Théorie des groupes.

1 Quelques rappels

Groupe

Définition *Groupe*

On appelle *groupe* un ensemble G muni d'une loi interne $\star$ telle que $\star$ est associative, admettant un élément neutre $e \in G$ et tout élément $x \in G$ admet un symétrique dans G.

Lorsque la loi $\star$ est commutative sur G, on dit que le groupe $(G, \star)$ est commutatif.

Exercice Unicité de l'élément neutre et de l'inverse

Montrer que si $(G\star)$ est un groupe, alors nous avons unicité de son élément neutre.
Montrer que si $x \in G$, alors il y a unicité de son symétrique.

Solution

Supposons que G admette deux éléments neutres e_G et e'_G. Alors par définition de l'élément neutre, nous avons que:

$$\forall x \in G, \quad x \star e_G = e_G \star x = x \quad et \quad x \star e'_G = e'_G \star e'_G = x$$

En utilisant ces égalités pour respectivement $x = e'_G$ et $x = e_G$, nous déduisons que: $e'_G \star e_G = e'_G$ et $e'_G \star e_G = e_G$. Il s'ensuit donc que $e_G = e'_G$ et donc nous avons unicité de l'élément neutre de $(G, \star)$.
Supposons de même que x admette deux inverses: y et z. Nous aurions alors par définition des inverses que $x \star y = y \star x = e_G$ et $x \star z = z \star y = e_G$. Alors, par associativité de la loi $\star$ sur G, nous avons que $y \star (x \star z) = (y \star x) \star z$ ce qui implique que $y = z$ et donc nous avons unicité de l'inverse de l'élément $x \in G$.

Définition

La loi $\star$ est dite associative sur G si $\forall (x, y, z) \in G^3$, $x \star (y \star z) = (x \star y) \star z$.
La loi $\star$ admet un élément neutre e_G si $\forall x \in G$, $x \star e_G = e_G \star x = x$.
Enfin, un symétrique de $x \in G$ est tout élément $y \in G$ vérifiant $x \star y = y \star x = e_G$

Exemples:
$(\mathbb{Z}; +)$ est un groupe commutatif, alors que $(\mathbb{Z}, -)$ n'en est pas un puisque la loi $-$ n'est pas associative sur $\mathbb{Z}$. $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(C, +)$ sont aussi des groupes (commutatifs). $(\mathbb{Z}^*; \times)$ n'est pas un groupe car les éléments n'ont pas d'inverse (pour la multiplication). Par contre, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes (commutatifs). L'ensemble des matrices $\mathcal{M}_n(\mathbb{R})$ à coefficients réels est un groupe pour la loi additive, mais ce même ensemble n'est pas un groupe pour le produit matriciel puisqu'il existe des matrices non inversibles. Par contre, $\mathcal{G}l_n(\mathbb{R})$ l'ensemble des matrices inversibles d'ordre n à coefficients réels est un groupe pour le produit matriciel: ce groupe n'est pas commutatif (le produit matriciel ne l'est pas). Enfin, l'ensemble des bijections de $\mathbb{R}$ dans lui-même est un groupe pour la loi de composition.

Notations: Nous venons de voir plusieurs ensembles classiques qui ont une structure de groupe une fois munit d'une loi additive, ou produit ou de composition. Nous allons particulariser les notations relatives aux groupes dans ces cas particuliers.
Notation additive Si $(G, +)$ est un groupe, alors on note 0_G l'élément neutre, et le symétrique de $x \in G$ est appelé son *opposé*, et est noté $-x$.
Notation multiplicative: Si $(G, \times)$ est un groupe, alors on note 1_G son élément neutre, et le symétrique de $x \in G$ est appelé son *inverse*, et est noté x^{-1}.
Notation composition: Si $(G, \circ)$ est un groupe, alors on note Id_G son élément neutre, et le symétrique de $x \in G$ est appelé sa *réciproque*, et est noté x^{-1}.

Attention

On fera attention de ne pas confondre $f^{-1} = \frac{1}{f}$ et f^{-1} la bijection réciproque de f ... il faut bien faire attention au contexte!

Sous-groupe

Définition *Sous-groupe*

Soit A une partie de G. On dit que A est un *sous-groupe* de $(G,\star)$ si $(A,\star)$ est un groupe.

Exemples: Si $(G,\star)$ est un groupe, alors $\{e_G\}$ et G sont toujours des sous-groupes de $(G,\star)$, appelés *sous-groupes triviaux* de $(G,\star)$.

Exercice Intersection et union de sous-groupes

Soient H_1 et H_2 deux sous-groupes du groupe $(G,\star)$.
1. Montrer que $H_1 \cap H_2$ est un sous-groupe de $(G,\star)$.
2. Monter que $H_1 \cup H_2$ est un sous-groupe de $(G,\star)$ si et seulement si $H_1 \subset H_2$ ou $H_2 \subset H_1$.

Solution

1. Vérifions donc que $H_1 \cap H_2$ est un sous-groupe de $(G,\star)$. Déjà, puisque H_1 et H_2 sont des sous-groupes de $(G,\star)$, nous avons que $e_G \in H_1$ et $e_G \in H_2$ d'où $e_G \in H_1 \cap H_2$.
Ensuite, soient x, y deux éléments de $H_1 \cap H_2$. Donc x et y sont deux éléments de H_1 qui est un sous-groupe, d'où $x \star y \in H_1$. On montre de même que $x \star y \in H_2$ et donc $x \star y \in H_1 \cap H_2$.
Enfin, si $x \in H_1 \cap H_2$, alors $x \in H_1$ sous-groupe d'où $x^{-1} \in H_1$. De même, on montre que $x^{-1} \in H_2$ et donc $x^{-1} \in H_1 \cap H_2$ d'où $H_1 \cap H_2$ est un sous-groupe de $(G,\star)$.
2. Supposons par l'absurde que $H_1 \not\subset H_2$ et $H_2 \not\subset H_1$. Aussi, il existe $h_1 \in H_1 \setminus H_2$ et $h_2 \in H_2 \setminus H_1$. Comme $H_1 \cup H_2$ est un sous-groupe de $(G,\star)$, alors il est stable par la loi interne $\star$ et donc $h_1 \star h_2 \in H_1 \cup H_2$. Etudions alors les possibilités: si $h_1 \star h_2 \in H_1$, alors nous devrions avoir $h_2 \in H_1$ (il suffit de multiplier par h_1^{-1} à gauche) ce qui est absurde. De même, si $h_1 \star h_2 \in H_2$, alors par multiplication par H_2^{-1} à droite, nous en déduisons que $h_1 \in H_2$ ce qui est absurde. Aussi en déduit-on que l'on aboutit à une contradiction, ce qui implique que nécessairement $H_1 \subset H_2$ ou $H_2 \subset H_1$.

Définition *Ordre d'un groupe*

Si G est un groupe fini, on appelle *ordre* du groupe G le nombre $Card(G)$.

Théorème *Théorème de Lagrange*

Soit G un groupe. L'ordre de tout sous-groupe de G divise l'ordre du groupe G.

La démonstration de ce théorème fait l'objet de l'exercice suivant:

Exercice Démonstration du théorème de Lagrange

Soit $(G,\times)$ un groupe fini, et H un sous-groupe de G. On définit la relation binaire $\mathcal{R}$ sur G par: $x\mathcal{R}y$ si $x \times y^{-1} \in H$.
1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Pour tout $x \in G$, on considère l'application $f_x : H \to Hx$ définie par $f_x(y) = y \times x$.
Montrer que f_x est une bijection de H dans Hx. On a ainsi $Card(H) = Card(Hx)$.
3. Montrer que $Card(G) = n \times Card(H)$ où $n = Card(G/\mathcal{R})$ désigne le nombre de classes d'équivalences.

Définition *Ordre d'un élément, groupe engendré par un élément*

Soit G un groupe fini et $x \in G$. On note $< x >$ le plus petit sous-groupe de G, au sens de l'inclusion, contenant x. Ce sous-groupe est appelé *groupe engendré par x*. On appelle *ordre de x* le cardinal du sous-groupe $< x >$.

Exemple: Le sous-groupe engendré par $< e_G >$ est le sous-groupe trivial $\{e_G\}$.
Pour $a \in G, n \in \mathbb{N}$ posons $a^n = \underbrace{a \star a \star \cdots a}_{n \quad fois}$ et $a^{-n} = \underbrace{a^{-1} \star a^{-1} \star \cdots \star a^{-1}}_{n \quad fois}$. On a $< a >= \{a^k, k \in \mathbb{Z}\}$.

Corollaire *Version allégée du théorème de Lagrange*

L'ordre d'un élément divise l'ordre du groupe G.

