# Feuille 3

**Exercice 1.**

Soit G un groupe. Soient H et K deux sous-groupes de G tels que $K \subset H \subset G$.

a) Supposons que G soit fini. Montrer que

$$|G : K| = |G : H| \cdot |H : K| .$$

b) On ne suppose plus que G est fini. On suppose par contre que H et K sont distingués dans G. Montrer que

$$|G : K| = |G : H| \cdot |H : K| .$$

**Éléments de solution 1.**

a) Comme G est fini, on a

$$|G| = |G : H|\,|H| \qquad |H| = |H : K|\,|K| \qquad |G| = |G : K|\,|K|$$

Par conséquent

$$|G : H|\,|H| = |G : H|\,|H : K|\,|K| = |G : K|\,|K|$$

L'ordre d'un groupe n'est jamais nul donc $|K| \neq 0$ et

$$|G : K| = |G : H| \cdot |H : K| .$$

b) Les groupes $G/H$ et $\left(G/K\right)/\left(H/K\right)$ sont isomorphes donc $\left|G/H\right| = \left|\left(G/K\right)/\left(H/K\right)\right|$ soit $|G : H| = \left|G/K : H/K\right|$ d'où $|G : H|\left|H/K\right| = \left|G/K\right|$, *i.e.*

$$|G : H| \cdot |H : K| = |G : K| .$$

**Exercice 2.** [Indice]
Soit H un groupe. Soient $H_0$ et G des sous-groupes de H tels que $H_0$ est d'indice fini dans H. Montrer que

$$|G : G \cap H_0| \leq |H : H_0| .$$

**Éléments de solution 2.**

**Exercice 3.** [Sous-groupes / Sous-groupes distingués, Dummit-Foot, page 95 exercice 5]
Soit G un groupe. Soient H un sous-groupe de G et $g \in G$.

a) Montrer que $gHg^{-1}$ est un sous-groupe de G du même ordre que H.
b) En déduire que si H est le seul sous-groupe de G d'ordre $n$ ($n \in \mathbb{N}^*$), alors H est distingué dans G.

**Éléments de solution 3.**

**Exercice 4.** [Sous-groupes distingués, Dummit-Foot, page 88 exercice 25]
Soit $G = GL_2(\mathbb{Q})$. Soit N le sous-groupe des matrices triangulaires supérieures à coefficients entiers et dont tous les coefficients diagonaux valent 1. Soit $g$ la matrice diagonale dont les coefficients sont 2 et 1.

Montrer que $gNg^{-1} \subset N$ mais que $g$ ne normalise pas N.

**Éléments de solution 4.**

**Exercice 5.** [Sous-groupes distingués / isomorphismes]
Soient $H_1 \subset G_1$ et $H_2 \subset G_2$ des groupes.

a) Supposons $H_1$ et $H_2$ distingués. Montrer que $H_1 \times H_2$ est distingué dans $G_1 \times G_2$. Montrer qu'il y a un isomorphisme de groupes $(G_1 \times G_2)/(H_1 \times H_2) \simeq G_1/H_1 \times G_2/H_2$.

b) Supposons que $H_1$ soit distingué et qu'il existe un *isomorphisme* $\phi\colon G_1 \to G_2$ tel que $H_2 = \phi(H_1)$. Montrer que $H_1$ et $H_2$ sont isomorphes puis que $G_1/H_1$ et $G_2/H_2$ sont isomorphes.

c) Supposons que $G_1$ et $G_2$ soient isomorphes et que $H_1$ et $H_2$ soient isomorphes et distingués. Les groupes $G_1/H_1$ et $G_2/H_2$ sont-ils nécessairement isomorphes ?

**Éléments de solution 5.**

a) Soit $\varphi\colon G_1 \times G_2 \to \left(G_1/H_1\right) \times \left(G_2/H_2\right)$ l'homomorphisme défini par

$$\varphi((a,b)) = (aH_1, bH_2).$$

On a

$$\begin{aligned} \ker\varphi &= \left\{(a,b) \in G_1 \times G_2 \,|\, (aH_1, bH_2) = (H_1, H_2)\right\} \\ &= \left\{(a,b) \in G_1 \times G_2 \,|\, a \in H_1 \text{ et } b \in H_2\right\} \\ &= H_1 \times H_2 \end{aligned}$$

De plus $\varphi$ est surjectif ($(aH_1, bH_2)$ est l'image de $(a,b)$ par $\varphi$). Par conséquent $\varphi$ induit un isomorphisme de $(G_1 \times G_2)/(H_1 \times H_2)$ sur $\left(G_1/H_1\right) \times \left(G_2/H_2\right)$.

b)

c)

**Exercice 6.** [Groupes quotients, Dummit-Foot, page 89 exercice 36, page 95 exercice 4]

a) Soient G un groupe et $Z(G)$ son centre. Supposons que $G/Z(G)$ soit cyclique. Montrer que G est abélien.
Donner un exemple de groupes $H \lhd G$ tels que H et $G/H$ soient abéliens mais pas G.

b) Montrer que si $|G| = pq$, pour $p$ et $q$ des nombres premiers, alors G est abélien ou $Z(G) = 1$.

