TD1 : Généralités sur les groupes

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆
Soit E un ensemble muni d'une loi de composition, associative, avec élément neutre e, et telle que tout élément de E possède un inverse à gauche. Montrer que tout élément de E possède un inverse à droite qui coïncide avec son inverse à gauche. En déduire que E est un groupe.

Solution de l'exercice 1. Soit $g \in E$. Par hypothèse, il existe $h \in E$ tel que $h \cdot g = e$.
De même, il existe $k \in E$ tel que $k \cdot h = e$. L'associativité assure alors que $g = (k \cdot h) \cdot g = k \cdot (h \cdot g) = k$, donc $g \cdot h = e$, donc h est aussi inverse à droite de g.
Par conséquent, tout élément de E admet un inverse (à droite et à gauche), donc E est un groupe.

Exercice 2 : ⋆
Soit G un groupe tel que $g^2 = e$ pour tout $g \in G$. Montrer que G est abélien.

Solution de l'exercice 2. Pour tous $g, h \in G$, on a $(g \cdot h)^2 = e$, i.e. $g \cdot h \cdot g \cdot h = e$, donc en multipliant à droite par $h \cdot g$, on a $g \cdot h = h \cdot g$, i.e. G est commutatif.

Exercice 3 : ⋆
Soit G un groupe et soit H un sous-ensemble fini non vide de G stable pour la loi de composition du groupe G.

a) Montrer que H est un sous-groupe de G.
b) Trouver un exemple d'un groupe G et d'un sous-ensemble non vide de G stable pour la loi de composition du groupe G qui ne soit pas un sous-groupe de G.

Solution de l'exercice 3.

a) Soit $h \in H$. Comme H est fini et $h^n \in H$ pour tout $n \in \mathbb{N}$, il existe deux entiers $n > m \geq 0$ tels que $h^n = h^m$. Or h admet un inverse dans G, donc on en déduit l'égalité suivante de G : $h^{n-m} = e$. Or H est stable par multiplication, donc $e \in H$ et $h^{-1} = h^{n-m-1} \in H$, donc H est stable par inverse. Cela assure que H est un sous-groupe de G.
b) On peut prendre $G = (\mathbb{Z}, +)$ et $H = \mathbb{N}$.

Exercice 4 : ⋆
Soit G un groupe et soit H un sous-groupe de G d'indice 2. Montrer que H est distingué dans G.

Solution de l'exercice 4. Les classes à gauche de G modulo H sont $\{H, G \setminus H\}$. Donc les classes à droite de G modulo H sont $\{H, G \setminus H\}$. Si $g \notin H$, on a donc $g \cdot H = G \setminus H = H \cdot g$, ce qui assure le résultat.

Exercice 5 :
Soit G un groupe fini.

a) Montrer que des éléments conjugués dans G sont de même ordre.
b) Deux éléments de même ordre dans G sont-ils toujours conjugués ?
c) Trouver tous les groupes abéliens finis G pour lesquels la question précédente a une réponse positive. Un exemple non abélien ?

Solution de l'exercice 5.

a) Si $g, h \in G$ et $n \in \mathbb{N}$, on a $(h \cdot g \cdot h^{-1})^n = h \cdot g^n \cdot h^{-1}$, donc $(h \cdot g \cdot h^{-1})^n = e$ si et seulement si $g^n = e$, ce qui assure le résultat.

b) Non. Par exemple, dans le groupe commutatif $G = \mathbb{Z}/3\mathbb{Z}$, on a deux éléments d'ordre 3 qui ne sont pas conjugués.

c) Dans un groupe abélien fini, les classes de conjugaison sont réduites à un élément. Donc la question précédente a une réponse positive dans un groupe abélien fini G si et seulement si tous les éléments de G ont des ordres distincts. Or si un groupe admet un élément g d'ordre $n \geq 3$, alors il admet d'autres éléments d'ordre n, par exemple g^{-1}. Donc les seuls groupes abéliens convenables sont le groupe trivial et le groupe $\mathbb{Z}/2\mathbb{Z}$.

Si $G = \mathfrak{S}_3$, alors les éléments d'ordre 2 dans G sont les transpositions $(12), (13), (23)$ qui sont bien conjuguées, et les éléments d'ordre 3 sont les 3-cycles (123) et (132), qui sont également conjugués. Donc G est un exemple de groupe non abélien convenable.

Exercice 6 :
Soit $f : G_1 \to G_2$ un morphisme de groupes et soit x un élément de G_1 d'ordre fini. Montrer que l'ordre de $f(x)$ divise l'ordre de x.