Pratique

Pour montrer que A est un sous-groupe de $(G,\star)$, on prouve que A est non vide, que A est stable par $\star$ et que A est stable par passage au symétrique

Lagrange

Généralement, le théorème de Lagrange est vu en première année sous une forme moins forte, à savoir que l'ordre d'un élément de G divise l'ordre de G.

Remarque

La définition de l'ordre d'un élément nécessite de vérifier qu'il existe bien un plus petit sous-groupe au sens de l'inclusion. Comme G est un sous-groupe contenant x, l'ensemble des sous-groupes de $(G,\star)$ contenant x est non vide. En effectuant l'intersection de tous ces sous-groupes, nous obtenons un sous-groupe qui est le plus petit au sens de l'inclusion.

Démo

Si $a \in G$ et G d'ordre fini, alors l'ordre de a est égal à l'ordre du sous-groupe $< a >$. Or, d'après le théorème de Lagrange, nous avons $| < a > |$ divise $|G|$ d'où l'ordre de a divise l'ordre de G.

Morphisme de groupes

Définition *Morphisme de groupes*

Soient $(G,\star)$ et $(G',\cdot)$ deux groupes. Une application $\varphi : G \to G'$ est un *morphisme de groupes* si

$$\forall x,y \in G, \quad \varphi(x\star y)=\varphi(x)\cdot\varphi(y).$$

Idée

Les morphismes de groupes sont les applications respectant les structures des groupes de départ et d'arrivée.

Exercice Propriétés élémentaires des morphismes de groupes

Soit $\varphi : (G,\star) \to (G',\dot{)}$ un morphisme de groupes.
Montrer que $\varphi(e_G)=e_{G'}$ et $\varphi(x^{-1})=\varphi(x)^{-1}$.

Solution

Soit $x \in G$. Par définition d'un morphismes de groupes, nous avons: $\varphi(x\star e_G)=\varphi(x)\dot{\varphi}(e_G)$. Or, $\varphi(x\star e_G)=\varphi(x)$. Aussi, en multipliant à gauche par $\varphi(x)^{-1}$ (inverse de $\varphi(x)$ dans $(G',\dot{)}$) nous obtenons que $\varphi(e_G)=e_{G'}$.
Soit $x \in G$. Nous avons alors: $\varphi(x\star x^{-1})=\varphi(x)\dot{\varphi}(x^{-1})$, soit d'après la question précédente $\varphi(x)\dot{\varphi}(x^{-1})=e_{G'}$. Il s'ensuit alors par unicité de l'inverse de $\varphi(x)$ dans $(G',\dot{)}$ que $\varphi(x^{-1})=\varphi(x)^{-1}$.

Proposition *Structures de l'image et du noyau d'un morphisme de groupes*

Soit $\varphi : G \to G'$ un morphisme de groupes. Alors $Ker(\varphi)$ et $Im(\varphi)$ sont des sous-groupes respectivement de G et G'.
Plus généralement, si H et H' deux sous-groupes respectivement de G et G', alors $\varphi(H)$ est un sous-groupe de G' et $Ker(\varphi)$ est un sous-groupe de G.

Définitions

Si $A \subset G$, alors *l'image directe* de A par f est $f(A)=\{f(a), a\in A\}$.
Si $B \subset G'$, alors *l'image réciproque* de B par f est $f^{-1}(B)=\{a \in A, f(a)\in B\}$.

Démonstration Déjà, il suffit de démontrer les deux dernières affirmations puisque $Ker(\varphi)=\varphi^{-1}(\{e_{G'}\})$ et $\{e_{G'}\}$ est un sous-groupe (trivial) de G' (et de même, $Im(\varphi)=\varphi(E)$ et G est un sous-groupe trivial de G).
Soit donc H un sous-groupe de $(G,\star)$. Montrons que $\varphi(H)$ est un sous-groupe de $(G',\cdot)$. Déjà, $e_G \in H$ puisque H sous-groupe de G. Or, φ étant un morphisme de G dans G', il envoie l'élément neutre e_G sur $e_{G'}$, d'où $\varphi(e_G)=e_{G'}$ ce qui implique que $e_{G'}\in\varphi(H)$. Aussi, $\varphi(H)$ n'est pas vide.
Soient à présent x et y deux éléments de $\varphi(H)$. Il existe donc h_1 et h_2 des éléments de H tels que $x=\varphi(h_1)$ et $y=\varphi(h_2)$. Alors le produit $x\cdot y=\varphi(h_1)\cdot\varphi(h_2)=\varphi(\underbrace{h_1\star h_2}_{\in H})\in\varphi(H)$. Aussi, l'ensemble $\varphi(H)$ est bien stable par produit (de G').
Enfin, soit $x\in\varphi(H)$. Montrons que $x^{-1}\in\varphi(H)$. Si $x\in\varphi(H)$, il existe donc $h\in H$ tel que $x=\varphi(h)$. Or, x étant un groupe, $x^{-1}\in H$ d'où nous avons que $\varphi(x^{-1})=\varphi(x)^{-1}\in H$, d'où H est stable par passage à l'inverse. Aussi, on démontre que $\varphi(H)$ est un sous-groupe de G'.
On procède de même pour $\varphi^{-1}(H')$ pour H' sous-groupe de G'. Comme e_G vérifie $\varphi(e_G)=e_{G'}\in H'$, nous avons $e_G\in\varphi^{-1}(H')$ d'où φ^{-1} non vide. Si $x,y\in\varphi^{-1}(H')$ nous avons donc $\varphi(x)\in H'$ et $\varphi(y)\in H'$. Le produit $x\star y$ vérifie alors $\varphi(x\star y)=\varphi(x)\cdot\varphi(y)\in H'$ puisque H' est un sous-groupe de G' donc est stable par produit ($\varphi(x)\in H$ et $\varphi(y)\in H$). Il s'ensuit alors que $x\star y\in\varphi^{-1}(H')$, ce qui démontre que $\varphi^{-1}(H')$ est stable par produit. Enfin, si $x\in\varphi^{-1}(H')$, alors $\varphi(x)\in H'$. Mais H' sous-groupe de G' donc est stable par inverse: $(\varphi(x))^{-1}\in H'$. Comme montré plus haut, $\varphi(x)^{-1}=\varphi(x)^{-1}$ d'où $\varphi(x^{-1})\in H'$ ce qui implique que $x^{-1}\in\varphi^{-1}(H')$.

2 Sous-groupes distingués

Nous souhaitons savoir à quelle condition sur le sous-groupe H nous pouvons munir l'ensemble G/H des classes d'équivalence de G sous H d'une structure de groupe. C'est pour cela que nous allons considérer la notion de sous-groupe distingué de G.

Définition *Classe à droite de x par rapport à un sous-groupe*

Soit H un sous-groupe de G et $x \in G$. On appelle *classe à droite* de l'élément x par rapport à H l'ensemble $Hx = \{h \star x | h \in H\}$, et *classe à gauche de x par rapport à H* l'ensemble $xH = \{x \star h | h \in H\}$.

Proposition *Critère pratique pour déterminer si deux éléments sont dans la même classe à gauche*

Soient g_1 et g_2 deux éléments de G. Ils sont dans la même classe à gauche par rapport à H si $g_1^{-1} \star g_2 \in H$.

Démonstration Supposons que $g_1^{-1} \star g_2 \in H$, et soit $x \in G$ tel que $g_1 \in xH$ (i.e. g_1 est dans la classe à gauche de x par rapport à H). Alors il existe $h \in H$ tel que $g_1 = xh$. En multipliant par la droite par $g_1^{-1} \star g_2$ nous obtenons: $g_1 \star (g_1^{-1} \star g_2) = xh \star (g_1^{-1} \star g_2)$. Dans le membre de gauche, nous obtenons g_2 après simplification. Comme h et $g_1^{-1} \star g_2$ sont deux éléments de H sous-groupe, nous en déduisons que $h \star (g_1^{-1} \star g_2)$ est un élément de H. Aussi: $g_2 = x \star \underbrace{(h \star (g_1^{-1} \star g_2))}_{\in H} \in xH$.

L'élément g_2 est donc bien dans la même classe à gauche que g_1. La condition proposée implique donc bien que g_1 et g_2 sont dans la même classe à gauche par rapport à H.

Si H est un sous-groupe, on peut considérer G/H l'ensemble quotient des classes à gauches. On se demande à quelle condition peut-on propager la structure de groupe de G à G/H. Pour ce faire, il faut que les classes à gauches et à droites coincident, soit $xH = Hx$.

Définition *Sous-groupe distingué*

Soit G un groupe. Un sous-groupe H est dit *distingué* (ou encore *normal* ou *invariant*) dans G si pour tout $x \in G$, $xH = Hx$. On note alors $H \triangleleft G$.

Proposition *Caractérisation pratique de H distingué.*

Soit G un groupe et H un sous-groupe de G. H est un sous-groupe distingué de G si $\forall x \in G$, $xHx^{-1} \subset H$.

