\mathcal{A}_4$ ne contient pas de sous-groupe d'ordre 6.
4.3. Donner la liste de tous les sous-groupes de $\mathcal{A}_4$, vérifier qu'il contient un sous-groupe distingué isomorphe

au groupe de Klein.
4.4. Montrer que $\mathcal{A}_4$ n'est pas diédral.

Solution. 1 - Soient $(ij),(kl)$ deux transpositions distinctes.

• Si $\{i,j\}\cap\{k,l\}=\varnothing$, on a $(ij)(kl)=(ij)(jk)(jk)(kl)=(ijk)(jkl)$.

• Si $\{i,j\}\cap\{k,l\}\neq\varnothing$, on a par exemple $j=k$, alors $(ij)(kl)=(ij)(jl)=(ijl)$.

Puisque $\mathcal{A}_n$ est engendré par l'ensemble des produits de deux transpositions, et que chaque produit de deux transpositions est un 3-cycle ou un produit de deux 3-cycles, il en résulte que $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles.
2 - Remarquons d'abord que $(ijk)^{-1}=(ikj)$. On a $(12i)(2jk)(12i)^{-1}=(12i)(2jk)(1i2)=(ijk)$, $(12j)(12k)(12j)^{-1}=(12j)(12k)(1j2)=(2jk)$. Par conséquent on a $(ijk)=(12i)(2jk)(12i)^{-1}=(12i)(12j)(12k)(12j)^{-1}(12i)^{-1}$. Il en résulte que $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles de la forme $(123),(124),\dots(12n)$.
3 - Soit H un sous-groupe distingué de $\mathcal{A}_n$. On suppose que H contient un 3-cycle. Montrons que $H=\mathcal{A}_n$. Il suffit de montrer, d'après 2, que H contient tous les 3-cycles du type $(12l)$.
Soit $l\geq 3$ et $(ijk)\in H$, alors $(1i)(2j)(1kl)(ijk)(1kl)^{-1}(2j)(1i)=(12l)\in H$, car $H\lhd\mathcal{A}_n$.
4 - 4.1. On a $E=\{(123),(132),(124),(142),(134),(143),(234),(243)\}$, qui est de cardinal 8.
4.2. Supposons que $\mathcal{A}_4$ contient un sous-groupe H d'ordre 6. On a $H\cap E\neq\varnothing$ (sinon, $\operatorname{card}(H\cup E)=14>|\mathcal{A}_4|$). Donc H contient un 3-cycle. Or $[\mathcal{A}_n:H]=\frac{12}{6}=2$, par suite $H\lhd\mathcal{A}_4$. Ce qui implique, d'après 3, que $H=\mathcal{A}_4$, ce qui est absurde.
Autre démonstration : Soit H un sous-groupe d'ordre 6 de $\mathcal{A}_4$. Puisque H est d'indice 2, on a $\forall\sigma\in\mathcal{A}_4$, $\sigma^2\in H$. Soit donc σ un 3-cycle quelconque. On a $\sigma^3=1$, par suite $\sigma^{-1}=\sigma^2\in H$. D'où $\sigma\in H$, H contient tous les 3-cycles, absurde.
5 - En utilisant la décomposition en cycles disjoints, il est facile de voir que les seuls ordre possibles des éléments de $\mathcal{A}_4$ sont $1,2,3$.
• Les éléments d'ordre 2 sont les produits de transpositions disjointes :
$(12)(34),(13)(24),(14)(23)$.
• Les éléments d'ordre 3 sont les 3-cycles :
$(123),(132),(124),(142),(134),(143),(234),(243)$.
Les sous-groupes de $\mathcal{A}_4$ sont alors :
• Ordre 1 : $\{I\}$,
• Ordre 2 : $\{I,(12)(34)\},\{I,(13)(24)\},\{I,(14)(23)\}$,
• Ordre 3 : $\{I,(123),(132)\},\{I,(124),(142)\},\{I,(134),(143)\},\{I,(234),(243)\}$,
• Ordre 4 : $\{I,((12)(34),(13)(24),(14)(23)\}$,
• Ordre 12 : $\mathcal{A}_4$.
L'ensemble $V=\{I,((12)(34),(13)(24),(14)(23)\}$ est un sous-groupe d'ordre 4 non cyclique de $\mathcal{A}_4$, il est isomorphe au group de Klein. Par ailleurs $V=\{\sigma\in\mathcal{A}_4:\sigma^2=I\}$. Si $\rho\in\mathcal{A}_4$ et $\sigma\in V$, $(\rho\sigma\rho^{-1})^2=\rho\sigma^2\rho^{-1}=I$. Donc $\rho\sigma\rho^{-1}\in V$. Par suite $V\lhd\mathcal{A}_4$.
6 - Le groupe diédral d'ordre 12 est engendré par un élément d'ordre 6 et un élément d'ordre 2. Donc contient un sous-groupe d'ordre 6, ce n'est pas le cas pour $\mathcal{A}_4$. Donc $\mathcal{A}_4$ n'est pas diédral.