Solution de l'exercice 6. On note n l'ordre de x. On a $x^n = e$, donc $f(x)^n = f(x^n) = e$, donc l'ordre de $f(x)$ divise n.

Exercice 7 : $\star$
Montrer qu'il n'existe pas de morphisme de groupes surjectif de $(\mathbb{Q}, +)$ dans $(\mathbb{Q}_+^*, \times)$.

Solution de l'exercice 7. Soit $\phi : (\mathbb{Q}, +) \to (\mathbb{Q}_+^*, \times)$ un morphisme surjectif. Alors $2 \in \mathbb{Q}_+^*$ admet un antécédent x par φ. Alors $y := \frac{x}{2} \in \mathbb{Q}$ vérifie que $2y = x$, donc $\varphi(y)^2 = \varphi(x) = 2$. Par conséquent, on a construit un rationnel $\varphi(y) \in \mathbb{Q}_+^*$ tel que $\varphi(y)^2 = 2$, ce qui contredit l'irrationnalité de $\sqrt{2}$.

Exercice 8 :
Donner la liste de tous les groupes (à isomorphisme près) de cardinal inférieur ou égal à 7.

Solution de l'exercice 8.
- le seul groupe de cardinal 1 est le groupe trivial.
- si p est un nombre premier et si G est de cardinal p, alors tout élément $g \in G$ distinct de l'élément neutre est d'ordre p, ce qui assure que G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Il y a donc un unique groupe de cardinal p (qui est $\mathbb{Z}/p\mathbb{Z}$) pour $p = 2, 3, 5, 7$.
- Soit G un groupe d'ordre 4. Si G admet un élément d'ordre 4, G est isomorphe à $Z/4\mathbb{Z}$. Sinon, tous ses éléments sont d'ordre 1 ou 2. Donc G est abélien, et le choix de deux éléments distincts (non neutres) g et h de G fournit un isomorphisme entre G et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il y a donc exactement deux groupes d'ordre 4.
- Soit G un groupe d'ordre 6. Si G est commutatif, G admet nécessairement un élément d'ordre 2 et un élément d'ordre 3 (sinon tous les éléments de G sont d'ordre divisant 2, auquel cas G contient $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, ce qui n'est pas possible, ou tous les élélléments de G sont d'ordre divisant 3, auquel cas G contient $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, ce qui n'est pas possible non plus). Alors le produit de ces deux éléments est d'ordre 6, ce qui assure que G est isomorphe à $\mathbb{Z}/6\mathbb{Z}$.
  Si G n'est pas commutatif : alors G contient un élément d'ordre 3, noté a, et aussi un élément b d'ordre 2 (sinon on montre que G aurait au moins 7 éléments). Nécessairement, a et b ne commutent pas, et ils engendrent G. Les éléments de G sont donc $e, a, a^2, b, a \cdot b, b \cdot a$. Donc néssairement on a $a^2 \cdot b = b \cdot a$ et $b \cdot a^2 = a \cdot b$, ce qui détermine complétement la table de multiplication de G. Il y a donc au plus un groupe non commutatif d'ordre 6. Or $\mathfrak{S}_3$ en est un, donc c'est le seul.
  Il y a donc exactement deux groupes d'ordre 6 : $\mathbb{Z}/6\mathbb{Z}$ et $\mathfrak{S}_3$.

Exercice 9 : $\star\star$
Soit G un groupe tel que le quotient par son centre est monogène. Prouver que G est abélien.

Solution de l'exercice 9. On rappelle que le centre $Z(G)$ de G est distingué. On considère le morphisme quotient $\pi : G \to G/Z(G)$. Par hypothèse, $G/Z(G)$ est engendré par un élément $\overline{g_0}$. Comme π est surjective, il existe $g_0 \in G$ tel que $\pi(g_0) = \overline{g_0}$. Soient alors $g, h \in G$. Il existe des entiers $n, m \in \mathbb{Z}$ tels que $\pi(g) = \overline{g_0}^n$ et $\pi(h) = \overline{g_0}^m$. Donc $\pi(g \cdot g_0^{-n}) = \pi(h \cdot g_0^{-m}) = e$, donc $y = g \cdot g_0^{-n}$ et $z = h \cdot g_0^{-m}$ sont dans $Z(G)$.
Alors

$$g \cdot h = y \cdot g_0^n \cdot z \cdot g_0^m = y \cdot z \cdot g_0^{n+m} = z \cdot g_0^m \cdot y \cdot g_0^n = h \cdot g\,,$$

donc G est commutatif.