Démonstration Supposons que H soit distingué dans G (donc que $\forall x \in G$, $xH = Hx$). Alors considérons $x \in G$ et un élément z de xHx^{-1}, c'est-à-dire qu'il existe $h \in H$ tel que $z = x \star h \star x^{-1}$. Comme $xH = Hx$, il existe $h' \in H$ tel que $x \star h = h' \star x$, d'où nous obtenons $z = h' \star \underbrace{x \star x^{-1}}_{=e_G} = h' \in H$.

Réciproquement, supposons que H est un sous-groupe de G vérifiant $\forall x \in G$, $xHx^{-1} \subset H$. Alors, soit $z \in xH$ ie il exite $h \in H$ tel que $z = x \star h$. En écrivant $z = x \star h \star (x^{-1} \star x)$ et en utilisant l'associativité de $\star$ on a $z = \underbrace{(x \star h \star x^{-1})}_{\in H} \star x \in Hx$. On montre ainsi que $\forall x \in G$, $xH \subset Hx$. On démontre de même l'inclusion inverse.

Exemples Les sous-groupes triviaux de $(G, \star)$ sont distingués dans G. Si $(G, \star)$ est un groupe commutatif, alors tout sous-groupe de $(G, \star)$ est distingué dans G.

Définition

Un groupe dont les seuls sous-groupes distingués sont triviaux est dit *simple*.

Exercice Etude d'un exemple

On considère $\mathcal{S}_3$ le groupe des permutations de l'ensemble $\{1;2;3\}$. On note $\tau = (1\ 2)$ et $\sigma = (1\ 2\ 3)$.
1. Le sous-groupe $H_1 = \{e;\tau\}$ est-il distingué dans $\mathcal{S}_3$?
2. Le sous-groupe $H_2 = \{e;\sigma;\sigma^2\}$ est-il distingué dans $\mathcal{S}_3$?

Solution

1. On vérifie déjà que H_1 est bien un groupe puisque τ est une transposition. Considèrons l'élément σ: nous avons $\sigma H_1 = \{\sigma;(2\ 3)\}$ alors que $H_1\sigma = \{\sigma;(1\ 3)\}$. Il s'ensuit donc que le sous-groupe H_1 n'est pas distingué dans Σ_3.
2. Considérons alors H_2. En effectuant les différentes vérifications (à savoir que $\forall x \in S_3$, $xH_2 = H_2x$) et on obtient que H_2 est un sous-groupe distingué de $\mathcal{S}_3$. On peut aussi utiliser l'exercice suivant pour éviter la vérification.

Définition *Indice d'un sous-groupe*

Soit H un sous-groupe de $(G,\star)$. Alors on définit *l'indice de H dans G* comme étant l'entier $\frac{|G|}{|H|}$. On le note $[G:H]$.

Remarque

$[G:H]$ est un entier grace au théorème de Lagrange

Exercice Sous-groupe d'indice 2

Soit G un groupe d'ordre $2n$ et H un sous-groupe de G d'indice 2 dans G (i.e. G est donc d'ordre n).
Montrer alors que H est distingué dans G ($H \triangleleft G$). Pour montrer que $xH = Hx$, on pourra distinguer le cas $x \in H$ de $x \notin H$ et, dans ce dernier cas, montrer que $xH = G \setminus H$ et $Hx = G \setminus H$.

Proposition *Structure du noyau d'un morphisme*

Soit $\varphi : G \to G'$ un morphisme de groupes. Alors $Ker(\varphi)$ est un sous-groupe distingué de G.

Démonstration Soit $x \in G$. Montrons que $xKer(\varphi)x^{-1} \subset Ker(\varphi)$. Pour ce faire, soit $y \in Ker(\varphi)$. Alors $\varphi(xyx^{-1}) = \varphi(x)\varphi(y)\varphi(x^{-1}) = \varphi(x)\varphi(x^{-1}) = \varphi(e_G) = e_{G'}$. Comme nécessairement $e_G \in Ker(\varphi)$, on a $e_G \in xKer(\varphi)x^{-1}$. Aussi $Ker(\varphi)$ est un sous-groupe distingué de G.

Le résultat précédent se généralise: n'oublions pas que $Ker(\varphi)$ est l'image réciproque de $\{e_{G'}\}$, l'un des deux sous-groupes triviaux de G' qui sont tous deux distingués dans G'.

Proposition *Structure de l'image réciproque d'un sous-groupe distingué*

Soit $\varphi : G \to G'$ un morphisme de groupes et H' un sous-groupe distingué de G'. Alors $\varphi(H')$ est un sous-groupe distingué de G.

Démonstration Nous savons déjà que l'image réciproque de H' par φ est un sous-groupe de G. Il reste donc à montrer que c'est un sous-groupe distingué de G. Pour ce faire, considérons $x \in G$. Alors $\forall y \in \varphi^{-1}(H')$, nous avons: xyx^{-1} qui vérifie $\varphi(xyx^{-1}) = \varphi(x)\varphi(y)\varphi x^{-1}$. Or, $\varphi(y) \in H'$ qui est distingué donc $\varphi(x)\varphi(y)\varphi(x)^{-1} \in H'$. Aussi, $\varphi(xyx^{-1}) \in H'$, d'où $xyx^{-1} \in \varphi^{-1}(H')$. Il s'ensuit donc que $\varphi^{-1}(H')$ est un sous-groupe distingué de G.

Par contre, le résultat analogue n'est pas vrai pour l'image directe: l'image directe par un morphisme d'un sous-groupe distingué n'est pas nécessairement distinguée.

Exercice Etude de l'image directe d'un sous- groupe distingué par un morphisme.

Soit H un sous-groupe non distingué de G. On considère $i : H \to G$ l'inclusion de H dans G. Montrer que i est bien un morphisme, et en déduire que l'image d'un sous-groupe distingué n'est pas nécessairement distingué.

Solution

L'inclusion est bien un morphisme, dont l'image est H. Or, H est distingué dans H mais non dans G, d'où l'image directe d'un sous-groupe distingué par un morphisme n'est pas nécessairement un sous-groupe distingué.

Pour pouvoir affirmer que l'image d'un sous-groupe distingué par φ un morphisme de groupes est un sous-groupe distingué, il faut donc ajouter une hypothèse supplémentaire, à savoir que φ doit être surjectif.

Proposition *Image directe d'un sous-groupe distingué par un morphisme surjectif de groupes*

Soit $\varphi : G \to G'$ un morphisme surjectif de groupes, et H un sous-groupe distingué de G. Alors l'image directe $\varphi(H)$ de H par φ est un sous-groupe distingué de G'.

Démonstration Supposons donc $\varphi : G \to G'$ un morphisme surjectif de groupes et $H \triangleleft G$. Nous savons déjà que $\varphi(H)$ est un sous-groupe de G': reste à montrer qu'il est distingué dans G'. Soit alors $y \in G'$, et montrons que $y\varphi(H)y^{-1} \subset \varphi(H)$. Le morphisme φ étant surjectif, il existe $x \in G$ tel que $\varphi(x) = y$. Aussi, si h désigne un élément quelconque de H, nous avons $y\varphi(h)y^{-1} = \varphi(x)\varphi(h)\varphi(x)^{-1} = \varphi(x)\varphi(h)\varphi(x^{-1}) = \varphi(xhx^{-1})$. Or, $h \in H$ et $H \triangleleft G$ donc $xhx^{-1} \in H$ ce qui implique que $y\varphi(h)y^{-1} = \varphi(xhx^{-1}) \in \varphi(H)$. Nous en déduisons donc bien que $\varphi(H)$ est un sous-groupe distingué de G'.

Le théorème suivant permet de montrer que la condition H distingué dans G est bien nécessaire à ce que G/H ai une structure de groupe héritée de celle de G.

Théorème

Soit H un sous-groupe de G. Nous avons l'équivalence des conditions suivantes:

i. Il existe G' groupe et $\varphi : G \to G'$ morphisme tel que $Ker(\varphi) = H$.

ii. H est un sous-groupe distingué dans G.

iii. L'ensemble G/H est muni d'une structure de groupe quotient, propagée par celle de H, telle que l'application $\pi : G \to G/H$ définie par $\pi(a) = aH$ soit un morphisme de groupes.