Exercice 51. Soit n un entier naturel supérieur ou égal à 2. On considère $\mathcal{S}_n$ le groupe symétrique des permutations de l'ensemble $\{1,2,\dots,n\}$. Pour tout $i\neq j$, des entiers apppartenant à $\{1,2,\dots,n\}$, on note (ij) la transposition $i\to j$ et $j\to i$.
1 - Calculer le produit $(1i)(1j)(1i)$ et montrer que $\mathcal{S}_n$ est engendré par l'ensemble $\{(12),(13),\dots(1n)\}$.
2 - Calculer $(k\ k+1)(1k)(k\ k+1)$. En déduire, par récurrence sur k, que $\mathcal{S}_n$ est engendré par l'ensemble $\{(12),(23),\dots(i\ i+1),\dots,(n-1\ n)\}$.
3 - Soient c le cycle $(12\dots n)$ et τ la transposition (12). Calculer $c^i\tau c^{-i}$, pour tout $i\in\{0,1,2,\dots,n-1\}$. En déduire que $\mathcal{S}_n$ est engendré par $\{\tau,c\}$.

Dans la suite, on suppose que $n=p$ est un nombre premier.

4 - Montrer que tout élément d'ordre p de $\mathcal{S}_p$ est un p-cycle.
5 - Soit H un sous-groupe de $\mathcal{S}_p$ contenant le cycle $c=(12\dots p)$ et une transposition de la forme $(1i)$.
a - Montrer que c^{i-1} est un p-cycle et qu'il existe une permutation ρ telle que $\rho c^{i-1}\rho^{-1}=c$ et que $\rho(1i)\rho^{-1}=$

(12).
b - Déduire de a) que $H = \mathcal{S}_p$.
6 - Montrer que $\mathcal{S}_p$ est engendré par un p-cycle σ et une transposition θ quelconques.
(Indication : Si H est un sous-groupe contenant σ et θ, montrer qu'il existe une permutation π telle que $\pi H \pi^{-1}$ contient le cycle $c = (12\dots p)$ et une transposition de la forme $(1i)$).
7 - Le résultat de la question 6, reste - il valable si n n'est pas premier ? (Indication : prendre $n = 4$, $\rho = (1234)$ et θ une transposition autre que (12)).