Exercice 10 : ⋆⋆
Soit G un groupe. Vrai ou faux ?

a) Si tout sous-groupe H de G est distingué dans G, alors G est abélien.

b) Si $H \triangleleft G$ et $K \triangleleft H$, alors $K \triangleleft G$.

c) Soient x et $y \in G$ d'ordre fini. Alors xy est nécessairement d'ordre fini.

d) Si G a un nombre fini de sous-groupes, alors G est fini.

e) Si H et K sont des sous-groupes de G, alors $\langle H \cup K \rangle = HK$.

Solution de l'exercice 10.

a) Faux. On considère par exemple le groupe H des quaternions, d'ordre 8. Ce groupe est définit de la façon suivante : l'ensemble H est

$$H = \{\pm 1, \pm i, \pm j, \pm k\}\,,$$

et la loi de groupe est définie par

$$\begin{array}{l}(-1)^2 = 1\,,\ i^2 = j^2 = k^2 = -1\,,\\ (-1) \cdot i = i \cdot (-1) = -i\,,\ (-1) \cdot j = j \cdot (-1) = -j\,,\ (-1) \cdot k = k \cdot (-1) = -k\,,\\ i \cdot j = -j \cdot i = k\,.\end{array}$$

On voit que les sous-groupes de H sont les suivants :
– le sous-groupe trivial $\{1\}$, qui est distingué.
– le sous-groupes de cardinal 2 engendré par -1, qui est distingué car contenu dans le centre de H.
– les sous-groupes de cardinal 4 sont d'indice 2 dans H, donc distingué.
– le sous-groupe H entier, qui est distingué.
Donc les sous-groupes de H sont tous distingués, alors que H n'est pas commutatif.

b) Faux. On peut prendre $G = \mathfrak{S}_4$ ou $\mathfrak{A}_4$, $H = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $K = \{\mathrm{id}, (12)(34)\} \cong \mathbb{Z}/2\mathbb{Z}$.

c) Faux. Pour avoir un contre-exemple, il faut nécessairement que le groupe G soit infini et non commutatif. On peut prendre par exemple le groupe libre sur deux générateurs a et b d'ordre 2, i.e. l'ensemble des mots finis formés des lettres a et b sans répétition, avec la loi de concaténation des mots (avec simplification éventuelle des mots aa et bb apparaissant). Dans ce groupe, les éléments a et b sont d'ordre 2, alors que leur produit $a \cdot b = ab$ est d'ordre infini.
Pour un exemple plus concret, on peut prendre $G = \mathrm{GL}_2(\mathbb{Q})$, $x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $y = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$.
Alors x est d'ordre 2, y est d'ordre 3 et $x \cdot y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini.

d) Vrai. Il est clair que tout élément de G est d'ordre fini : si $g \in G$ est d'ordre infini, alors le sous-groupe engendré par g est isomorphe à $\mathbb{Z}$, et il contient donc une infinité de sous-groupes distincts. Or G a un nombre fini de sous-groupes cycliques, noté $\langle g_1 \rangle, \ldots, \langle g_n \rangle$. Donc pour tout $g \in G$, il existe i tel que $\langle g \rangle = \langle g_i \rangle$, donc g est une puissance de g_i, ce qui assure que le cardinal de G est borné par la somme des ordres des g_i, donc G est fini.

e) Faux. Il est clair que l'inclusion $HK \subset \langle H \cup K \rangle$ est toujours vérifiée. En revanche, le sous-ensemble HK n'est en général pas un sous-groupe de G, au contraire de $\langle H \cup K \rangle$: par exemple, si on prend $G = \mathfrak{S}_3$, $H = \{\mathrm{id}, (12)\}$ et $K = \{\mathrm{id}, (13)\}$, alors on a $\langle H \cup K \rangle = G$ (de cardinal 6), alors que $HK = \{\mathrm{id}, (12), (13), (132)\}$ (de cardinal 4) n'est pas un sous-groupe de G. La réponse est en revanche affirmative si H ou K est distingué dans G.

Exercice 11 :
Soit S un sous-ensemble non vide d'un groupe fini G. Soient $N(S) := \{g \in G \mid gSg^{-1} = S\}$ et $C(S) := \{g \in G \mid \forall s \in S\,, gsg^{-1} = s\}$ le normalisateur et le centralisateur de S dans G. Montrer que :

a) $N(S) < G$ et $C(S) \triangleleft N(S)$.

b) $N(S) = G$ si et seulement si $S = \bigcup_{g \in G} gSg^{-1}$.

c) Si $H \triangleleft G$, alors $C(H) \triangleleft G$.

d) Si $H < G$, alors $N(H)$ est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.