Démonstration *i.* $\Rightarrow$ *ii.* Nous avons déjà vu que le noyau d'un morphisme de groupe est un sous-groupe distingué.
ii. $\Rightarrow$ *iii.* On suppose $H \triangleleft G$. Définissions une structure de groupe sur G/H, de sorte que $\pi : G \to G/H$ soit un morphisme de groupe de noyau H. Si aH et bH sont deux éléments de G/H alors notons $aH \star bH = abH$. Vérifions que cette application est bien définie (i.e. ne dépends pas du représentant choisi). Soient a, a', b, b' dans G tels que $aH = a'H$ et $bH = b'H$. Alors il existe h_a et h_b dans H tels que $a = a' \times h_a$ et $b = b' \times h_b$. Aussi, $ab = a'h_ab'h_b$. Mais puisque H est distingué, il existe h_c tel que $h_ab' = b'h_3$. Aussi, nous avons $ab = a'b'h_3h_b$ d'où nous avons bien $abH \subset a'b'H$. Par symétrie des indices nous en déduisons l'inclusion réciproque, d'où $abH = a'b'H$. Ainsi, le produit $aH \star bH$ est indépendant du représentant choisi dans la classe: on muni donc G/H d'une structure de groupe; l'élément neutre de ce groupe est H puisque l'on vérifie aisément que $H \star aH = ah \star H = aH$. Enfin, l'application $\pi : G \to G/H$ définie par $\pi(a) = aH$ est un morphisme de groupe de G sur G/H.
iii. $\Rightarrow$ *i.* Il suffit ici de prendre $G' = G/H$ et $\pi = \varphi$ pour retrouver i.

Feuille de TD : Groupes

Dans la suite, nous désignons par E un ensemble non vide. Une relation $\mathcal{R}$ sur E est une partie de $E \times E$.

Définition *Relation d'équivalence*

Une relation $\mathcal{R}$ sur E est une *relation d'équivalence* si elle vérifie:
$\mathcal{R}$ est réflexive ($\forall x \in E$, $x\mathcal{R}x$)
$\mathcal{R}$ est symétrique ($\forall (x,y) \in E^2$, $x\mathcal{R}y \quad \Rightarrow \quad y\mathcal{R}x$)
$\mathcal{R}$ est transitive ($\forall (x,y,z) \in E^3$, si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $x\mathcal{R}z$)

Définition *Classe d'équivalence*

Soit $x \in E$. On appelle *classe d'équivalence de x* l'ensemble des éléments $y \in E$ qui sont en relation avec x, soit $\mathcal{C}l(x) = \{y \in E, \quad x\mathcal{R}y\}$. La classe d'équivalence de x est souvent notée $\overline{x}$.
On désigne par $E/\mathcal{R}$ l'ensemble des classes d'équivalence de E sous $\mathcal{R}$.

Exercice Propriété des classes d'équivalences

Montrer que l'ensemble des classes d'équivalences de E sous $\mathcal{R}$ forme une partition de E

Exercice Classes $\mathbb{Z}/n\mathbb{Z}$

Dans cet exercice, on désigne par n un entier naturel supérieur ou égal à 2. On considère la relation $\mathcal{R}$ définie sur $\mathbb{Z}$ définie par $x\mathcal{R}y$ si x et y ont même reste dans la division euclidienne par n. On pourra librement utiliser que $x\mathcal{R}y$ si et seulement si $y - x$ est un multiple de n.
1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{Z}$.
2. Précisez le nombre de classes d'équivalences.
On désigne par $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences pour cette relation, et celle-ci sont appelées *classes de congruence*.

A présent, considérons l'interraction de la relation d'équivalence $\mathcal{R}$ avec la structure de groupe: soit $(G, \star)$ un groupe et $\mathcal{R}$ une relation d'équivalence sur G.

Définition *Compatibilité d'une relation d'équivalence avec la loi du groupe*

Soit $\mathcal{R}$ une relation d'équivalence sur G. On dit que $\mathcal{R}$ est compatible avec la loi de groupe $\star$ si, $\forall (a, a', b, b') \in G^4$, $a\mathcal{R}a'$ et $b\mathcal{R}b'$, alors $(a \star b)\mathcal{R}(a' \star b')$.
Lorsque tel est le cas, l'ensemble quotient $G/\mathcal{R}$ hérite d'une loi $\star$ définie par $\mathcal{C}l(x) \star \mathcal{C}l(y) = \mathcal{C}l(x \star y)$, de sorte que $(G/\mathcal{R}; +)$ soit un groupe.

Exercice Compatibilité de l'addition avec la relation de congruence modulo n

On considère $n \geq 2$ ainsi que la relation d'équivalence $\mathcal{R}$ précédente.
Montrer que la relation $\mathcal{R}$ est compatible avec la loi $+$ de $\mathbb{Z}$.
On en déduit alors que l'ensemble $(\mathbb{Z}/n\mathbb{Z}, +)$ admet une structure de groupe commutatif.

Exercice 1: Démonstration du théorème de Lagrange

Soit $(G, \times)$ un groupe fini, et H un sous-groupe de G.
On définit la relation binaire $\mathcal{R}$ sur G par: $x\mathcal{R}y$ si $x \times y^{-1} \in H$.
1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Pour tout $x \in G$, on considère l'application $f_x : H \to Hx$ définie par $f_x(y) = y \times x$.
Montrer que f_x est une bijection de H dans Hx. On a ainsi $Card(H) = Card(Hx)$.
3. Montrer que $Card(G) = n \times Card(H)$ où $n = Card(G/\mathcal{R})$ désigne le nombre de classes d'équivalences.

Exercice 2: Etude de la structure produit cartésien de groupes

Dans la suite, on désigne par $(G_1, \star)$ et $(G_2, \star)$ deux groupes, et par $G_1 \times G_2$ l'ensemble des couples d'élements (x, y) avec $x \in G_1$ et $y \in G_2$ (il s'agit du produit cartésien d'ensemble G_1 et G_2). On définit sur l'ensemble $G_1 \times G_2$ la loi $\star$ par $\forall (x, y), (x', y') \in G_1 \times G_2$, $(x, y) \star (x', y') = (x \star x'; y \star y')$.
Montrer que $(G_1 \times G_2, \star)$ est un groupe, appelé groupe produit des groupes G_1 et G_2.

Exercice 3: Produit de deux sous-groupes

On considère $(G, \times)$ un groupe commutatif d'élément neutre e et soient A et B deux sous-groupes de G.
On appelle AB la partie de G égale à $\{ab, a \in A, b \in B\}$.
1. Montrer que AB est un sous-groupe de G.
2. On suppose de plus que $AB = G$ et que $A \cap B = \{e\}$. Montrer que l'application $f : A \times B \to G$ définie par $f : (a, b) \mapsto ab$ est un isomorphisme du groupe produit $A \times B$ sur le groupe G.
On démontre ainsi que les groupes $A \times B$ et AB sont isomorphes.
3. On considère dans la suite que le groupe $(G, \times)$ est fini et de cardinal pair $n = 2m$. On suppose de plus qu'il existe deux éléments, a et b, respectivement d'ordre m et 2 tels que $b \notin < a >$.
a. Soient $i, j \in \{1, \cdots, m\}$. Montrer que $a^i = a^j$ si et seulement si $i = j$.
b. Calculer $Card\left(\{a^i, i \in \{1, \cdots, m\} \cup \{a^i b, i \in \{1, \cdots, m\}\right)$.
c. En déduire que $G =< a >< b >$
d. Montrer que les groupes $< a > \times < b >$ et G sont isomorphes.

Exercice 4: Groupes dihédraux

Pour tout $n \geq 3$, on note D_n l'ensemble des isométries du plan affine euclidien laissant globalement invariant l'ensemble des sommets d'un polygône régulier à n sommets.
1. Montrer que D_n est un groupe d'ordre $2n$, appelé groupe dihédral.
2. Démontrer que D_3 est engendré par deux éléments, r et s, vérifiant $r^3 = e$ et $s^2 = e$ et $sr = r^{-1}s$, et que D_3 est isomorphe à S_3.
3. Montrer que, plus généralement, le groupe D_n admet deux éléments, l'un noté r d'ordre n, et l'autre noté s d'ordre 2.
4. En utilisant le résultat de l'exercice 3, donner l'écriture de tout élément de D_n à l'aide de r et s.
5. A quel groupe produit le groupe D_n est-il isomorphe ? (on attends des groupes produits de groupes $\mathbb{Z}/m\mathbb{Z}$)

Exercice 5: Etude des sous-groupes d'indice 2

Soit G un groupe fini d'ordre $2n$ avec $n \in \mathbb{N}^*$.
1. Soit H un sous groupe de G d'ordre n. Montrer que H est distingué dans G.
2. On suppose qu'il existe deux sous groupes H_1 et H_2 de G d'ordre n et tels que $H_1 \cap H_2 = \{e_G\}$. Montrer que $n = 1$ ou $n = 2$.
3. On suppose qu'il existe deux sous groupes H_1 et H_2 de G, distincts et tout deux d'ordre n. Montrer que $H = H_1 \cap H_2$ est un sous-groupe distingué dans G. En déduire que l'ordre de G est un multiple de 4.