Solution.
1 - $(1i)(1j)(1i) = (ij)$. Comme $\mathcal{S}_n$ est engendré par l'ensemble des transpositions et que chaque transposition est le produit de transpositions d la forme $(1i)$, il en résulte que $\mathcal{S}_n$ est engendré par l'ensemble $\{(12), (13), \dots (1n)\}$.
2 - $(k\ k+1)(1k)(k\ k+1) = (1\ k+1)$. Par récurrence on a :
$(1k) = (k-1\ k)(k-2\ k-1)\dots(23)(12)(23)\dots(k-2\ k-1)(k-1\ k)$.
Donc toute transposition $(1i)$ de $\mathcal{S}_n$ est le produit de transpositions de la forme $(k\ k+1)$. Par conséquent le groupe $\mathcal{S}_n$ est engendré par l'ensemble des transpositions $\{(12), (23), \dots (i\ i+1), \dots, (n-1\ n)\}$.
3 - Soient c le cycle $(12\dots n)$ et τ la transposition (12). On a $c^i \tau c^{-i} = (i+1\ i+2)$, pour tout $i \in \{0, 1, 2, \dots, n-2\}$. Il en résulte que $\mathcal{S}_n$ est engendré par $\{\tau, c\}$.
4 - Soit σ un élément d'ordre p de $\mathcal{S}_p$. $\sigma = c_1 \circ c_2 \circ \dots \circ c_k$, où les c_i sont des cycles disjoints. Comme $o(c_i) \mid o(\sigma)$, on a $o(c_i) = p$. La longueur de chaque c_i est donc égale à p. Par suite, $k = 1$ et $\sigma = c$ est un p-cycle.
5 - a - On a $(c^{i-1})^p = I$. Si $(c^{i-1})^k = c^{k(i-1)} = I$, alors $p \mid k(i-1)$. Comme $1 < i \leq p$, on a $0 < i-1 \leq p-1$. Ce qui entraîne que $p \mid k$. Donc $o(c^{i-1}) = p$. D'après 4, c^{i-1} est un p-cycle.
On a $c^{i-1} = (1\, i j_3 \dots j_p)$. Soit la permutation ρ définie par $\rho(1) = 1$, $\rho(i) = 2$, $\rho(j_k) = k$, pour $k = 3, \dots, p$. Alors on a : $\rho c^{i-1} \rho^{-1} = \rho(1 i j_3 \dots j_p)\rho^{-1} = (123\dots p) = c$ et $\rho(1i)\rho^{-1} = (12)$.
b - On a $\rho H \rho^{-1}$ est un sous-groupe de $\mathcal{S}_p$ qui contient le cycle $c = (12\dots p)$ et la transposition (12). Donc, d'après 3, $\rho H \rho^{-1} = \mathcal{S}_p$. Ce qui implique que $H = \mathcal{S}_p$.
6 - Soit H est un sous-groupe contenant un cycle $\sigma = (i_1 i_2 \dots i_p)$ et une transposition $\theta = (kl)$ quelconques. Soit π la permutation défine par $\pi^{-1}(m) = i_m$. Alors $\pi\sigma\pi^{-1} = c$. Soit $t = \pi^{-1}(1)$, puisque σ est un p-cycle, il existe s tel que $\sigma^s(k) = t$. Alors $\pi\sigma^s(kl)\sigma^{-s}\pi^{-1} = (\pi\sigma^s(k)\ \pi\sigma^s(l)) = (1l')$. Donc $\pi H \pi^{-1}$ contient le cycle $c = (12\dots p)$ et une transposition de la forme $(1l')$. Ce qui implique d'après 6, que $\pi H \pi^{-1} = \mathcal{S}_p$. Donc $H = \mathcal{S}_p$.
7 - Si on prend $n = 4$, $\rho = (1234)$ et $\theta = (13)$, on a : $o(\rho) = 4$, $o(\theta) = 2$, $\rho \circ \theta = (14)(23)$, par suite $o(\rho \circ \theta) = 2$. Le groupe engendré par ρ et θ est le groupe diédral d'ordre 8, alors que l'ordre de $\mathcal{S}_4$ est 24.

Exercice 52. Soit $(G, \cdot)$ un groupe d'élément neutre e, $G \neq \{e\}$, et dont les seuls sous-groupes sont $\{e\}$ et G.
1 - Montrer que G est monogène.
2 - Montrer que G est cyclique.
3 - Montrer que l'ordre de G est un nombre premier.

Solution.
1 - Soit $g \in G$, tel que $g \neq e$. H le sous-groupe de G engendré par g. Puisque $H \neq \{e\}$, on a : $H = G$. Donc G est monogène.
2 - Montrons que g est d'ordre fini. Si $g^2 = e$, c'est vrai. Sinon, $g^2 \neq e$ et $gr\langle g^2 \rangle = G$. Il en résulte que $g \in gr\langle g^2 \rangle$, ou encore $g = (g^2)^k = g^{2k}$, il s'ensuit que $g^{2k-1} = e$. G est fini.
3 - Notons n l'ordre de G et $G = gr <g>$. Soit k un entier tel que $1 < k < n$ divisant n. On a $g^k \neq e$, d'où $gr\langle g^k \rangle = G$. Par suite, $g = (g^k)^m = g^{km}$, d'où $g^{km-1} = e$. Ou encore $n \mid km-1$, il en résulte que $n \wedge k = 1$ et par suite, n est un nombre premier.