**Éléments de solution 6.**

a) Soient G un groupe et $Z(G)$ son centre. Supposons que $G/Z(G)$ soit cyclique. Montrons que G est abélien.
Rappelons que le centre $Z(G)$ de G est distingué. Considérons le morphisme quotient $\pi\colon G \to G/Z(G)$. Par hypothèse $G/Z(G)$ est engendré par un élément $\overline{g_0}$. Puisque $\pi$ est surjective il existe $g_0 \in G$ tel que $\pi(g_0) = \overline{g_0}$. Soient $g$, $h$ dans G. Il existe $n$, $m \in \mathbb{Z}$ tels que $\pi(g) = \overline{g_0}^n$ et $\pi(h) = \overline{g_0}^m$. Par suite $\pi(gg_0^{-n}) = \pi(hg_0^{-m}) = e$ et $y = gg_0^{-n}$, $z = gg_0^{-m}$ appartiennent à $Z(G)$. Alors

$$gh = yg_0^n z g_0^m = yz g_0^{n+m} = z g_0^m y g_0^n = hg$$

c'est-à-dire G est abélien.
Donnons un exemple de groupes $H \lhd G$ tels que H et $G/H$ soient abéliens mais pas G.**finir**

b) **finir**

**Exercice 7.** [Sous-groupes distingués / Groupes quotients]
Pour les exemples suivants, vérifier que H est distingué dans G et déterminer les quotients :

a) $G = GL_n(\Bbbk)$, $H = SL_n(\Bbbk)$ (pour $\Bbbk$ un corps)

b) $G = O_n(\mathbb{R})$, $H = SO_n(\mathbb{R})$

c) $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $H = \langle(0,2)\rangle$ (resp. $H = \langle(1,2)\rangle$, resp. $H = \langle(1,1)\rangle$)

d) $G = H_8$ (les quaternions) et $H = \langle -1\rangle$ (resp. $H = \langle i\rangle$)

e) $\mathrm{G} = \mathcal{S}_4$ et $\mathrm{H} = \{\mathrm{id},\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\}$.

**Éléments de solution 7.**

**Exercice 8.** [Normalisateur, Dummit-Foot, page 88 exercice 31]
Soient G un groupe et H un sous-groupe de G.

a) Montrer que H est distingué dans $N_{\mathrm{G}}(\mathrm{H})$.
b) Montrer que $N_{\mathrm{G}}(\mathrm{H})$ est le plus grand sous-groupe de G dans lequel H est distingué.

**Éléments de solution 8.**

**Exercice 9.** [Sous-groupes distingués / Groupes quotients / Groupe diédral]
Notons $\mathrm{D}_{2n}$ le $n$-ème groupe diédral. Soit H un sous-groupe strict distingué de $\mathrm{D}_{2n}$.

a) Montrer que si $n$ est impair alors H est un sous-groupe du groupe des rotations. Déterminer les H possibles.
b) Si $n$ est pair, montrer que $\mathrm{D}_{2n}$ admet deux sous-groupes distingués isomorphes à $\mathrm{D}_{2\frac{n}{2}}$ et que ce sont les seuls H possibles qui contiennent une symétrie.
c) Déterminer les quotients de $\mathrm{D}_{2n}$.

**Éléments de solution 9.**

**Exercice 10.** [Abélianisé, Dummit-Foot, page 89 exercice 41, page 169 proposition 7, page 171 exemple 3]
Soit G un groupe fini. Notons $D(\mathrm{G})$ le sous-groupe de G engendré par les commutateurs (c'est-à-dire les éléments de la forme $ghg^{-1}h^{-1}$, $g$, $h \in \mathrm{G}$) ; c'est le groupe dérivé de G.

a) Montrer que $D(\mathrm{G})$ est un sous-groupe distingué de G.
b) Montrer que le quotient $\mathrm{G}/D(\mathrm{G})$ est abélien.
c) Montrer que $\mathrm{G}/D(\mathrm{G})$ est le plus gros quotient abélien de G au sens que si $\mathrm{H} \lhd \mathrm{G}$ et $\mathrm{G}/\mathrm{H}$ est abélien, alors $D(\mathrm{G}) \subset \mathrm{H}$.
d) Montrer que si $D(\mathrm{G}) \subset \mathrm{H}$, alors $\mathrm{H} \lhd \mathrm{G}$ et $\mathrm{G}/\mathrm{H}$ est abélien.
e) Soit $\varphi\colon \mathrm{G} \to A$ un morphisme dans un groupe abélien $A$. Montrer que $\varphi$ se factorise par la projection canonique $\mathrm{G} \to \mathrm{G}/D(\mathrm{G})$.
f) $\mathrm{G}/D(\mathrm{G})$ s'appelle l'abélianisé de G et se note parfois $\mathrm{G}_{\mathrm{ab}}$. Calculer l'abélianisé du groupe diédral $\mathrm{D}_{2n}$.

**Éléments de solution 10.**

a) Montrons que $D(\mathrm{G})$ est un sous-groupe distingué de G.
Direct.
b) Montrons que le quotient $\mathrm{G}/D(\mathrm{G})$ est abélien.
Soient $g$ et $h$ deux éléments de G. Alors $ghg^{-1}h^{-1}$ appartient à $D(\mathrm{G})$ et

$$\overline{ghg^{-1}h^{-1}} = e_{\mathrm{G}/D(\mathrm{G})}$$

c'est-à-dire

$$\overline{g}\,\overline{h}\,\overline{g}^{-1}\,\overline{h}^{-1} = e_{\mathrm{G}/D(\mathrm{G})}$$

ou encore

$$\overline{g}\,\overline{h} = \overline{h}\,\overline{g}.$$

Autrement dit $\mathrm{G}/D(\mathrm{G})$ est abélien.
c) Montrons que $\mathrm{G}/D(\mathrm{G})$ est le plus gros quotient abélien de G, *i.e.* que si $\mathrm{H} \lhd \mathrm{G}$ et $\mathrm{G}/\mathrm{H}$ est abélien, alors $D(\mathrm{G}) \subset \mathrm{H}$.
Notons $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{H}$ la projection canonique. D'une part $\pi(D(\mathrm{G})) = D(\pi(\mathrm{G}))$ donc $\pi(D(\mathrm{G})) \subset D\left(\mathrm{G}/\mathrm{H}\right)$. D'autre part $\mathrm{G}/\mathrm{H}$ est abélien donc $D\left(\mathrm{G}/\mathrm{H}\right) = \{\mathrm{id}\}$. Par conséquent $\pi(D(\mathrm{G})) = \{\mathrm{id}\}$ c'est-à-dire $D(\mathrm{G}) \subset \ker\pi = \mathrm{H}$.