Exercice 6: Groupes cycliques

Soit $(G, \cdot)$ un groupe, et a un élément de G. On note 1_G l'élément neutre de G et par a^{-1} le symétrique de l'élément a. Pour tout entier naturel n, on définit par récurrence la puissance n-ième de a par $a^0 = 1_G$ et $\forall n \in \mathbb{N}$, $a^{n+1} = a^n \cdot a$. Pour tout entier relatif $m \in \mathbb{Z}_-$, on désigne par a^m l'élément $\left(a^{-1}\right)^{-m}$.

Un groupe est appelé *monogène* s'il est engendré par un seul élément, c'est-à-dire s'il existe $a \in G$ tel que $G = \{a^k, k \in \mathbb{Z}\}$. Un groupe est dit *cyclique* s'il est monogène et d'ordre fini.

1. Soit $(G, \cdot)$ un groupe cyclique d'ordre n.
   a. Montrer alors qu'il existe $a \in G$ tel que $G = \{a, a^2, \cdots, a^n\}$. Dans la suite, un tel élément sera appelé un *générateur* du groupe $(G, \cdot)$.
   b. Montrer que n est le plus petit entier naturel non nul tel que $a^n = 1_G$.
2. Montrer que tout groupe cylique $(G, \cdot)$ d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
3. Montrer que l'ordre de tout élément du groupe cyclique $(G, \cdot)$ est un diviseur de l'ordre de ce groupe.
4. Montrer que les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les classes $\overline{k}$ telles que $k \wedge n = 1$.
5. Si $(G, \cdot)$ est un groupe cyclique d'ordre n et si $a \in G$ est un générateur de $(G, \cdot)$, montrer que l'ensemble des générateurs de $(G, \cdot)$ est l'ensemble $\{a^k, k \wedge n = 1\}$.
6. (Application)
   Pour $n \geq 2$, on désigne par $\mathbb{U}_n$ l'ensemble des nombres complexes z vérifiant $z^n = 1$. Ces éléments sont appelés *racines n-ième de l'unité*.
   (a) Décrivez l'ensemble des éléments de $\mathbb{U}_n$.
   (b) Montrer que $(\mathbb{U}_n, \times)$ est un groupe.
   (c) Précisez l'isomorphisme entre $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{U}_n, \times)$.
   (d) Quels sont les générateurs de $(\mathbb{U}_n, \times)$? Ces éléments sont appelées *racines primitives n-ième de l'unité*.

Exercice 7: Groupe de Klein

On munit le produit cartésien du groupe $(\mathbb{Z}/2\mathbb{Z}, +)$ par lui-même de la structure de groupe produit. On appelle ce groupe produit le **Groupe de Klein**.

1. Donner la table d'addition du groupe de Klein (on précisera ses éléments).
2. Trouver une interprétation géométrique de ce groupe.
3. Le groupe de Klein est-il isomorphe au groupe $\mathbb{Z}/4\mathbb{Z}$?

Exercices libres

Exercice 1: Une loi sur $\mathbb{R}$

On considère la loi $\star$ définie sur $\mathbb{R}$ par $x \star y = x + y - xy$.

1. Cette loi est-elle associative ? Commutative ?
2. Admet-elle un élément neutre ?
3. Précisez quels sont les réels qui admettent un inverse pour $\star$.
4. Existe-t'il $\mathcal{A} \subset \mathbb{R}$ une partie de $\mathbb{R}$ pour laquelle $(\mathcal{A}, \star)$ soit un groupe?

Exercice 2: Suffisance de l'inverse à gauche

On suppose que G est un ensemble non vide, $\star$ une loi de composition interne sur G telle que $\star$ est associative sur G, $\star$ admet un élément neutre $e \in G$, et tel que pour tout élément $x \in G$, il existe un inverse à gauche dans G (c'est-à-dire qu'il existe $y \in G$ tel que $y \star x = e$).
Montrer alors que $(G, \star)$ est un groupe.

Exercice 3: A gauche toute!

Soit G un ensemble non vide muni d'une loi $\star$, associative et qui vérifie les propriétés suivante:

- Il existe un neutre à gauche e_g (c'est-à-dire que $\forall x \in G$, $e_g \star x = x$).
- Tout élément de G admet un inverse à gauche (c'est-à-dire que $\forall x \in G$, $\exists y \in G$ tel que $y \star y = e_g$).

Montrer alors que $(G, \star)$ est un groupe.

Exercice 4: Sous-groupes de $(\mathbb{Z},+)$

Le but de cet exercice est de montrer que les sous-groupes additifs de $\mathbb{Z}$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$. Soit H un sous-groupe de $\mathbb{Z}$.

1. Montrer que si $H = \{0\}$, alors H est bien de la forme demandé. On suppose dans la suite que $H \neq \{0\}$.
2. Montrer alors que $\mathcal{A} = H \cap \mathbb{N}^*$ admet un plus petit élément n.
3. Montrer alors que $H = n\mathbb{Z}$.

Solution des exercices libres

Exercice 1: Une loi sur $\mathbb{R}$

1. Soient x, y, z trois réels. Alors, nous avons que
$$x \star (y \star z) = x \star (y+z-yz) = x + (y+z-yz) - x(y+z-yz) \quad (1)$$
$$= x+y+z-yz-xy-xz+xyz = (x+y-xy) \star z = (x \star y) \star z \quad (2)$$
Aussi, la loi $\star$ est associative sur $\mathbb{R}$.
Elle est aussi clairement commutative car la somme et le produit réel le sont.

2. Procédons par analyse-synthèse:
Analyse: supposons que $\star$ admet un élément neutre $e \in \mathbb{R}$. Alors nécessairement, nous devons avoir pour tout réel x: $x \star e = e \star x = e$, soit encore $x + e - ex = x$, soit $e(1-x) = 0$. Comme cette égalité doit être vérifiée pour tout réel x, nous en déduisons que $e = 0$ et obtenons une condition nécessaire.
Synthèse: Soit $x \in \mathbb{R}$. Alors $x \star 0 = x + 0 - 0 = x = 0 \star x$ d'où $e = 0$ est un élément neutre de $\star$ sur $\mathbb{R}$.
Note: L'élément neutre est unique: pour le montrer, soit on traite le cas général (il y a unicité du neutre pour tout groupe $(G, \times)$), soit on utilise la partie Analyse de notre raisonnement: nous avons obtenue que, si $\star$ admet un élément neutre, alors celui-ci doit nécessairement vérifier $e = 0$, d'où l'unicité du neutre de $\mathbb{R}$ pour la loi $\star$.

3. Soit $x \in \mathbb{R}$. Raisonnons par analyse-synthèse:
Analyse: On suppose donc qu'il existe y symétrique de x. Aussi, nous devons avoir: $x \star y = e$, soit encore $x + y - xy = 0$. Aussi, nous en déduisons que $y(1-x) = -x$. Donc, si $x \neq 1$, nous en déduisons que $y = \frac{x}{x-1}$ ce qui nous donne une condition nécessaire dans le cas où $x \neq 1$. Si $x = 1$, alors nous constatons que l'équation $1 + x - x = 0$ n'admet pas de solution: aussi, 1 n'a-t'il pas d'inverse pour cette loi (c'est une condition nécessaire: 1 n'est pas inversible par $\star$).
Synthèse: Pour tout $x \in \mathbb{R} \setminus \{1\}$, considérons $y = \frac{x}{x-1}$. Nous avons alors:
$$x \star y = x + y - xy = x + \frac{x}{x-1} - \frac{x^2}{x-1} = \frac{x(x-1) + x - x^2}{x-1} = 0.$$
On en déduit donc que tout réel différent de 1 est inversible pour $\star$.

4. On considère alors $\mathcal{A}$ l'ensemble des réels admettant un inverse pour $\star$, c'est-à-dire $\mathcal{A} = \mathbb{R} \setminus \{1\}$. Alors, nous vérifions tous les axiomes de groupe, et donc $(\mathbb{R} \setminus \{1\}, \star)$ est un groupe abélien.

Exercice 2: Suffisance de l'inverse à gauche
Pour vérifier que $(G, \star)$ est un groupe, il suffit de montrer que l'inverse à gauche de x est aussi son inverse à droite pour la loi $\star$ (il sera ainsi son élément symétrique). Soit donc $x \in G$ et y son inverse à gauche. On note z l'inverse à gauche de y: nous avons donc $yx = e$ et $zy = e$. Calculons donc
$$x \star y = e \star (x \star y) = (z \star y) \star (x \star y) = z \star \underbrace{(y \star x)}_{=e} \star y = z \star y = e.$$
On en déduit donc bien que tout élément $x \in G$ admet un inverse (i.e. un inverse à gauche et à droite).
Note: Il est donc suffisant, dans la définition de groupe, de demander à ce que tout élément $x \in G$ admet un symétrique à gauche au lieu d'un symétrique.