Exercice 53. Dans tout ce problème, $(G, \cdot)$ désigne un groupe fini d'ordre n et d'élément neutre noté e. On pose $G = \{x_1, x_2, \dots, x_n\}$. Pour tout $g \in G$, on considère l'application $\sigma_g : \{1, \dots, n\} \to \{1, \dots, n\}$, définie par $\sigma_g(i) = j \Leftrightarrow g x_i = x_j$.
1 - Montrer que $\sigma_g \in \mathcal{S}_n$.
2 - Montrer que l'application $\phi : G \to \mathcal{S}_n$, définie par $\phi(g) = \sigma_g$, est un morphisme injectif de groupes.
3 - On note ϵ le morphisme signature $\epsilon : \mathcal{S}_n \to (\{-1, 1\}, \times)$. On suppose que G est d'ordre $2m$ avec m un entier impair. Montrer que le morphisme $\epsilon \circ \phi$ est surjectif et en déduire que G contient un sous-groupe distingué d'ordre m.

Solution.
1 - σ_g est une application de $\{1, \dots, n\}$ dans lui même. Il suffit de montrer qu'elle est injective. Soit i, j tels que $\sigma_g(i) = \sigma_g(j)$. Alors $g x_i = g x_j$. Mais G est un groupe, donc $x_i = x_j$. Par suite $i = j$.
2 - Posons $\phi(gh)(i) = j$, $\phi(h)(i) = k$. On a alors $ghx_i = x_j$ et $hx_i = x_k$. Il en résulte que $gx_k = ghx_i = x_j$.

Donc $\phi(g)(\phi(h)(i)) = \phi(g) \circ \phi(h)(i) = j$. Par conséquent $\phi(gh) = \phi(g) \circ \phi(h)$. ϕ est donc un morphisme.
3 - $f = \epsilon \circ \phi$ est un morphisme de G dans $(\{-1, 1\}, \times)$. Montrons qu'il est surjectif. Il suffit de montrer l'existence de $g \in G$, tel que $\epsilon \circ \phi(g) = -1$. Ensuite, puisque $2 \mid |G|$, on a d'après le théorème de Cauchy, G contient un élément a d'ordre 2. Si $\phi(a)(i) = j$, on a $i \neq j$ et $\phi(a)(j) = i$. Il en résulte que toutes les orbites de $\phi(a)$ sont de cardinal 2. G est alors une réunion de m orbites de cardinal 2. Donc $\epsilon(\phi(a)) = (-1)^{n-m} = (-1)^m = -1$, car m est impair. par conséquent, f est surjectif. D'après le premier théorème des isomorphismes, on a $G/\mathrm{Ker}f \cong \mathrm{Im}f = \{-1, 1\}$. D'où Ker$f$ est un sous-groupe distingué d'indice 2, donc d'ordre m.

Exercice 54. Soit H un sous-groupe d'indice 2 de $\mathcal{S}_n$. Montrer que $H = \mathcal{A}_n$.

Solution. On a H est distingué dans $\mathcal{S}_n$ et $\forall \sigma \in \mathcal{S}_n$, on a $\sigma^2 \in H$. Soit (ijk) un 3-cycle quelconque. On a $(ijk)^4 = (ijk) \in H$. Donc H contient tous les 3-cycle. Il en résulte que $\mathcal{A}_n \subset H$. Or $[\mathcal{S}_n : \mathcal{A}_n] = 2 = [\mathcal{S}_n : H][H : \mathcal{A}_n]$, par conséquent, $[H : \mathcal{A}_n] = 1$. D'où $H = \mathcal{A}_n$.

Exercice 55. Soit G un groupe et H un sous-groupe de G. On note E l'ensemble quotient à gauche de G modulo H, i.e $E = (G/H)_g = \{xH : x \in G\}$. On note $\mathcal{B}(E)$ le groupe des bijection de E.
Pour tout $a \in G$, on définit l'application $\rho_a : E \to E$, par $\rho_a(xH) = axH$.
1 - Montrer que ρ_a est bien définie et que $\rho_a \in \mathcal{B}(E)$.
2 - Montrer que G l'application $\Phi : G \to \mathcal{B}(E)$, $a \mapsto \rho_a$ est un morphisme de groupes
Dans la suite on notera N le noyau de ce morphisme.
3 - Montrer que G/N est isomorphe à un sous-groupe de $\mathcal{B}(E)$.
4 - Montrer que N est le plus grand sous-groupe distingué de G contenu dans H.
5 - On suppose que H est d'indice fini m.
a - Montrer que $[H : N]$ divise $(m - 1)!$.
b - On suppose de plus que m est le plus petit nombre premier qui divise $|G|$. Montrer que H est distingué dans G.