d) Montrons que si $D(\mathrm{G}) \subset \mathrm{H}$, alors $\mathrm{H} \lhd \mathrm{G}$ et ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ est abélien.
Soit $\mathrm{H} \subset \mathrm{G}$ tel que $D(\mathrm{G}) \subset \mathrm{H}$.
Montrons que $\mathrm{H} \lhd \mathrm{G}$. Rappelons que si G est un groupe et K un sous-groupe distingué de G, alors un sous-groupe H de G contenant K est distingué dans G si et seulement si ${}^{\mathrm{H}}\!/_{\mathrm{K}}$ est distingué dans ${}^{\mathrm{G}}\!/_{\mathrm{K}}$.
Dans le cas où $\mathrm{K} = D(\mathrm{G})$, le quotient ${}^{\mathrm{G}}\!/_{\mathrm{K}} = {}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ est commutatif, donc tous ses sous-groupes sont distingués. Il en résulte que tout sous-groupe H de G contenant $D(\mathrm{G})$ est distingué dans G.
Montrons que ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ est abélien. D'après le troisième théorème d'isomorphisme

$$ {}^{\mathrm{G}}\!/_{\mathrm{H}} \simeq {}^{{}^{\mathrm{G}}\!/_{D(\mathrm{G})}}\!/_{{}^{\mathrm{H}}\!/_{D(\mathrm{G})}}. $$

Comme ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ est abélien et que tout quotient d'un groupe abélien est abélien, ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ est abélien.

e) Soit $\varphi\colon \mathrm{G} \to A$ un morphisme dans un groupe abélien $A$. Montrer que $\varphi$ se factorise par la projection canonique $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{D(\mathrm{G})}$.
D'une part $\pi(D(\mathrm{G})) = D(\pi(\mathrm{G}))$ donc $\pi(D(\mathrm{G})) \subset D\left({}^{\mathrm{G}}\!/_{D(\mathrm{G})}\right)$. D'autre part ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ est abélien donc $D\left({}^{\mathrm{G}}\!/_{D(\mathrm{G})}\right) = \{\mathrm{id}\}$. Par conséquent $\pi(D(\mathrm{G})) = \{\mathrm{id}\}$ c'est-à-dire $D(\mathrm{G}) \subset \ker \pi$.
Le théorème d'isomorphisme assure l'existence de $\overline{\varphi}\colon {}^{\mathrm{G}}\!/_{D(\mathrm{G})} \to A$ tel que $\varphi = \overline{\varphi} \circ \pi$

f) ${}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ s'appelle l'abélianisé de G et se note parfois $\mathrm{G}_{\mathrm{ab}}$. Calculons l'abélianisé du groupe diédral $\mathrm{D}_{2n}$.
Rappelons que

$$ \mathrm{D}_{2n} = \langle \rho, \sigma, \,|\, \rho^n = \sigma^2 = \mathrm{id},\, \rho\sigma = \sigma\rho^{-1} \rangle $$

Un calcul montre que

$$ \sigma\rho\sigma^{-1} = \sigma\rho\sigma = \rho^{-1} $$

et par récurrence nous obtenons

$$ \sigma\rho^k\sigma^{-1} = \rho^{-k}. $$

Par suite tous les éléments de $\langle \rho, \sigma \rangle$ sont de la forme $\rho^k$ ou $\rho^k\sigma$. Par conséquent

$$ \mathrm{D}_{2n} = \left\{ \rho^k,\, \rho^k\sigma \,|\, 0 \leq k \leq n-1 \right\}. $$

Un calcul montre que $D(\mathrm{D}_{2n}) = \langle \rho^2 \rangle$ ; en effet d'une part

$$ [\rho^k, \rho^\ell\sigma] = \rho^{2k} $$

d'autre part

$$ [\rho^k\sigma, \rho^\ell\sigma] = \rho^{2(k-\ell)}. $$

Ce groupe est de cardinal $n$ si $n$ est impair, de cardinal $\frac{n}{2}$ si $n$ est pair.
L'abélianisé de $\mathrm{D}_{2n}$ est ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ si $n$ est impair et ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ si $n$ est pair.

**Exercice 11.** [Groupes quotients / Ordre d'un élément / Isomorphismes, Dummit-Foot. page 86 exercice 14, page 96 exercice 21]
Considérons le groupe additif ${}^{\mathbb{Q}}\!/_{\mathbb{Z}}$.

a) Montrer que chaque classe à gauche de $\mathbb{Z}$ dans $\mathbb{Q}$ contient exactement un représentant $q \in \mathbb{Q}$ avec $0 \leq q < 1$.
b) Montrer que chaque élément de ${}^{\mathbb{Q}}\!/_{\mathbb{Z}}$ est d'ordre fini mais qu'il existe des éléments d'ordre arbitrairement grand.
c) Montrer que ${}^{\mathbb{Q}}\!/_{\mathbb{Z}}$ est le groupe de torsion de ${}^{\mathbb{R}}\!/_{\mathbb{Z}}$.
d) Montrer que ${}^{\mathbb{Q}}\!/_{\mathbb{Z}}$ est isomorphe au groupe multiplicatif des racines de l'unité de $\mathbb{C}^*$.

e) Montrer que $\mathbb{Q}/\mathbb{Z}$ n'a pas de sous-groupe propre d'indice fini.

**Éléments de solution 11.**

**Exercice 12.** [Automorphismes du groupe symétrique, Perrin, Cours d'algèbre, page 30]
Soit $n \geq 3$.

a) Soient $a$, $b$ dans $\{1, 2, \ldots, n\}$ et $\sigma$ dans $\mathcal{S}_n$. Montrer que

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b))$$

b) En déduire que le centre de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$.

c) Soit $\varphi$ un automorphisme de $\mathcal{S}_n$ qui envoie transpositions sur transpositions. Montrer que $\varphi$ est un morphisme intérieur, c'est-à-dire $\varphi$ appartient à $\mathrm{Int}(\mathcal{S}_n)$.

d) Supposons que $n \neq 6$. Montrer que $\mathrm{Aut}(\mathcal{S}_n) = \mathrm{Int}(\mathcal{S}_n) \simeq \mathcal{S}_n$.