Exercice 3: A gauche toute!
Nous devons ici montrer deux choses: que l'élément neutre à gauche e_g est un neutre e et que tout inverse à gauche est aussi un inverse à droite (donc est l'inverse). Débutons par montrer que si y est l'inverse à gauche de x, alors y est aussi l'inverse à droite de x, c'est-à-dire que si $y \star x = e_g$ alors $x \star y = e_g$. Soit alors z l'inverse à gauche de y: nous avons donc $yx = e_g$ et $zy = e_g$. Il s'ensuit donc que:
$$xy = e_G \star (xy) = (zy) \star (xy) = z \underbrace{(yx)}_{=e_g} y = z \underbrace{(e_G \star y)}_{=y} = zy = e_g.$$
Donc, l'inverse à gauche de x est aussi son inverse à droite, et il s'ensuit que tout élément x admet in inverse.
Montrons que l'élément neutre à gauche e_g est aussi un neutre à droite, c'est-à-dire que $\forall x \in G$, $x \star e_g = x$. Pour ce faire, soit y l'inverse de x. Nous avons alors:
$$x \star e_g = (x \star e_g) \star (y \star x) = x \star \underbrace{(e_g \star y)}_{=y} \star x = \underbrace{(x \star y)}_{=e_G} \star x = x.$$
Il s'ensuit donc qu'il existe un élément $e = e_g$ dans G vérifiant $\forall x \in G$, $e \star x = x \star e = x$. De plus, pour tout élément $x \in G$, il existe $y \in G$ tel que $x \star y = y \star x = e$, d'où $(G, \star)$ est un groupe.

Exercice 4: Sous-groupes de $\mathbb{Z}$

1. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$ est bien de la forme souhaitée.

2. On suppose donc $H \neq \{0\}$. Aussi, il existe $h \in H$ avec $h \neq 0$. Comme H est un sous-groupe de $(\mathbb{Z}, +)$, on en déduit que $-h \in H$, donc sans perte de généralité, nous pouvons considérer que $h > 0$ et donc $h \in \mathcal{A}$, ce qui implique que $\mathcal{A}$ est un ensemble non vide. Comme c'est un sous-ensemble de $\mathbb{N}$, il admet un plus petit élément: soit n celui-ci. Nous avons bien sûr $n > 0$ (car $0 \notin \mathcal{A}$).

3. Nous allons procéder par double inclusion. Déjà, puisque $n \in \mathcal{A} \subset H$, nous avons clairement l'inclusion $n\mathbb{Z} \subset H$.
Montrons donc l'inclusion réciproque: soit $h \in H$. Effectuons la division euclidienne (dans $\mathbb{Z}$) de h par n: il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $h = qn + r$ avec $0 \leq r < n$. Aussi, $r = h - qn$, mais comme $h \in H$ et $n \in H$, il s'ensuit que $r \in H$ (car H stable par la somme ou la différence d'éléments de H). Il s'ensuit donc que $0 \leq r < n$ et $r \in H$, d'où $r = 0$ (sinon, cela contredirait la minimalité de n dans $\mathcal{A}$). Donc $h = qn \in n\mathbb{Z}$ et on en déduit l'inclusion $H \subset n\mathbb{Z}$ d'où l'égalité souhaitée.

Solution: Propriété des classes d'équivalences

La relation $\mathcal{R}$ étant une relation d'équivalence, elle est réflexive. Aussi, nous constatons que tout élément $x \in E$ appartient à sa classe d'équivalence puisque $x\mathcal{R}x$. Aussi l'ensemble des classes d'équivalence de E sous $\mathcal{R}$ forme-t'il un recouvrement de E. Pour montrer que l'ensemble des classes d'équivalence forme une partition de E, montrons que deux classes sont soient disjointes, soient confondues.
Considérons alors $\mathcal{C}l(x)$ et $\mathcal{C}l(y)$ deux classes d'équivalence non disjointes. Aussi, soit $z \in \mathcal{C}l(x) \cap \mathcal{C}l(y)$. Alors, $z \in \mathcal{C}l(x)$ implique que $x\mathcal{R}z$ et $z \in \mathcal{C}l(y)$ implique que $z\mathcal{R}y$, d'où nous déduisons par transitivité de $\mathcal{R}$ que $x \in \mathcal{R}y$.
Montrons à présent que $\mathcal{C}l(x) \subset \mathcal{C}l(y)$. Pour ce faire, considérons $x' \in \mathcal{C}l(x)$. Alors $x'\mathcal{R}x$ et comme nous savons que $x\mathcal{R}y$, par transitivité de la relation $\mathcal{R}$ nous en déduisons que $x'\mathcal{R}y$ et donc $x' \in \mathcal{C}l(y)$. Il s'ensuit que $\mathcal{C}l(x) \subset \mathcal{C}l(y)$. Par symétrie des rôles entre x et y, nous en déduisons que $\mathcal{C}l(y) \subset \mathcal{C}l(x)$ et nous obtenons l'égalité de deux ensembles par double inclusion.

Solution: Classes de congruence modulo n

1. Montrons que la relation $\mathcal{R}$ est une relation d'équivalence. Cette relation est évidemment réflexive et symétrique. Reste alors à montrer la transitivité: soient x, y, z des entiers tels que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors, nous en déduisons que x, y et z ont même reste dans la division euclidienne par n. Aussi nous avons $x\mathcal{R}z$ et donc $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{Z}$.
2. Il y a autant de classes de congruences modulo n qu'il y a de restes différents dans la division euclidienne par n; aussi en déduisons-nous qu'il existe n classes de congruences différentes.

Solution: Compatibilité de l'addition avec la relation de congruence modulo n

Soient donc a, a', b, b' des entiers relatifs tels que $a\mathcal{R}a'$ et $b\mathcal{R}b'$. Alors $n|(a-a')$ et $n|(b-b')$ d'où $n|(a+b-a'-b')$, ce qui implique que $(a+b)\mathcal{R}(a'+b')$. Il s'ensuit donc que nous pouvons munir l'ensemble des classes de congruence $\mathbb{Z}/n\mathbb{Z}$ d'une loi $+$ de sorte que $\mathbb{Z}/n\mathbb{Z}$ soit un groupe commutatif.

Solution Exercice 1: Démonstration du théorème de Lagrange

1. La relation $\mathcal{R}$ est déjà réflexive puisque pour tout $x \in G$, nous avons $x \circ x^{-1} = e_G \in H$ puisque H sous-groupe de G (donc il contient l'élément neutre e_G de G). Ainsi, nous avons $x\mathcal{R}x$. La relation est aussi symétrique: en effet, si x et y sont deux élements de E vérifiants $x\mathcal{R}y$, alors $x \circ y^{-1} \in H$. Or, H est un sous-groupe de G donc $(x \circ y^{-1})^{-1} \in H$. Or, $(x \circ y^{-1})^{-1} = y \circ x^{-1}$, soit donc $y\mathcal{R}x$. Enfin, montrons que la relation $\mathcal{R}$ est transitive: supposons que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors $xy^{-1} \in H$ et $yz^{-1} \in H$. Comme H est un sous-groupe, il est stable par produit d'où $(xy^{-1}) \circ (yz^{-1}) = xy^{-1}yz^{-1} = xz^{-1} \in H$, ce qui implique que $x\mathcal{R}z$. Il s'ensuit donc que la relation $\mathcal{R}$ est transitive.
2.L'application f_x est clairement surjective: montrons qu'elle est injective. Supposons $y, y' \in H$ tels que $f_x(y) = f_x(y')$. Alors $x \circ y^{-1} = x \circ y'^{-1}$, soit en composant par la gauche par x^{-1} nous obtenons $y^{-1} = y'^{-1}$. Il s'ensuit alors que les deux éléments sont égaux (par unicité de l'inverse). On a ainsi $Card(H) = Card(Hx)$.
3. Faisons le lien entre la relation d'équivalence et la question précédente: $\mathcal{R}$ est donc une relation d'équivalence. Aussi, on peut partitionner le groupe G en classes d'équivalences. Si x est fixé, sa classe d'équivalence est l'ensemble des y tels que $x\mathcal{R}y$ ou encore $y\mathcal{R}x$ (puisque la relation est réflexive). Ainsi, c'est l'ensemble des $y \in G$ tels que $y \in xH$: c'est par définition l'ensemble xH. Aussi, G est partitionné en $n = Card(G/\mathcal{R})$ classes d'équivalences, ayant toutes même cardinal: $Card(H)$. Enfin, puisque G est union disjointe de ses classes, nous en déduisons que $Card(G) = n \times Card(H)$, d'où l'ordre du sous-groupe H divise l'ordre du groupe G.