Solution de l'exercice 11.

a) On a $e \in N(S)$. Soient $g, h \in N(S)$. Alors on a $(gh)S(gh)^{-1} = g(hSh^{-1})g^{-1} = gSg^{-1} = S$, donc $gh \in N(S)$. Si $g \in N(S)$, on a $gSg^{-1} = S$, donc en multipliant à gauche et à droite par g^{-1} et g respectivement, on a $S = g^{-1}Sg$, donc $g^{-1} \in N(S)$. Donc $N(S)$ est un sous-groupe de G. De même, il est clair que $C(S)$ est un sous-groupe de G contenu dans $N(S)$. Montrons qu'il est distingué dans $N(S)$. Soit $g \in C(S)$ et $h \in N(S)$. Soit $s \in S$. Alors

$$(hgh^{-1})s(hgh^{-1})^{-1} = hg(h^{-1}sh)g^{-1}h^{-1}\,,$$

et comme $h \in N(S)$, on a $h^{-1}sh \in S$, donc comme $g \in C(S)$, $g(h^{-1}sh)g^{-1} = h^{-1}sh$, donc finalement $(hgh^{-1})s(hgh^{-1})^{-1} = h(h^{-1}sh)h^{-1} = s$, donc $hgh^{-1} \in C(S)$, donc $C(S) \triangleleft N(S)$.

b) On suppose $N(S) = G$. Alors pour tout $g \in G$, on a $gSg^{-1} = S$, donc $S = \bigcup_{g \in G} gSg^{-1}$. Réciproquement, si on suppose $S = \bigcup_{g \in G} gSg^{-1}$, pour tout $g \in G$, on a donc $g^{-1}Sg \subset S$, donc en multipliant par g et g^{-1} à gauche et à droite respectivement, on a $S \subset gSg^{-1} \subset S$, ce qui assure que $gSg^{-1} = S$, donc $g \in N(S)$, donc $G = N(S)$.

c) On suppose H distingué dans G. Soit $g \in G$ et $c \in C(H)$. Soit enfin $h \in H$. On calcule $(gcg^{-1})h(gcg^{-1})^{-1} = gc(g^{-1}hg)c^{-1}g^{-1}$: puisque H est distingué dans G, on sait que $g^{-1}hg \in H$. Or $c \in C(H)$, donc $c(g^{-1}hg)c^{-1} = g^{-1}hg$, donc finalement $(gcg^{-1})h(gcg^{-1})^{-1} = g(g^{-1}hg)g^{-1} = h$, ce qui assure que $gcg^{-1} \in C(H)$. Donc $C(H)$ est distingué dans G.

d) Par définition et via la question a), il est clair que $N(H)$ est un sous-groupe de G contenant H, et que H est distingué dans $N(H)$. Soit maintenant K un sous-groupe de G contenant H tel que $H \triangleleft K$. Alors par définition, pour tout $k \in K$, on a $kHk^{-1} = H$, donc $k \in N(H)$, donc $K \subset N(H)$, ce qui assure la maximalité de $N(H)$ parmi les sous-groupes de G concernés.

Exercice 12 : $\star\star$
Soit G un groupe et soit $H \triangleleft G$ un sous-groupe distingué.

a) Décrire les sous-groupes distingués de G/H en fonction de ceux de G.

b) Soit K un sous-groupe de G.

i) Si K est distingué dans G et contient H, montrer que l'on a un isomorphisme $(G/H)/(K/H) \cong G/K$.

ii) Montrer que HK est un sous-groupe de G égal à KH.

iii) Montrer que H est distingué dans HK.

iv) Montrer que l'on a un isomorphisme $K/(K \cap H) \cong (HK)/H$.

Solution de l'exercice 12.

a) On note $\pi : G \to G/H$ la projection canonique. On sait que la correspondance $K \mapsto \pi(K)$ établit une bijection entre l'ensemble des sous-groupes de G contenant H est l'ensemble des sous-groupes de G/H, dont la réciproque est donnée par $\overline{K} \mapsto \pi^{-1}(\overline{K})$. On vérifie immédiatemment que cette bijection induit une bijection entre les sous-groupes distingués de G contenant H et les sous-groupes distingués de G/H.

b) i) Le morphisme $\pi : G \to G/H$, composé avec la projection $\pi' : G/H \to (G/H)/(K/H)$, induit un morphisme surjectif $q : G \to (G/H)/(K/H)$. Par construction, un élément $g \in G$ est dans $\mathrm{Ker}(q)$ si et seulement si $\pi(g) \in \mathrm{Ker}(\pi') = K/H$ si et seulement si $g \in K$. Donc $\mathrm{Ker}(q) = K$. Le théorème de factorisation assure alors que q induit un isomorphisme $\overline{q} : G/K \xrightarrow{\simeq} (G/H)/(K/H)$.

ii) Soient $h, h' \in H$ et $k, k' \in K$. Comme H est distingué dans G, il existe $h'' \in H$ tel qu'on ait $k \cdot h' = h'' \cdot k$, donc $(h \cdot k) \cdot (h' \cdot k') = (h \cdot h'') \cdot (k \cdot k') \in HK$, donc HK est un sous-groupe de G.