Solution.
1 - Soit $a \in G$, si $xH = yH$, alors $x^{-1}y \in H$, par conséquent $(ax)^{-1}(ay) = x^{-1}a^{-1}ay = x^{-1}y \in H$. Donc $axH = ayH$. Par conséquent, ρ_a est bien définie.
On considère l'application $G \times E \to E$; $(g, xH) \mapsto gxH$. Il est clair que c'est une opération de G sur E.
Soit xH et yH tels que $\rho_a(xH) = \rho_a(yH)$. Alors $axH = ayH$ par suite, $(ax)^{-1}(ay) \in H$. Or $(ax)^{-1}(ay) = x^{-1}y$. Donc $xH = yH$, ce qui implique que ρ_a est injective.
Soit $yH \in E$, alors $\rho_a(a^{-1}yH) = yH$. D'où ρ_a est surjective.
Conclusion : ρ_a est une bijection de E.
2 - $\forall a, b, x \in G$, on a $\rho_{ab}(xH) = abxH = \rho_a(\rho_b(xH))$, donc $\rho_{ab} = \rho_a \circ \rho_b$. D'où$\Phi(ab) = \Phi(a) \circ \Phi(b)$. Φ est donc un morphisme de groupes. D'après le premier théorème des isomorphismes on a : $G/\mathrm{Ker}\Phi \cong \mathrm{Im}\Phi$, qui est un sous-groupe de $\mathcal{B}(E)$. Donc G/N est isomorphe à un sous-groupe de $\mathcal{B}(E)$.
3 - Evidemment, puisque N est le noyau d'un morphisme, c'st un sous-groupe distingué de G. Soit $g \in N$, on a $gxH = H$, pour tout $x \in G$. En prenant $x = e$, on obtient $gH = H$. par conséquent, $g \in H$. D'où $N \subset H$.
Soit maintenant un K sous-groupe distingué de G contenu dans H. Montrons que $K \subset N$. Soit $g \in K$ et $x \in G$. On a : $K \lhd G$, donc $x^{-1}gx \in K$. Par conséquent puisque $K \subset H$, on a $x^{-1}gxH = H$. Donc $gxH = xH$. Il en résulte que $g \in N$.
4 - a - On a G/N est isomorphe à un sous-groupe de $\mathcal{B}(E)$. Comme card$E = [G : H]$, on a $\mathcal{B}(E) \cong \mathcal{S}_m$, le groupe symétrique. D'où $|G/N| = [G : N] = [G : H][H : N] \mid m!$. Il en résulte que $[H : N] \mid (m-1)!$.
b - Montrons que $[H : N] = 1$. Sinon, il existe un nombre premier p qui divise $[H : N]$. Donc $p \mid (m-1)!$. Comme p st premier, il divise alors l'un des $k = 1, \ldots, m-1$. Il en résulte que $p \leq m - 1 < m$. Mais p divise $|G|$, donc $p \geq m$, puisque que m est le plus petit nombre premier qui divise $|G|$. Contradiction.

Exercice 56. (Cet exercice utilise le théorème de Cauchy général).
Soit G un groupe d'ordre pq, où p et q sont des nombres premiers tels que $p < q$.
1 - Montrer que G contient un sous-groupe H d'ordre p et un sous-groupe N d'ordre q.
2 - On suppose que G est abelien. Montrer que G est cyclique.
3 - On suppose que G n'est pas abélien. On pose H le sous-groupe d'ordre p et N un sous-groupe d'ordre q, alors $N \lhd G$ et $G = NH$, de plus N est l'unique sous-groupe d'ordre q de G.
(Indication : utiliser l'exercice 55. 4-b)
4 - Montrer que tout groupe d'ordre $2q$, avec q un nombre premier $\neq 2$, est ou bien cyclique ou bien diédral.