**Éléments de solution 12.**

a) Direct.

b) Soit $\sigma$ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite a) entraîne

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma \circ (1\ 3) = (1\ 3) \circ \sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et $n$. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations.

c) Les transpositions de la forme $(1\ \ i)$ où $2 \leq i \leq n$ engendrent $\mathcal{S}_n$. Posons $\tau_i = \varphi(1\ \ i)$. Remarquons que pour $i$ et $j$ distincts $\tau_i$ et $\tau_j$ ne commutent pas car $(1\ \ i)$ et $(1\ \ j)$ ne commutent pas. Il en résulte que les transpositions $\tau_i$ et $\tau_j$ ont exactement un élément en commun dans leur support. On peut donc écrire $\tau_2$ et $\tau_3$ sous la forme

$$\tau_2 = (\alpha_1\ \ \alpha_2) \qquad\qquad \tau_3 = (\alpha_1\ \ \alpha_3)$$

avec $\alpha_2 \neq \alpha_3$. Montrons que pour tout $k \geq 4$ on a $\tau_k = (\alpha_1\ \ \alpha_k)$ pour un certain $\alpha_k \in \{1, 2, \ldots, n\}$. En effet si $\alpha_1$ n'était pas dans le support de $\tau_k$ on aurait $\tau_k = (\alpha_2\ \ \alpha_3)$ et

$$\tau_2 \circ \tau_k = (\alpha_1\ \ \alpha_2\ \ \alpha_3) \qquad\qquad \tau_3 \circ \tau_k = (\alpha_1\ \ \alpha_3\ \ \alpha_2)$$

seraient inverses l'un de l'autre. Mais

$$(1\ \ 2)(1\ \ k) = (2\ \ 1\ \ k)$$

n'est pas l'inverse de

$$(1\ \ 3)(1\ \ k) = (3\ \ 1\ \ k)$$

contradiction.

Notons que $\alpha\colon k \mapsto \alpha_k$ est un élément de $\mathcal{S}_n$.

L'automorphisme $\varphi$ et la conjugaison par $\alpha$ coïncident sur les générateurs $(1\ \ j)$ de $\mathcal{S}_n$ ; ils coïncident donc sur $\mathcal{S}_n$ tout entier.

d) Soit $\varphi$ un automorphisme non intérieur de $\mathcal{S}_n$. Montrons que $n = 6$.

D'après c) il existe une transposition $\tau$ telle que $\varphi(\tau)$ ne soit pas une transposition. Puisque $(\varphi(\tau))^2 = \mathrm{id}$, $\varphi(\tau)$ est un produit de $k \geq 2$ transpositions à supports disjoints. Désignons par $\mathrm{C}(\tau)$ le centralisateur de $\tau$

$$\mathrm{C}(\tau) = \big\{ f \in \mathcal{S}_n \,|\, f \circ \tau = \tau \circ f \big\}.$$

On a

$$\mathrm{C}(\tau) = \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{engendré par } \tau} \times \underbrace{\mathcal{S}_{n-2}}_{\text{permutations de support disjoint de celui de } \tau}$$

En particulier on a un morphisme surjectif

$$\psi \colon \mathrm{C}(\tau) \to \mathcal{S}_{n-2}$$

de noyau $\mathbb{Z}/2\mathbb{Z}$.
Posons $\mathrm{H} = \mathrm{C}(\varphi(\tau)) = \{f \in \mathcal{S}_n \mid f \circ \varphi(\tau) = \varphi(\tau) \circ f\}$. Les groupes H et $\mathrm{C}(\tau)$ sont isomorphes via $\varphi$. Chacune des transpositions de la décomposition de $\varphi(\tau)$ commute avec $\varphi(\tau)$ donc H contient un sous-groupe N isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}\right)^k$. De plus N est le noyau du morphisme

$$\begin{array}{ccl} \mathrm{H} & \to & \mathcal{S}_k \\ h & \mapsto & \text{permutation induite sur les } k \text{ transpositions de la décomposition de } \varphi(\tau) \end{array}$$

donc $\mathrm{N} \lhd \mathrm{H}$.
Ainsi comme $\mathrm{C}(\tau) \simeq \mathrm{H}$, $\mathrm{C}(\tau)$ contient un sous-groupe $\mathrm{N}'$ avec les deux propriétés suivantes :

$$\begin{cases} \mathrm{N}' \lhd \mathrm{C}(\tau) \\ \mathrm{N}' \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^k \end{cases}$$

Via $\psi$ on obtient que $\mathcal{S}_{n-2}$ contient un sous-groupe distingué isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}\right)^k$ ou $\left(\mathbb{Z}/2\mathbb{Z}\right)^{k-1}$ suivant que $\tau \in \mathrm{N}'$ ou $\tau \notin \mathrm{N}'$.
Or les sous-groupes distingués de $\mathcal{S}_n$ sont

- $\{\mathrm{id}\}$, $\mathcal{A}_n$, $\mathcal{S}_n$ si $n \neq 4$ ;
- $\{\mathrm{id}\}$, $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathcal{A}_4$, $\mathcal{S}_4$.

On en déduit les deux possibilités suivantes

- $n = 4$ car $\mathcal{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ peut alors correspondre à $\left(\mathbb{Z}/2\mathbb{Z}\right)^{k-1}$ avec $k = 2$ ;
- $n = 6$ car $\mathcal{S}_4$ contient $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Supposons que $n = 4$. Le centralisateur d'une transposition dans $\mathcal{S}_4$ est de cardinal 4 (c'est le groupe $V_4$) alors que le centralisateur d'une double transposition est de cardinal 8 (en effet il divise strictement 24, est multiple strict de 4 car contient $V_4$ mais aussi au moins un 4-cycle) : contradiction.
Ainsi $n = 6$.