Puisque pour tous $h \in H$ et $k \in K$, il existe $h' \in H$ tel que $h \cdot k = k \cdot h'$, on voit que $HK \subset KH$. De même, pour tous $h \in H$ et $k \in K$, il existe $h' \in H$ tel que $k \cdot h = h' \cdot k$, donc $HK = KH$.

iii) C'est évident.

iv) L'inclusion $K \to HK$ induit un morphisme $p : K \to (HK)/H$. Montrons que p est surjectif : si $h \in H$ et $k \in K$, on voit que la classe $(h \cdot k)H = kH$ est l'image de k par p, donc p est surjectif. En outre, un élément $k \in K$ est dans $\mathrm{Ker}(p)$ si et seulement si il est dans H, donc $\mathrm{Ker}(p) = K \cap H$. Le théorème de factorisation permet de conclure.

Exercice 13 :
Quel est le nombre minimal de transpositions nécessaires pour engendrer le groupe $\mathfrak{S}_n$.

Solution de l'exercice 13. Montrons que ce nombre vaut $n-1$. Il est clair qu'il existe une famille de $n-1$ transpositions engendrant $\mathfrak{S}_n$ (par exemple les transpositions de la forme $(1i)$, avec $2 \leq i \leq n$). Montrons que l'on ne peut pas faire mieux. Soit $E \subset \mathfrak{S}_n$ un ensemble de transpositions. On considère le graphe fini Γ dont les sommets sont les entiers $1, 2, \ldots, n$, de sorte que deux sommets distincts i et j sont reliés par une arête si et seulement si $(ij) \in E$. Supposons la partie E génératrice. Alors il est clair que le graphe Γ est connexe.
Il suffit donc de montrer, par récurrence sur n, qu'un graphe connexe à n sommets possède au moins $n-1$ arêtes : le cas $n = 2$ est évident. Montrons l'hérédité : soit donc un tel graphe Γ, connexe à $n+1$ sommets. On a l'alternative suivante :
– soit chaque sommet a au moins deux voisins. Alors le nombre total d'arêtes est au moins égal à $\frac{1}{2}(n+1) \cdot 2 = n+1$.
– soit il existe un sommet s ayant un unique voisin. On considère alors le graphe Γ' dont les sommets sont les sommets de Γ autres que s et les arêtes celles de Γ autres que celle contenant s. Alors il est clair que Γ' est un grpahe connexe à n sommets, donc il admet au moins $n-1$ arêtes, donc Γ a au moins n arêtes.
Cela conclut la preuve par récurrence.

Exercice 14 : $\star\star\star$
Soit G un groupe de type fini

a) Un sous-groupe H de G est-il nécessairement de type fini ?

b) Même question en supposant de plus que le cardinal de G/H est fini.

Solution de l'exercice 14.

a) Non. Un contre-exemple est donné par le groupe libre G sur deux générateurs a et b, et H le sous-groupe engendré par tous les éléments de la forme ab^n, avec $n \in \mathbb{N}$. Supposons que H soit de type fini. Alors il existe un entier N tel que dans tout mot de H, le nombre de b consécutifs est toujours strictement inférieur à N. Or il est clair que $ab^N \in H$, ce qui est contradictoire. Donc H n'est pas de type fini, alors que G l'est.

Un autre exemple est donné par le sous-groupe G de $\mathrm{GL}_2(\mathbb{Q})$ engendré par les matrices $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, et le sous-groupe H de G formé des matrices de G avec des 1 sur la diagonale. Supposons que H soit de type fini. Alors il existe un entier $N \geq 1$ tel que H soit contenu dans le sous-groupe de $\mathrm{GL}_2(\mathbb{Q})$ formé des matrices de la forme $\begin{pmatrix} 1 & \frac{a}{N} \\ 0 & 1 \end{pmatrix}$. Or $A^{-N} \cdot B \cdot A^N = \begin{pmatrix} 1 & \frac{1}{2^N} \\ 0 & 1 \end{pmatrix}$ est dans H, ce qui est contradictoire puisque $2^N > N$, donc H n'est pas de type fini, alors que G l'est