Solution. 1 - Puisque p et q sont des nombres premiers qui divisent l'ordre de G, alors d'après le théorème de Cauchy, G contient un élément a d'ordre q et un élément b d'ordre p. On pose $N = gr\langle a \rangle$ et $H = gr\langle b \rangle$

2 - Si G est abélien, alors HN est un sous-groupe de G et $|HN| = |H||N|/|H \cap N|$. Puisque $|H|$ et $|N|$ sont premiers entre-eux, on a $H \cap N = \{e\}$, donc $|HN| = |H||N| = pq = |G|$. D'où $G = HN \cong H \times N$ est produit direct de deux groupes cycliques d'ordres premiers entre-eux, donc G est cyclique. (voir Exercice 44).
3 - Le sous-groupe N est d'indice p qui est le plus petit premier divisant l'ordre de G. D'après l'exercice 55. 4-b, N est distingué dans G et on a, comme dans la question 2, $G = HN$.
4 - On prend ici $p = 2$. Si G est abélien, alors il est cyclique d'après les résultats de la question 2. Si G n'est pas abélien, on a $G = HN = gr\langle a, b\rangle$ avec $o(a) = q$, $o(b) = 2$. Montrons que $(ab)^2 = abab = e$, i.e $bab = a^{-1}$. En effet, puisque $N \lhd G$, on a $bab = bab^{-1} = a^k \in N$, et $a = bbabb = ba^kb = (bab)^k = (a^k)^k = a^{k^2}$. Ce qui implique que $a^{k^2-1} = e$. D'où $q \mid k^2 - 1 = (k-1)(k+1)$. Ou encore, puisque q est premier, $q \mid k-1$ ou $q \mid k+1$. Or $k \in \{0, 1, 2 \dots q-1\}$, donc $k = 1$, ou $k = p-1$. Comme $k = 1$ entraîne $ab = ba$ et que G est abélien, on a $k = p-1$. i.e. $bab = a^{p-1} = a^{-1}$. G est donc diédral.

Exercice 57. On note $\mathcal{M}_2(\mathbb{Z})$ l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients dans l'anneau $\mathbb{Z}$ des entiers relatifs.
1 - On note $\mathrm{GL}_2(\mathbb{Z})$, l'ensemble des éléments inversibles du monoïde $(\mathcal{M}_2(\mathbb{Z}), \times)$. Montrer que $(\mathrm{GL}_2(\mathbb{Z}), \times)$ est un groupe.
2 - Soit $A \in \mathcal{M}_2(\mathbb{Z})$. Montrer que $A \in \mathrm{GL}_2(\mathbb{Z})$, si et seulement si, $|\det(A)| = 1$.
3 - On pose $SL_2(\mathbb{Z}) = \{A \in \mathcal{M}_2(\mathbb{Z}) : \det(A) = 1\}$. Montrer que $SL_2(\mathbb{Z})$ est un sous-groupe distingué de $\mathrm{GL}_2(\mathbb{Z})$.
4 - Déterminer l'ensemble des couples $(c, d) \in \mathbb{Z} \times \mathbb{Z}$, tels que $\left(\begin{smallmatrix} 3 & 5 \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$
5 - On se propose de déterminer les ordres des matrices d'ordre fini de $GL_2(\mathbb{Z})$. Soit donc $A \in GL_2(\mathbb{Z})$ d'ordre fini. On note m l'ordre de A. Soit $z \in \mathbb{C}$ une valeur propre de A.

5.1 Montrer que A est diagonalisable dans $\mathcal{M}_2(\mathbb{C})$.

5.2 Montrer que $z^m = 1$. On posera alors $z = \cos(\theta) + i\sin(\theta)$, $\theta \in [0, 2\pi]$

5.3 On suppose que $m \geq 3$, montrer que $z \notin \mathbb{R}$ et que $2\cos(\theta) \in \mathbb{Z}$.

5.4 En déduire que si $m \geq 3$, $\cos(\theta) \in \{-\frac{1}{2}, 0, \frac{1}{2}\}$

6 - Déduire de ce qui précéde que $m \in \{1, 2, 3, 4, 6\}$, et pour chaque m, donner le polynôme caractéristique de A.
7 - Montrer que si A est d'ordre ≥ 3, alors $A \in SL_2(\mathbb{Z})$.
8 - Donner un élément d'ordre 6 de $SL_2(\mathbb{Z})$