**Exercice 13.**
Soit G un groupe. Soit H un sous-groupe de G d'indice 2.
Montrer que H est distingué dans G.

**Éléments de solution 13.**
Les classes à gauche de G modulo H sont $\{\mathrm{H}, \mathrm{G} \smallsetminus \mathrm{H}\}$. Donc les classes à droite de G modulo H sont $\{\mathrm{H}, \mathrm{G} \smallsetminus \mathrm{H}\}$. Si $g \notin \mathrm{H}$, on a donc $g \cdot \mathrm{H} = \mathrm{G} \smallsetminus \mathrm{H} = \mathrm{H} \cdot g$ ce qui assure le résultat.

**Exercice 14.** [Isomorphismes exceptionnels, Perrin, Cours d'algèbre, p. 106]

a) Montrer que tout sous-groupe d'indice $n$ dans $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$.

b) Montrer que
   (a) $\mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathcal{S}_3$,
   (b) $\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathcal{A}_4$,
   (c) $\mathrm{PSL}_2(\mathbb{F}_4) \simeq \mathcal{A}_5$,
   (d) $\mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathcal{A}_5$

**Éléments de solution 14.**

a) Soit H un sous-groupe d'indice $n$ dans $\mathcal{S}_n$.

Si $n \geq 3$, on vérifie l'énoncé directement.

Si $n = 4$, alors : si $\mathrm{H} \not\simeq \mathcal{S}_3$, alors H est cyclique (rappel : si $p$, $q$ sont des nombres premiers tels que $p < q$ et $p$ ne divise pas $q - 1$ alors tout groupe d'ordre $pq$ est cyclique) : contradiction avec le fait que $\mathcal{S}_4$ ne contient pas d'élément d'ordre 6.

Supposons $n \geq 5$. Le groupe $\mathcal{S}_n$, et donc aussi H, opère par translation à gauche sur $E = {}^{\mathcal{S}_n}\!/_{\mathrm{H}}$ d'où un homomorphisme

$$\varphi \colon \mathcal{S}_n \to \mathcal{S}_E \simeq \mathcal{S}_n.$$

Puisque $\ker\varphi = \bigcap_{a \in \mathcal{S}_n} a\mathrm{H}a^{-1}$, $\ker\varphi$ est distingué dans $\mathcal{S}_n$ et $\ker\varphi \subset \mathrm{H}$ on a $\ker\varphi = \{\mathrm{id}\}$ (rappel : pour $n \geq 5$ les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$). Pour des raisons de cardinalité ($|\mathcal{S}_n| = |\mathcal{S}_E \simeq \mathcal{S}_n|$), $\varphi$ est un isomorphisme.

Comme H est le stabilisateur de la classe de idH on a : $\varphi(\mathrm{H}) \subset \mathcal{S}_n$ est le stabilisateur d'un point et c'est donc un sous-groupe isomorphe à $\mathcal{S}_{n-1}$.

b) Soit $E$ un $\Bbbk$-espace vectoriel. On introduit l'espace projectif $\mathbb{P}(E)$ associé à $E$ ; c'est l'ensemble des droites vectorielles de $E$. Le groupe $\mathrm{GL}(E)$ opère sur $\mathbb{P}(E)$ et les homothéties opérant trivialement $\mathrm{PGL}(E)$ opère aussi sur $\mathbb{P}(E)$. De plus $\mathrm{PGL}(E)$ opère fidèlement sur $\mathbb{P}(E)$ ([Perrin, Cours d'algèbre, p. 98]).

On fait agir $\mathrm{PGL}(2, \mathbb{F}_q)$ sur les droites vectorielles de $(\mathbb{F}_q)^2$. Il y a $q + 1$ telles droites de sorte que l'on a un morphisme injectif

$$\varphi \colon \mathrm{PGL}(2, \mathbb{F}_q) \hookrightarrow \mathcal{S}_{q+1}.$$

Par ailleurs le cardinal de $\mathrm{PGL}(2, \mathbb{F}_q)$ est $\frac{(q^2-1)(q^2-q)}{q-1} = q(q^2-1)$ ; c'est aussi le cardinal de $\mathrm{SL}(2, \mathbb{F}_q)$. Notons aussi que si la caractéristique de $\mathbb{F}_q$ n'est pas 2, alors $\mathrm{PSL}(2, \mathbb{F}_q)$ est d'indice 2 dans $\mathrm{PGL}(2, \mathbb{F}_q)$.

(a) On a $\mathrm{PGL}(2, \mathbb{F}_2) = \mathrm{GL}(2, \mathbb{F}_2) = \mathrm{SL}(2, \mathbb{F}_2) = \mathrm{PSL}(2, \mathbb{F}_2)$.

(b) Comme $|\mathrm{PGL}(2, \mathbb{F}_3)| = 24$, on a $\mathrm{PGL}(2, \mathbb{F}_3) \simeq \mathcal{S}_4$. Puisque $\mathcal{A}_4$ est le seul sous-groupe d'indice 2 dans $\mathcal{S}_4$ on a $\mathrm{PSL}(2, \mathbb{F}_3) \simeq \mathcal{A}_4$.

(c) On a $|\mathrm{PGL}(2, \mathbb{F}_4)| = |\mathrm{PSL}(2, \mathbb{F}_4)| = 60$. Puisque $\mathcal{A}_5$ est l'unique sous-groupe d'indice 2 dans $\mathcal{S}_5$ on a $\mathrm{PGL}(2, \mathbb{F}_4) \simeq \mathcal{A}_5$.

(d) On a $|\mathrm{PGL}(2, \mathbb{F}_5)| = 120$ donc $\mathrm{PGL}(2, \mathbb{F}_5)$ s'identifie à un sous-groupe d'indice 6 de $\mathcal{S}_6$. Ainsi, d'après a), le groupe $\mathrm{PGL}(2, \mathbb{F}_5)$ est isomorphe à $\mathcal{S}_5$. Il en résulte que

$$\mathrm{PSL}(2, \mathbb{F}_5) \simeq \mathcal{A}_5.$$

**Exercice 15.**

Soit G un groupe. Les assertions suivantes sont-elles vraies ou fausses ? Justifier.