b) On suppose G/H fini. Alors on peut trouver un nombre fini déléments $g_1 = e, \ldots, g_n$ de G tels que $G/H = \{g_1 H, \ldots, g_n H\}$. Puisque G est de type fini, on dispose de $h_1, \ldots, h_m \in G$ tels que tout éléments de G est produit des h_i. Alors pour tout i, j, il existe $1 \leq k \leq n$ et $h_{i,j} \in H$ tels que $h_i \cdot g_j = g_k \cdot h_{i,j}$.
Montons alors que les $h_{i,j}$ engendrent H. Soit $h \in H$. On sait qu'il existe des entiers $i_1, \ldots, i_r$ tels que $h = h_{i_1} \ldots h_{i_r}$. On a donc $h_{i_r} = h_{i_r} \cdot e = h_{i_r} \cdot g_1 = g_{k_r} \cdot h_{i_r,1}$, donc finalement

$$h = h_{i_1} \cdot \cdots \cdot h_{i_{r-1}} \cdot g_{k_r} \cdot h_{i_r,1} \,.$$

De même, $h_{i_{r-1}} \cdot g_{k_r} = g_{k_{r-1}} \cdot h_{i_{r-1},k_r}$, donc

$$h = h_{i_1} \cdot \cdots \cdot h_{i_{r-2}} \cdot g_{k_{r-1}} \cdot h_{i_{r-1},k_r} \cdot h_{i_r,1} \,.$$

Donc par récurrence, on trouve

$$h = g_{k_1} \cdot h_{i_1,k_2} \cdot \cdots \cdot h_{i_{r-1},k_r} \cdot h_{i_r,1} \,.$$

Enfin, h et les $h_{i,j}$ sont dans H, donc $g_{k_1} \in H$, donc $k_1 = 1$ et donc

$$h = h_{i_1,k_2} \cdot \cdots \cdot h_{i_{r-1},k_r} \cdot h_{i_r,1} \,,$$

ce qui conclut la preuve.

Exercice 15 : $\star\star$
On dit qu'un groupe G est d'exposant e si e est le plus petit entier $n \geq 1$ tel que pour tout $g \in G$, on a $g^n = 1$. Pour quels entiers e un groupe d'exposant e est-il nécessairement commutatif ?

Solution de l'exercice 15. On a déjà vu que $e = 2$ convenait. Et $e = 1$ aussi évidemment. Montrons que ce sont les entiers convenables. Supposons que e soit divisible par 4. Alors le groupe $G = \mathbb{Z}/e\mathbb{Z} \times H$, où H est le groupe des quaternions d'ordre 8, est d'exposant e et n'est pas commutatif (car H ne l'est pas).
Supposons $e \geq 3$ non divisible par 4. Alors e admet un facteur premier impair p. On considère alors le groupe $G = \mathbb{Z}/e\mathbb{Z} \times U(p)$, où $U(p)$ est le sous-groupe de $\mathrm{GL}_p(\mathbb{F}_p)$ formés des matrices triangulaires supérieures avec des 1 sur la diagonale. On voit facilement que G est d'exposant e et n'est pas commutatif, car $U(p)$ n'est pas commutatif.

Exercice 16 :

a) Prouver que les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

b) Prouver que les sous-groupes non denses de $\mathbb{R}$ sont les $a\mathbb{Z}$, avec $a \in \mathbb{R}$.

Solution de l'exercice 16.

a) Soit G un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$. Alors $G \cap \mathbb{N}^*$ admet un plus petit élément noté n. Soit alors $x \in G$. Écrivons la divisions euclidienne de x par n : il existe $q, r \in \mathbb{N}$ tel que $x = nq + r$, avec $0 \leq r < n$. Comme $x, n \in G$ et $r = x - nq$, on a $r \in G \cap \mathbb{N}$ et $r < n$. Donc la minimalité de n assure que $r = 0$, donc $x = nq \in n\mathbb{Z}$. Cela prouve que $G = n\mathbb{Z}$.