Solution. 1 - $\mathrm{GL}_2(\mathbb{Z})$, l'ensemble des éléments inversibles d'un monoïde, donc c'est un groupe.
2 - Soit $A \in \mathcal{M}_2(\mathbb{Z})$. Supposons que $A \in \mathrm{GL}_2(\mathbb{Z})$. Alors il existe $B \in \mathcal{M}_2(\mathbb{Z})$ telle que $AB = I_2$. On a alors $det(AB) = det(I_2) = det(A)det(B) = 1$. Comme $det(A), det(b) \in \mathbb{Z}$, on a $|\det(A)| = 1$.
3 - L'application déterminant $(GL_2(\mathbb{Z}), \times) \to (\{-1, 1\}, \times)$, $A \mapsto det(A)$, est un morphisme de groupes, dont le noyau est $\{A \in GL_2(\mathbb{Z}) : det(A) = 1\} = SL_2(\mathbb{Z})$, c'est donc un sous-groupe distingué de $GL_2(\mathbb{Z})$.
4 - $A = \left(\begin{smallmatrix} 3 & 5 \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \Leftrightarrow 3d - 5c = 1$. Une solution particulière est donnée par $d = 2$ et $c = 1$. Donc $3(d-2) = 5(c-1)$. Comme 3 et 5 sont premiers entre eux, on a $3 \mid c-1$ et $5 \mid d-2$, ce qui implique : $c = 3k+1$ et $d = 5k+2$, $k \in \mathbb{Z}$. D'où $A = \left(\begin{smallmatrix} 3 & 5 \\ 3k+1 & 5k+2 \end{smallmatrix}\right), k \in \mathbb{Z}$.
5- 5.1. Puisque $A^m = I_2$, on a $P(A) = 0$, où $P = X^m - 1$. Comme A est annulée par un polynôme P dont les racines sont simples dans $\mathbb{C}$, A est diagonalisable $\mathcal{M}_2(\mathbb{C})$.
5.2. Puisque z est valeure propre de A et que $A^m = I_2$, on a $z^m = 1$.
5.3. Supposons que $m \geq 3$, alors z est d'ordre ≥ 3. Par conséquent, $z \notin \mathbb{R}$. Il en résulte que , $\bar{z} \neq z$ est aussi valeur propre de A et que A est semblable à $\left(\begin{smallmatrix} z & 0 \\ 0 & \bar{z} \end{smallmatrix}\right)$, dans $\mathcal{M}_2(\mathbb{C})$. Le polynôme caractéristique de A est alors $X^2 - 2\Re(z)X + 1$. Comme ce polynôme caractéristique est à coefficients dans $\mathbb{Z}$, on a $2\Re(z) = 2cos(\theta) \in \mathbb{Z}$.
5.4. On a $2\cos(\theta) \in \mathbb{Z}$, comme $\cos(\theta) \in [-1, 1]$, alors $2\cos(\theta) \in [-2, 2]$. Il en résulte que $\cos(\theta) \in \{-1, -\dfrac{1}{2}, 0, \dfrac{1}{2}, 1\}$.
6 - Si $m = 1$, on a $A = I_2$. Le polynôme caractéristique est $P_A = X^2 - 2X + 1$.
Si $m = 2$, deux cas possibles :
$A = -I_2$, $P_A = X^2 + 2X + 1$
ou A est semblable à $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $P_A = X^2 - 1$.
- Si $m = 3$, $o(z) = 3$, les valeurs propres sont $z = j = e^{\frac{2i\pi}{3}} = -\dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$ et $\bar{j}$. A est semblable à $\left(\begin{smallmatrix} j & 0 \\ 0 & \bar{j} \end{smallmatrix}\right)$, $P_A = X^2 + X + 1$.
- Si $m = 4$, $o(z) = 4$, les valeurs propres sont $z = i$, et $\bar{z} = -i$. A est semblable à $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$, $P_A = X^2 + 1$.
- Si $m = 6$, $o(z) = 6$, les valeurs propres sont $z = -j = e^{\frac{2i\pi}{6}} = \dfrac{1}{2} - i\dfrac{\sqrt{3}}{2}$ et $-\bar{j}$. A est semblable à $\left(\begin{smallmatrix} -j & 0 \\ 0 & -\bar{j} \end{smallmatrix}\right)$,

$P_A = X^2 - X + 1$.
7 - Si $m \geq 3$, les valeurs propres de A sont z et $\bar{z}$ complexes non réelles. On a $\det A = z\bar{z} = |z|^2 = 1$, car z est une racine de l'unité.
8 - On cherche une matrice A à coefficients entier dont le polynôme caractéristique est $X^2 - X + 1$. $A = \left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ est une telle matrice.