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

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

c) Soient $g$ et $h$ dans G d'ordre fini. Alors $gh$ est 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 $\langle \mathrm{H} \cup \mathrm{K} \rangle = \mathrm{HK}$.

**Éléments de solution 15.**

a) Faux. Considérons le groupe H des quaternions. Rappelons qu'il est défini de la façon suivante : H est l'ensemble

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

et la loi de groupe est définie par

$$(-1)^2 = 1,\ \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$$
$$(-1)\cdot\mathbf{i} = \mathbf{i}\cdot(-1) = -\mathbf{i},\ (-1)\cdot\mathbf{j} = \mathbf{j}\cdot(-1) = -\mathbf{j},\ (-1)\cdot\mathbf{k} = \mathbf{k}\cdot(-1) = -\mathbf{k}$$
$$\mathbf{i}\cdot\mathbf{j} = -\mathbf{j}\cdot\mathbf{i} = \mathbf{k}.$$

Les sous-groupes de H sont
— le sous-groupe trivial {id} qui est distingué,
— le sous-groupe 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 distingués,
— ls sous-groupe H entier qui est distingué.
Les sous-groupes de H sont donc tous distingués mais H n'est pas abélien.

b) Faux. Considérons par exemple $\mathrm{G} = \mathcal{S}_4$, $\mathrm{H} = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{K} = \{\mathrm{id}, (1\ 2)(3\ 4)\} \simeq \mathbb{Z}/2\mathbb{Z}$.

c) Faux. Pour avoir un contre-exemple il faut que le groupe G soit infini et non abélien. Prenons par exemple $\mathrm{G} = \mathrm{GL}(2,\mathbb{Q})$, $x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $x = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. L'élément $x$ est d'ordre 2, l'élément $y$ est d'ordre 3 mais $xy = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini.

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

e) Faux. L'inclusion $\mathrm{HK} \subset \langle \mathrm{H}\cup\mathrm{K}\rangle$ est toujours vérifiée. En revanche le sous-ensemble HK n'est en général pas un sous-groupe de G contrairement à $\langle \mathrm{H}\cup\mathrm{K}\rangle$. En effet prenons par exemple $\mathrm{G} = \mathcal{S}_3$, $\mathrm{H} = \{\mathrm{id}, (1\ 2)\}$ et $\mathrm{K} = \{\mathrm{id}, (1\ 3)\}$. Alors $\langle \mathrm{H}\cup\mathrm{K}\rangle$ coïncide avec G et $\mathrm{HK} = \{\mathrm{id}, (1\ 2), (1\ 3), (1\ 3\ 2)\}$ n'est pas un sous-groupe de G.

La réponse est vraie si l'on suppose que H ou K est distingué dans G (exercice).

**Exercice 16.**

Soit $S$ un sous-ensemble non vide d'un groupe fini G. Soit $N(S) = \left\{g \in \mathrm{G} \,|\, gSg^{-1} = S\right\}$ le normalisateur de $S$ dans G. Soit $C(S) = \left\{g \in \mathrm{G} \,|\, \forall\, s \in S,\ gsg^{-1} = s\right\}$ le centralisateur de $S$ dans G.

Montrer que

a) $N(S) \subset \mathrm{G}$ et $C(S) \lhd N(S)$.

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

c) Si $\mathrm{H} \lhd \mathrm{G}$, alors $C(\mathrm{H}) \lhd \mathrm{G}$.

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

**Éléments de solution 16.**

a) Montrons que $N(S) \subset \mathrm{G}$ et $C(S) \lhd N(S)$. Bien sûr $e$ appartient à $N(S)$. Soient $g$ et $h$ dans $N(S)$. Alors

$$(gh)S(gh)^{-1} = g(hSh^{-1})g^{-1} = gSg^{-1} = S$$

donc $gh$ appartient à $N(S)$. Si $g$ appartient à $N(S)$ on a $gSg^{-1} = S$ donc en multipliant à gauche et à droite par $g^{-1}$ et $g$ respectivement on a $S = g^{-1}Sg$, autrement dit $g^{-1}$ appartient à $N(S)$. Ainsi $N(S)$ est un sous-groupe de G.

De même $C(S)$ est un sous-groupe de G contenu dans $N(S)$. Montrons que $C(S)$ est distingué dans $N(S)$. Soient $g \in C(S)$ 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 $h$ appartient à $N(S)$, on a $h^{-1}sh$ appartient à $S$. Donc puisque $g$ appartient à $C(S)$

$$g(h^{-1}sh)g^{-1} = h^{-1}sh$$

et finalement

$$(hgh^{-1})s(hgh^{-1})^{-1} = h(h^{-1}sh)h^{-1} = s.$$

Ainsi $hgh^{-1}$ appartient à $C(S)$ et $C(S) \triangleleft N(S)$.

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

Supposons que $N(S) = \mathrm{G}$. Alors pour tout $g \in \mathrm{G}$, on a $gSg^{-1} = S$ donc $S = \bigcup_{g\in\mathrm{G}} gSg^{-1}$.

Réciproquement supposons que $S = \bigcup_{g\in\mathrm{G}} gSg^{-1}$. Pour tout $g \in \mathrm{G}$ on a donc $g^{-1}Sg \subset S$ donc en multipliant par $g$ et $g^{-1}$ à gauche et à droite respectivement on a $S \subset gSg^{-1} \subset S$ d'où $S = gSg^{-1}$. Ainsi $g$ appartient à $N(S)$ et $\mathrm{G} = N(S)$.

c) Montrons que si $\mathrm{H} \triangleleft \mathrm{G}$, alors $C(\mathrm{H}) \triangleleft \mathrm{G}$. Supposons que H soit distingué dans G. Soient $g$ dans G, $c$ dans $C(\mathrm{H})$ et $h$ dans H. On a

$$(gcg^{-1})h(gcg^{-1})^{-1} = gc(g^{-1}hg)c^{-1}g^{-1}$$

puisque H est distingué dans G on sait que $g^{-1}hg$ appartient à H. Or $c$ appartient à $C(\mathrm{H})$ donc $c(g^{-1}hg)c^{-1} = g^{-1}hg$ et finalement

$$(gcg^{-1})h(gcg^{-1})^{-1}$$

ce qui assure que $gcg^{-1}$ appartient à $C(\mathrm{H})$. Le groupe $C(\mathrm{H})$ est donc distingué dans G.

d) Montrons que si $\mathrm{H} \subset \mathrm{G}$, alors $N(\mathrm{H})$ est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.