b) Soit G un sous-groupe de $\mathbb{R}$ distinct de $\{0\}$ et non dense. Montrons que 0 est un point isolé de G : supposons par l'absurde que tout intervalle ouvert contenant 0 contienne un élément non nul de G. Soit $x \in G$ et I un intervalle ouvert contenant x. Alors $I - x$ est un intervalle ouvert contenant 0. Donc par hypothèse, il existe $y \neq 0 \in G \cap (I - x)$. Alors $y + x \in G \cap I$ et $y + x \neq x$. Donc G est dense dans $\mathbb{R}$, ce qui est exclu. Donc 0 est un point isolé de G. Notons alors $a := \inf G \cap \mathbb{R}_+^*$. On sait donc que $a > 0$. Montrons que $a \in G$. Par définition, il existe une suite (x_n) dans $G \cap \mathbb{R}_+^*$ convergeant vers a. Comme 0 est un point isolé de G, la suite $(x_{n+1} - x_n)$ (à valeurs dans G et convergeant vers 0) est stationnaire à 0, donc la suite (x_n) est stationnaire, donc $a \in G$.
Soit alors $x \in G \cap \mathbb{R}_+^*$. En considérant la partie entière n de $\frac{x}{a}$, on voit que $na \leq x < (n+1)a$. Alors $0 \leq x - na < a$ et $x - na \in G$, donc la minimalité de a assure que $x - na = 0$, donc $x = na$. Cela assure que $G = a\mathbb{Z}$.

Exercice 17 : $\star\star$
Soit G un groupe fini.

a) Montrer qu'il existe $n \in \mathbb{N}$ tel que G soit un sous-groupe de $\mathfrak{S}_n$.

b) Montrer qu'il existe $n \in \mathbb{N}$ tel que G soit un sous-groupe de $\mathfrak{A}_n$.

c) Montrer qu'il existe $n \in \mathbb{N}$ tel que G soit un sous-groupe de $\mathrm{GL}_n(k)$, pour tout corps k.

Solution de l'exercice 17.

a) On considère l'action de G sur lui-même par translation à gauche. Autrement dit, on regarde le morphisme de groupes $\varphi : G \to \mathfrak{S}(G)$ défini par $\varphi(g)(h) := g \cdot h$. Comme G est de cardinal n, on sait que $\mathfrak{S}(G)$ est isomorphe à $\mathfrak{S}_n$. Il suffit donc de montrer que le morphisme φ est injectif. Soit $g \in \mathrm{Ker}(\varphi)$. Alors pour tout $h \in G$, on a $g \cdot h = h$, ce qui assure (en prenant $h = e$ par exemple) que $g = e$. Donc φ st injective.

b) Au vu de la question précédente, il suffit de plonger $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+2}$. Remarquons d'abord que l'on dispose d'un morphisme injectif naturel $\iota : \mathfrak{S}_n \to \mathfrak{S}_{n+2}$ obtenu en prolongeant une bijection de $\{1, \ldots, n\}$ en une bijection de $\{1, \ldots, n+2\}$ par l'identité sur les éléments $n+1$ et $n+2$. On définit alors l'application $\psi : \mathfrak{S}_n \to \mathfrak{A}_{n+2}$ de la façon suivante : si $\sigma \in \mathfrak{A}_n$, on pose $\psi(\sigma) := \iota(\sigma)$, et si $\sigma \in \mathfrak{S}_n \setminus \mathfrak{A}_n$, on pose $\psi(\sigma) := \iota(\sigma) \circ (n, n+1)$. On vérifie facilement que ψ est un morphisme de groupes injectif, ce qui conclut la preuve.

c) Au vu de la première question, il suffit de construire un morphisme de groupes injectif de $\mathfrak{S}_n$ dans $\mathrm{GL}_n(k)$. On utilise pour cela les matrices de permutations. On a en effet une application

$$\varphi : \mathfrak{S}_n \to \mathrm{GL}_n(k)$$

définie par $\varphi(\sigma) := P_\sigma$. Il est classique que φ est un morphisme de groupes, et il est clair que celui-ci est injectif. Cela conclut la preuve.

Exercice 18 : $\star\star\star$
Déterminer les classes de conjugaison dans $\mathfrak{S}_n$. Et dans $\mathfrak{A}_n$?

Solution de l'exercice 18. Soit $c = (a_1, \ldots, a_k)$ un k-cycle dans $\mathfrak{S}_n$. Il est clair que pour tout $\sigma \in \mathfrak{S}_n$, on a

$$\sigma \circ c \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k)) .$$

Comme toute permutation se décompose de façon unique en produit de cycles à supports disjoints, on trouve immédiatemment que les classes de conjugaisons dans $\mathfrak{S}_n$ sont paramétrée par les partitions de l'entiers n. On rappelle qu'une partition de l'entier n est une famille finie d'entiers $m_i \geq 1$ tels que $m_1 \leq \cdots \leq m_r$ et $\sum m_i = n$. La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i.
La description des classes de conjugaison dans $\mathfrak{A}_n$ est un peu plus subtile. On remarque d'abord que puisque $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$, la classe de conjugaison dans $\mathfrak{S}_n$ d'un élément de $\mathfrak{A}_n$ est contenue