Exercice 58. $(G, \cdot)$ un groupe abélien d'élément neutre e. Pour tout $s \in \mathbb{N}$, on pose $G_s = \{x \in G : x^s = e\}$.
1 - Montrer que G_s est un sous-groupe de G.
2 - On suppose $n = km$, avec $k \wedge m = 1$.
  2.1. Montrer que $G_k \cap G_m = \{e\}$.
  2.2. Montrer que $G = G_k G_m$ et que $G \cong G_k \times G_m$.
  2.3. En utilisant le théorème de Cauchy, montrer que $|G_k| \wedge m = 1$ et en déduire que $|G_k| = k$.
  2.3. Montrer que G_k est l'unique sous-groupe d'ordre k de G.
3 - Montrer que tout groupe abélien fini est isomorphe à un produit direct de p-groupes.
(On rappelle q'un p-groupe est un groupe d'ordre une puissance d'un nombre premier p)

Solution.
1 - On a $e \in G_s$. Soient $x, y \in G_s$, $(xy^{-1})^s = x^s y^{-s} = e$. Donc G_s est un sous-groupe de G.
2 - 2.1. Soit $x \in G_k \cap G_m$. Donc $o(x) \mid k$ et $o(x) \mid m$. Par suite $o(x) \mid k \wedge m = 1$. Donc $x = e$.
2.2. $x \in G$, comme $k \wedge m = 1$, il existe $u, v \in \mathbb{Z}$, tels que $uk + vm = 1$. Alors on a $x = x^1 = x^{uk+vm} = (x^k)^u.(x^m)^v$. Posons $y_1 = (x^m)^v$ et $y_2 = (x^k)^u$, on a $x = y_1 y_2$ et $y_1^k = y_2^m = e$. Donc $y_1 \in G_k$ et $y_2 \in G_m$. Il en résulte que $G = G_k G_m$ et comme $G_k \cap G_m = \{e\}$, on a $G \cong G_k \times G_m$.
2.3. par l'absurde, si $|G_k| \wedge m \neq 1$, il existe un nombre premier p qui divise $|G_k|$ et m. D'après le théorème de Cauchy, G_k contient un élément x d'ordre p. i.e. $x^p = e$. Comme $p \mid m$, on a $x^m = e$. Donc $x \in G_m$, absurde. d'où $|G_k| \wedge m = 1$.
On a $|G| = n = km$, d'autre part $|G| = |G_k||G_m|$. Comme $|G_k| \wedge m = 1$, et $|G_m| \wedge k = 1$, on a $|G_k| \mid k$ et $k \mid G_k$. D'où $G_k = k$.
2.4. Soit H un autre sous-groupe d'ordre k, alors $\forall x \in H, x^k = e$, donc $H \subset G_k$. Comme $|H| = |G_k|$, on a $H = G_k$. D'où l'unicité.
3 - Par récurrence sur le nombre d'entiers premiers qui divisent l'ordre de G. Si $|G| = p_1^{k_1} \cdots p_s^{k_s}$ est la factorisation de $|G|$ en produit de nombres premiers, on pose G_1 le sous-groupe de G d'ordre $p_1^{k_1}$, et H_1 le sous-groupe de G d'ordre $p_2^{k_2} \cdots p_s^{k_s}$. On a $|G_1| \wedge |H_1| = 1$, par suite $G \cong G_1 \times H_1$. On applique alors l'hypothèse de récurrence à H_1 : $H_1 \cong G_2 \times G_2 \ldots \times G_s$, où les G_i sont des sous-groupes d'ordre $p_i^{k_i}$, $i = 2, 3 \ldots, s$. Il s'ensuit que $G \cong G_1 \times G_2 \times \ldots G_s$.