Par définition et a) $N(\mathrm{H})$ est un sous-groupe de G contenant H et H est distingué dans $N(\mathrm{H})$. Considérons un sous-groupe K de G contenant H tel que $\mathrm{H} \triangleleft \mathrm{K}$. Par définition on a $k\mathrm{H}k^{-1} = \mathrm{H}$ pour tout $k \in \mathrm{K}$. Par conséquent $k$ appartient à $N(\mathrm{H})$ donc $\mathrm{K} \subset N(\mathrm{H})$ ce qui assure la maximalité de $N(\mathrm{H})$ parmi les sous-groupes de G concernés.

**Exercice 17.**

Soit G un groupe et soit $\mathrm{H} \triangleleft \mathrm{G}$ un sous-groupe distingué.

a) Décrire les sous-groupes distingués de $\mathrm{G}/\mathrm{H}$ 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

$$\left(\mathrm{G}/\mathrm{H}\right)\left(\mathrm{K}/\mathrm{H}\right) \simeq \mathrm{G}/\mathrm{K}$$

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

iii) Montrer que H est distingué dans HK.

iv) Montrer qu'on a un isomorphisme

$$\mathrm{K}/(\mathrm{K}\cap\mathrm{H}) \simeq \mathrm{HK}/\mathrm{H}.$$

**Éléments de solution 17.**

Soit G un groupe et soit $\mathrm{H} \triangleleft \mathrm{G}$ un sous-groupe distingué.

a) Décrivons les sous-groupes distingués de $\mathrm{G}/\mathrm{H}$ en fonction de ceux de G. On note $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{H}$ la projection canonique. La correspondance $\mathrm{K} \mapsto \pi(\mathrm{K})$ établit une bijection entre l'ensemble des sous-groupes de G contenant H et l'ensemble des sous-groupes de $\mathrm{G}/\mathrm{H}$ donc la réciproque est donnée par $\overline{\mathrm{K}} \mapsto \pi^{-1}(\overline{\mathrm{K}})$. Cette bijection induit une bijection entre les sous-groupes distingués de G contenant H et les sous-groupes distingués de $\mathrm{G}/\mathrm{H}$.

b) Soit K un sous-groupe de G.

i) Supposons que K soit distingué dans G et que K contienne H. Montrons que l'on a un isomorphisme

$$({}^{\mathrm{G}}\!/_{\mathrm{H}})({}^{\mathrm{K}}\!/_{\mathrm{H}}) \simeq {}^{\mathrm{G}}\!/_{\mathrm{K}}$$

Le morphisme $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ composé avec la projection $\pi'\colon {}^{\mathrm{G}}\!/_{\mathrm{H}} \to \left({}^{\mathrm{G}}\!/_{\mathrm{H}}\right)\!/\left({}^{\mathrm{K}}\!/_{\mathrm{H}}\right)$ induit un morphisme surjectif $q\colon \mathrm{G} \to \left({}^{\mathrm{G}}\!/_{\mathrm{H}}\right)\!/\left({}^{\mathrm{K}}\!/_{\mathrm{H}}\right)$. Par construction un élément $g$ de G appartient à $\ker q$ si et seulement si $\pi(g)$ appartient à $\ker \pi' = {}^{\mathrm{K}}\!/_{\mathrm{H}}$ si et seulement si $g$ appartient à K. Ainsi $\ker q = \mathrm{K}$. Le théorème de factorisation assure alors que $q$ induit un isomorphisme entre $\mathrm{G}/\ker q = {}^{\mathrm{G}}\!/_{\mathrm{K}}$ et $\left({}^{\mathrm{G}}\!/_{\mathrm{H}}\right)\!/\left({}^{\mathrm{K}}\!/_{\mathrm{H}}\right)$.

ii) Montrons que HK est un sous-groupe de G égal à KH.
Soient $h$, $h'$ dans H et $k$, $k'$ dans K. Le groupe H étant distingué dans G il existe $h''$ dans H tel que $k \cdot h' = h'' \cdot k$. Par suite

$$(h \cdot k) \cdot (h' \cdot k') = (h \cdot h") \cdot (k \cdot k')$$

appartient à HK et HK est un sous-groupe de G.

iv) Montrons que ${}^{\mathrm{K}}\!/_{(\mathrm{K} \cap \mathrm{H})}$ et ${}^{(\mathrm{HK})}\!/_{\mathrm{H}}$ sont isomorphes. L'inclusion $\mathrm{K} \to \mathrm{HK}$ induit un morphisme $p\colon \mathrm{K} \to {}^{(\mathrm{HK})}\!/_{\mathrm{H}}$. Montrons que $p$ est surjectif : si $h$ est dans H et $k$ dans K, alors la classe $(h \cdot k)\mathrm{H} = k\mathrm{H}$ est l'image de $k$ par $p$, donc $p$ est surjectif. De plus un élément $k \in \mathrm{K}$ appartient à $\ker p$ si et seulement si il est dans H. Autrement dit $\ker p = \mathrm{K} \cap \mathrm{H}$. On conclut à l'aide du théorème de factorisation.