dans $\mathfrak{A}_n$. Comme $\mathfrak{A}_n$ est d'indice 2 dans $\mathfrak{S}_n$, pour tout $\sigma \in \mathfrak{A}_n$, la classe de conjugaison de σ dans $\mathfrak{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathfrak{A}_n$, soit réunion de deux classes de conjugaison dans $\mathfrak{A}_n$ (celle de σ et une autre).
Montrons alors que l'on est dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition.
En effet, si σ admet un cycle c de longueur paire, pour tout $\tau \in \mathfrak{S}_n$, on a $\tau\sigma\tau^{-1} = (\tau c)\sigma(\tau c)^{-1}$, ce qui assure que les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathfrak{A}_n$ coïncident. Si σ admet deux cycles $c = (a_1, \dots, a_{2k+1})$ et $c' = (a'_1, \dots, a'_{2k+1})$ de même longueur impaire, alors si on note $d := (a_1 a'_1) \dots (a_{2k+1} a'_{2k+1})$ (permutation impaire), on a pour tout $\tau \in \mathfrak{S}_n$, $\tau\sigma\tau^{-1} = (\tau d)\sigma(\tau d)^{-1}$, ce qui assure que les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathfrak{A}_n$ coïncident.
Réciproquement, si σ n'a que des cycles de longueurs impaires deux-à-deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ, et on voit facilement que $(ij) \circ \sigma \circ (ij)$ n'est pas conjuguée à σ dans $\mathfrak{A}_n$ alors qu'elle l'est dans $\mathfrak{S}_n$.

Exercice 19 :
Montrer que si $n \geq 2$, $\mathfrak{S}_{n+2}$ a deux sous-groupes non conjugués isomorphes à $\mathfrak{S}_n$.

Solution de l'exercice 19. On a vu à l'exercice 17 que l'on disposait d'un morphisme injectif canonique $\iota : \mathfrak{S}_n \to \mathfrak{S}_{n+2}$ (prolongement des bijections par l'identité sur les éléments $n+1$ et $n+2$) compatible avec la signature, i.e. tel que pour tout $\sigma \in \mathfrak{S}_n$, on a $\epsilon(\iota(\sigma)) = \epsilon(\sigma)$, et d'un morphisme injectif canonique $\psi : \mathfrak{S}_n \to \mathfrak{A}_{n+2}$. Puisque deux permutations conjuguées ont même signature, et puisqu'il existe dans $\mathfrak{S}_n$ des permutations impaires, on voit donc que les deux sous-groupes $\iota(\mathfrak{S}_n)$ et $\psi(\mathfrak{S}_\mathfrak{n})$ de $\mathfrak{S}_{n+2}$ sont isomorphes à $\mathfrak{S}_n$ et ne sont pas conjugués.

Exercice 20 : $\star\star\star$
Montrer que tout sous-groupe d'indice n dans $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

Solution de l'exercice 20.
– On suppose $n \geq 5$. On note $G = \mathfrak{S}_n$ et H un sous-groupe de G d'indice n. On note enfin $X := G/H$ l'ensemble quotient de cardinal n. On dispose de l'action naturelle de G sur X par multiplication à droite, qui induit un morphisme de groupes

$$\psi : G \to \mathfrak{S}(X) \cong \mathfrak{S}_n \,.$$

Montrons que c'est un isomorphisme : son noyau est un sous-groupe distingué de $G = \mathfrak{S}_n$, non égal à $\mathfrak{S}_n$ (car l'action est transitive). La simplicité de $\mathfrak{A}_n$ assure que ce noyau est $\mathfrak{A}_n$ ou $\{\mathrm{id}\}$. Le premier cas est impossible car l'action est transitive et $|X| > 2$. Donc ψ est injective, donc par cardinalité, c'est un isomorphisme.
On peut restreindre l'action au sous-groupe H. D'où une action de H sur X. Or le point $x := H \in X$ est clairement un point fixe pour l'action de H, donc on en déduit une action de H sur $X' := X \setminus \{x\}$. D'où un morphisme

$$\varphi : H \to \mathfrak{S}(X') \cong \mathfrak{S}_{n-1} \,.$$

Ce morphisme φ est injectif car ψ l'est, donc par cardinalité, c'est un isomorphisme, d'où la conclusion.
– Si $2 \leq n \leq 4$, on montre le résultat à la main : si $n = 2$ ou 3, le résultat est évident. Si $n = 4$, on utilise l'exercice 8 pour savoir qu'un sous-groupe d'indice 4 dans $\mathfrak{S}_4$ est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ ou $\mathfrak{S}_3$. Or $\mathfrak{S}_4$ ne contient aucun élément d'ordre 6, donc ce sous-groupe est bien isomorphe à $\mathfrak{S}_3$.