Solution exercice 2: Loi de groupe produit

Attention aux notations dans cet exercice: il faut bien voir que la même notation $\star$ désigne trois choses différentes: les lois sur G_1 et G_2, qui sont données, et la loi $\star$ sur le produit cartésien dont on veut démontrer qu'elle lui donne une structure de groupe... Pour plus de précision, nous notons $\star_1$ la loi du groupe G_1 et $\star_2$ celle sur G_2.

Montrons que $(G_1 \times G_2, \star)$ est un groupe. On vérifie bien que la loi $\star$ définie sur le produit cartésien $G_1 \times G_2$ est une loi de composition interne sur $G_1 \times G_2$ (c'est-à-dire qu'à deux éléments de $G_1 \times G_2$, elle associe un unique élément de $G_1 \times G_2$), et est associative puisque les lois des groupes $(G_1, \star_1)$ et $(G_2, \star_2)$ le sont aussi. Ainsi, $\forall (x,y), (x',y')$ et $(x'',y'') \in G_1 \times G_2$, nous avons

$$\begin{aligned}(x,y) \star ((x',y') \star (x'',y'')) &= (x,y) \star (x' \star_1 x'', y' \star_2 y'') = (x \star_1 (x' \star_1 x''); y \star_2 (y' \star_2 y'')) \\ &= ((x \star_1 x') \star_1 x''; (y \star_2 y') \star_2 y'') = (x \star_1 x'; y \star_2 y') \star y'' \\ &= ((x,y) \star (x',y')) \star (x'',y'')\end{aligned}$$

De plus, $G_1 \times G_2$ admet un élément neutre pour cette loi: en effet, si e_1 et e_2 désignent respectivement les éléments neutres de G_1 et G_2, alors l'élément $(e_1, e_2) \in G_1 \times G_2$ vérifie $\forall (x,y) \in G_1 \times G_2$, $(e_1, e_2) \star (x,y) = (e_1 \star_1 x; e_2 \star_2 y) = (x;y)$. Reste alors à vérifier que tout élément (x,y) de $G_1 \times G_2$ admet bien un symétrique pour $\star$. Désignons par x^{-1} et y^{-1} respectivement les symétriques de x et y dans $(G_1, \star_1)$ et $(G_2, \star_2)$. Alors $(x,y) \star (x^{-1}, y^{-1}) = (x \star_1 x^{-1}, y \star_2, y^{-1}) = (e_1, e_2)$ d'où (x^{-1}, y^{-1}) est l'inverse de (x,y) dans $(G_1 \times G_2, \star)$, ce qui le muni donc d'une structure de groupe.

Solution exercice 3: Produit de deux sous-groupes

1. Montrons que $AB = \{ab, a \in A, b \in B\}$ est un sous-groupe de G. Déjà, AB est non vide puisque $e \in A$ et $e \in B$ puisque se sont des sous-groupes, d'où $e \in AB$. Ensuite, le produit de deux éléments de AB est aussi un élément de AB puisque G est commutatif. Reste à montrer que AB est stable par passage au symétrique: si $ab \in AB$, alors $a^{-1}b^{-1} \in AB$ et vérifie $ab \times a^{-1}b^{-1} = 1$. Il s'ensuit que AB est un sous-groupe de G.

2 Soient $(a,b), (a',b') \in A \times B$. Alors $f((a,b) \times (a',b')) = f((aa', bb')) = aa'bb' = f((a,b)) \times f((a',b'))$, d'où f est bien un morphisme de groupes. Reste à montrer que c'est un isomorphisme. Pour ce faire, considérons $f((a,b)) = f((a',b'))$. Alors $ab = a'b'$, et donc $bb'^{-1} = a'a^{-1}$. Aussi, l'élément $a'a^{-1} = bb'^{-1} = e$ car appartient à la fois à A et B. Par unicité de l'inverse d'un élément, nous en déduisons que $a = a'$ et $b = b'$ d'où f est injective. Elle est clairement surjective, d'où f réalise une bijection de $A \times B$ dans AB.

3.a Supposons G fini de cardinal $n = 2m$, et qu'il existe $a, b \in G$ avec $o(a) = m$ et $o(b) = 2$, et tel que $b \notin < a >$. Supposons donc l'existence de $i, j \in \{1, 2, \cdots, n\}$ tels que $a^i = a^j$ et raisonnons par l'absurde en supposant par exemple que $i < j$. Nous déduisons alors que $a^{j-i} = 1_G$. Or, $1 < j - i < m$ d'où nous obtenons une contradiction avec le fait que $o(a) = m$.

3.b La question précédente implique directement que $Card(\{a^i, i \in \{1, \cdots, m\}) = m$. Ensuite, tout élément de la forme $a^i b$ n'est pas un élément de $< a >$ puisque sinon, nous aurions $b \in < a >$ ce qui n'est pas. Aussi les deux ensembles en question sont-ils disjoints. Enfin, il est aisé de voir que tous les éléments de $a^i b$ sont différents puisque si $a^i b = a^j b$ alors $a^i = a^j$ et donc par la question précédente, $i = j$. Aussi, nous en déduisons que le cardinal de l'ensemble considéré est égal à $2m$.

3.c Nous savons que, par définition du produit de deux groupes, $< a >< b >= \{a^i b^j, i \in \{1, \cdots, m\}, j \in \{1, 2\}\}$ est un sous-groupe de G de même cardinal que G d'où $G =< a >< b >$.

3.d Reprenons l'application f de la question 1 avec $A =< a >$ et $B =< b >$. Nous en déduisons alors que $< a > \times < b >$ est isomorphe à $G =< a >< b >$.

Solution exercice 4: Groupes dihédraux

Nous allons déjà montrer que D_n est un sous-groupe du groupe des isométries du plan. Il est clair que D_n est non vide puisqu'il contient Id, l'élément neutre de $\mathcal{I}s(\mathbb{R}^2)$. Ensuite, la composée de deux isométries conservant l'ensemble des sommets d'un polygône régulier est une isométrie conservant cet ensemble. Enfin, si une isométrie conserve globalement les sommets du polygône régulier, alors son inverse aussi. Il s'ensuit donc que D_n est un sous groupe de $(\mathcal{I}s(\mathbb{R}^2), \circ)$, donc est un groupe pour la composition.

Pour dénombrer ce groupe, notons $A_0, \cdots, A_{n-1}$ les sommets du polygônes régulier à n sommets. Alors nous avons n choix pour obtenir l'image par f une telle isométrie de A_0 par une isométrie: notons $f(A_0)$ celle-ci. Alors, pour A_1, puisque nous considérons une isométrie, nous devons avoir $A_0A_1 = f(A_0)f(A_1)$ donc $f(A_1)$ est nécessairement l'un des deux sommets adjacents à $f(A_0)$: aussi, nous avons deux choix possibles. Pour l'image de A_3, par le précédent raisonnement c'est un voisin de $f(A_1)$, mais l'un d'eux est déjà l'image de A_0 par l'isométrie f, et comme une isométrie est bijective, nous en déduisons que nous n'avons d'autre choix pour $f(A_3)$ que l'autre voisin de $f(A_1)$. Aussi, nous en déduisons qu'il y a $2n$ isométries possibles conservant globalement les sommets d'un polygône régulier à n sommets.

2. Considérons à présent un triangle équilatéral ABC. Les isométries conservant globalement ses sommets sont: l'identité, la rotation r de centre O et d'angle $\frac{2\pi}{3}$, la rotation r^2 de centre O et dans $\frac{4\pi}{2}$. Enfin, les 3 symétries s_{Δ_A}, s_{Δ_B} et s_{Δ_C} par rapports aux bissectrices laissent globalement invariants les sommets du triangle, d'où nous en déduisons que nous avons obtenus les 6 isométries de D_3. Nous pouvons alors dresser la table de ce groupe:

	Id	r	r^2	s_{Δ_A}	s_{Δ_B}	s_{Δ_C}
Id	Id	r	r^2	s_{Δ_A}	s_{Δ_B}	s_{Δ_C}
r	r	r^2	Id	s_{Δ_C}	s_{Δ_A}	s_{Δ_B}
r^2	r^2	Id	r	s_{Δ_B}	s_{Δ_C}	s_{Δ_A}
s_{Δ_A}	s_{Δ_A}	s_{Δ_B}	s_{Δ_C}	Id	r	r^2
s_{Δ_B}	s_{Δ_B}	s_{Δ_C}	s_{Δ_A}	r^2	Id	r
s_{Δ_C}	s_{Δ_C}	s_{Δ_A}	s_{Δ_B}	r	r^2	Id

On voit alors que D_3 est isomorphe à S_3. En effet, considérons $\Phi : S_3 \to D_3$ qui envoie la permutation $(1,2,3)$ sur la rotation r et la transposition $(2,3)$ sur s_{Δ_A}. Alors les deux tables sont identiques, d'où les deux groupes sont isomorphes.
3. COnsidérons P_n un polynôme régulier à n sommets. Alors D_n admet la rotation de centre O et d'angle $2\pi/n$ pour élément r d'ordre n et la symétrie par rapport à la médiatrice d'un côté comme élément s d'ordre 2.
$s \notin < r >$ puisque s est impaire (change l'orientation) alors que r est pair (conserve l'orientation).
4. Tout élément de D_n s'écrit donc $r^i \circ s^j$ où $i \in \{1, \cdots, n\}$ et $j \in \{1, 2\}$.
5. Il s'ensuit alors que D_n est isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Solution des tests

Test 1. La loi $\star$ est *associative* si pour tout triplet (x, y, z) d'éléments de G, nous avons $a \star (b \star c) = (a \star b) \star c$. On dit que $e \in G$ est un *élément neutre* de G si pour tout élément $x \in G$, on a: $x \star e = e \star x = x$. Si $x \in G$, on appel *symétrique* de x dans G tout élément y de G vérifiant $x \star y = y \star x = e$.
Test 2. Un groupe est dit *abélien* ou *commutatif* si pour tout couple d'éléments $(x, y) \in G^2$ nous avons $x \star y = y \star x$. Le groupe $(\mathbb{Z}; +)$ est un exemple de groupe commutatif alors que $(\mathcal{G}l_n(\mathbb{R}), \circ)$ n'en est pas un.
Test 3. Sont des groupes! $(\mathbb{Z}; +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^*, \times)$, $(\mathcal{M}_n(\mathbb{R}), +)$, $(\mathbf{GL}_n(\mathbb{R}), \times)$. Ne sont pas des groupes: $(\mathbb{Z}, -)$ ($-$ n'est pas une loi associative), $(\mathbb{Z}^*; \times)$ (2 n'a pas d'inverse), $(\mathbb{Q}, \times)$ (0 n'a pas d'inverse).
Test 4. Supposons que e et e' soient des éléments neutres de G: alors, par définition de e neutre, on a: $\forall x \in G$, $x \star e = e \star x = x$ d'où en considérant cette relation pour $x = e'$ nous avons: $e' \star e = e \star e' = e$. En utilisant le fait que e' soit un élément neutre (avec $e \in G$) nous obtenons: $e \star e' = e' \star e = e'$, d'où $e = e'$. Le groupe G admet donc un unique élément neutre.
Supposons que y et y' soient deux éléments symétriques de x. Nous avons alors $y \star x = x \star y = e$. En composant cette relation par y' on a: $y' = y' \star (y \star x) = y' \star (x \star y)$. Comme la loi $\star$ est associative, nous obtenons que $y' \star (x \star y) = (y' \star x) \star y = e \star y = y$.
Test 5. La méthode classique pour montrer que $(A, \star)$ est un sous-groupe de G est de montrer que A est non vide (entendre qu'il contient l'élément neutre), qu'il est stable par produit (i.e. $\forall (a, a') \in A$, $a \times a' \in A$) et que pour tout élément de A, son symétrique (défini dans G) appartient à A (i.e. $\forall a \in A$, $a^{-1} \in A$).
Un critère équivalent mais bien plus rapide est de montrer que $A \neq \emptyset$ et $\forall (a, a') \in A$, $a \star a'^{-1} \in A$.
Test 6. Soient A et B deux sous-groupes de G. Montrons que $A \cap B$ est encore un sous-groupe de G: comme $e \in A$ et $e \in B$ donc $e \in A \cap B$. De plus, si $x \in A \cap B$, alors $x \in A$ sous-groupe de G implique $x^{-1} \in A$ et de même pour $x^{-1} \in B$, d'où $x^{-1} \in A \cap B$. Enfin, soient x et y dans $A \cap B$. Comme le prouit $x \star y$ appartient à la fois à A et B (puisque se sont des sous-groupes de G), on en déduit que $x \star y \in A \cap B$. On montre ainsi que l'intersection de deux sous-groupes est encore un sous-groupe. Cela s'étend immédiatement à l'intersection finie de sous-groupes.
Test 7. C'est faux: l'union de deux sous-groupes n'est pas nécessairement est un sous-groupe. En fait, si H_1 et H_2 sont des sous-groupes de G alors $H_1 \cup H_2$ est un sous-groupe si $H_1 \subset H_2$ ou $H_2 \subset H_1$. Pour le montrer, on raisonne par l'absurde: si $H_1 \not\subset H_2$ et $H_2 \not\subset H_1$, il existe $x_1 \in H_1 \setminus H_2$ et $x_2 \in H_2 \setminus H_1$. L'union étant un sous-groupe, le produit $x_1 \star x_2$ est un élément de $H_1 \cup H_2$, donc soit $x_1 \star x_2 \in H_1$, soit $x_1 \star x_2 \in H_2$. Dans le premier cas, nous avons que $x_2 = x_1^{-1} \star h_1$ (avec $h_1 \in H_1$) d'où $x_2 \in H_1$ ce qui est absurde. Le second cas est similaire (en échangeant les rôles de x_1 et x_2). On démontre donc que l'hypothèse initiale ($H_1 \not\subset H_2$ et $H_2 \not\subset H_1$) est absurde, donc que $H_1 \subset H_2$ ou $H_2 \subset H_1$.
Test 8. Pour que cette définition ait un sens, il faut vérifier que *le plus petit sous-groupe (au sens de l'inclusion) contenant* x existe bien. Déjà, montrons qu'il en existe au moins un: nous savons que G est un sous-groupe (trivial) de G, donc il existe bien un sous-groupe de G contenant x. Ensuite, considérons $\cap H_x$ l'intersection de tous les sous-groupes contenant x. Comme l'intersection de deux sous-groupes est un sous-groupe, nous

déduisons que c'est un sous-groupe de G et qu'il contient x (puisque tous les sous-groupes considérés dans cette intersection le contiennent). Enfin, on vérifie alors qu'un tel sous-groupe est bien minimal au sens de l'inclusion (il ne peut exister un autre sous-groupe de G contenant x qui soit strictement compris dans celui-ci). La définition de groupe engendré par un élément a donc bien un sens.

Test 9. On définit le sous-groupe engendré par la partie A comme l'intersection de tous les sous-groupes de G qui contiennent A (ou d'un point de vue plus théorique, comme le plus petit sous-groupe (au sens de l'inclusion) de G qui contient la partie A).

Test 10. $< \{e_G\} >= \{e_G\}$. En effet, le singleton $\{e_G\}$ est un sous-groupe de G contenant e_G... et c'est le plus petit possible! Notez que généralement, on note $< x >$ au lieu de $< \{x\} >$ (i.e. on devrait définir uniquement les sous-groupes engendré par une partie, éventuellement à un élément).

Test 11. Soit $\varphi : G \to G'$ un morphisme de $(G, \star)$ dans $(G', \cdot)$. Nous avons donc $\forall (x, y) \in G^2$, $\varphi(x \star y) = \varphi(x) \cdot \varphi(y)$. Aussi, en particularisant $y = e_G$, nous avons $\varphi(x) = \varphi(x \star e_G) = \varphi(x) \cdot \varphi(e_G)$. Aussi, nous en déduisons que $\varphi(e_G) = e_{G'}$.
De même, pour $y = x^{-1}$ nous avons $e_{G'} = \varphi(e_G) = \varphi(x \star x^{-1}) = \varphi(x) \cdot \varphi(x^{-1})$. Aussi, par définition de l'inverse d'un élément de G' nous en déduisons que $\varphi(x)^{-1} = \varphi(x^{-1})$. *Notez que l'on utilise l'unicité de l'inverse d'un élément ici.*

Test 12. L'image directe de la partie H par l'application φ est $\varphi(H) = \{y \in G', \exists x \in H, y = \varphi(x)\} = \{\varphi(x) | x \in H\}$.

Test 13. Si H' est une partie de G', l'image réciproque de H' par l'application φ est $\varphi^{-1}(H') = \{x \in G | \varphi(x) \in H'\}$. *Notez que $\varphi^{-1}(H')$ est une partie, et n'implique pas l'existence d'une application réciproque φ^{-1} à φ. En fait, si $\forall y \in G'$, $\varphi^{-1}(\{y\})$ est un singleton, alors l'application φ admet une application réciproque, notée φ^{-1} donc (et se sont toutes deux des bijections).*

Test 14. Les sous-groupes triviaux de G sont $\{e\}$ et G lui-même. On vérifie très facilement que sont tous deux des sous-groupes distingués de G (par exemple $x\{e_G\} = x = \{e_G\}x$...).

Test 15. Si G est abélien, alors tout sous-groupe H vérifie $\forall x \in G$, $xH = Hx$ d'où tout sous-groupe de G est distingué.