**Exercice 18.** [Automorphismes intérieurs d'un groupe]

Soit G un groupe. On désigne par Aut(G) le groupe des automorphismes de G. Si $a$ appartient à G, on note $\varphi(a)$ l'application

$$\varphi(a)\colon \mathrm{G} \to \mathrm{G} \qquad\qquad g \mapsto aga^{-1}.$$

a) Montrer que pour tout $a$ dans G $\varphi(a)$ est un automorphisme de G (appelé automorphisme intérieur de G).

b) Montrer que $\varphi$ est un homomorphisme de groupes de G dans Aut(G).

c) Notons Int(G) l'ensemble des automorphismes intérieurs de G. Montrer que Int(G) est un sous-groupe distingué de Aut(G).

d) Notons $Z$(G) le centre de G. Montrer que $\mathrm{Int(G)} \simeq {}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$.

**Éléments de solution 18.**

a) Il faut montrer que $\varphi(a)$ est un homomorphisme de G dans G, *i.e.* que $\varphi(a)(gg') = \varphi(a)(g)\varphi(a)(g')$. Or

$$\varphi(a)(gg') = agg'a^{-1} = (aga^{-1})(ag'a^{-1}) = \varphi(a)(g)\varphi(a')(g)$$

Montrons que $\ker \varphi(a) = \{e\}$. Soit $g \in \ker \varphi(a)$, autrement dit $aga^{-1} = e$ d'où $g = a^{-1}a = e$. Ainsi $\varphi(a)$ est un homomorphisme injectif.
Soit $g$ dans G. On a $g = a(a^{-1}ga)a^{-1} = \varphi(a)(a^{-1}ga)$. Autrement dit $\varphi(a)$ est surjectif.
Il en résulte que $\varphi(a)$ est un automorphisme de G dans G et $(\varphi(a))^{-1} = \varphi(a^{-1})$.

b) D'une part $\varphi(e)(g) = ege^{-1} = g$, *i.e.* $\varphi(e) = \mathrm{id}$. D'autre part

$$\varphi(a) \circ \varphi(a')(g) = a(a'ga'^{-1})a^{-1} = (aa')g(aa')^{-1} = \varphi(aa')(g)$$

c'est-à-dire $\varphi(a) \circ \varphi(a') = \varphi(aa')$. Par suite $\varphi$ est un homomorphisme de groupes de G dans Aut(G).

c) Int(G) est l'image de G par l'homomorphisme de groupes $\varphi$ ; c'est donc un sous-groupe de Aut(G). Soit $\tau$ un automorphisme de G ; alors

$$\tau \circ \varphi(a) \circ \tau^{-1}(g) = \tau(a\tau^{-1}(g)a^{-1}) = \tau(a)\tau(\tau^{-1}(g))\tau(a^{-1}) = \tau(a)g\tau(a^{-1})$$

Ainsi $\tau \circ \varphi(a) \circ \tau^{-1} = \varphi(\tau(a))$ appartient à $\operatorname{Im}\varphi$. Le groupe Int(G) est distingué dans Aut(G).

d) D'une part $\ker\varphi$ est le centre $Z(\mathrm{G})$ de G, d'autre part $\operatorname{Im}\varphi = \mathrm{Int}(\mathrm{G})$. Le théorème d'isomorphisme assure que $\mathrm{Int}(\mathrm{G}) \simeq {}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$.

**Exercice 19.**

Soit $Q_8$ le groupe des matrices $2 \times 2$ inversibles engendré par $\begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$ et $\begin{pmatrix} -\mathbf{i} & 0 \\ 0 & \mathbf{i} \end{pmatrix}$. Ce groupe est appelé le groupe des quaternions.

a) Quel est l'ordre de $Q_8$ ?

b) Montrer que $Q_8$ n'a qu'un élément d'ordre 2.

c) Quel est le centre de $Q_8$ ?

d) Montrer que tous les sous-groupes de $Q_8$ sont distingués.

e) Peut-on trouver un isomorphisme entre $Q_8$ et un produit semi-direct de ${}^{\mathbb{Z}}\!/_{4\mathbb{Z}}$ avec ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ ?

**Éléments de solution 19.**

Posons $\mathcal{I} = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$, $\mathcal{J} = \begin{pmatrix} -\mathbf{i} & 0 \\ 0 & \mathbf{i} \end{pmatrix}$, $\mathcal{K} = \mathcal{I}\mathcal{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

a) On vérifie que Id est l'élément neutre,

$$-\mathrm{Id}M = -M \quad \forall\, M \in \{\mathcal{I}, \mathcal{J}, \mathcal{K}\} \qquad \mathcal{I}^2 = \mathcal{J}^2 = \mathcal{K}^2 = -\mathrm{Id}$$
$$\mathcal{I}\mathcal{J} = \mathcal{K},\ \mathcal{J}\mathcal{K} = \mathcal{I},\ \mathcal{K}\mathcal{I} = \mathcal{J} \qquad \mathcal{J}\mathcal{I} = -\mathcal{K},\ \mathcal{K}\mathcal{J} = -\mathcal{I},\ \mathcal{I}\mathcal{K} = -\mathcal{J}$$

Il en résulte que $Q_8$ contient 8 élements.

b) D'après ce qui précède l'unique élément d'ordre 2 est $-\mathrm{Id}$.

c) D'après ce qui précède le centre de $Q_8$ est $\{\mathrm{Id}, -\mathrm{Id}\}$.

d) Les sous-groupes de $Q_8$ sont le groupe trivial, le centre de $Q_8$ et

$$\langle\mathcal{I}\rangle = \{\mathrm{Id}, -\mathrm{Id}, \mathcal{I}, -\mathcal{I}\} \qquad \langle\mathcal{J}\rangle = \{\mathrm{Id}, -\mathrm{Id}, \mathcal{J}, -\mathcal{J}\} \qquad \langle\mathcal{K}\rangle = \{\mathrm{Id}, -\mathrm{Id}, \mathcal{K}, -\mathcal{K}\}$$

e) Les groupes $\langle\mathcal{I}\rangle$, $\langle\mathcal{J}\rangle$ et $\langle\mathcal{K}\rangle$ sont tous trois cycliques d'ordre 4 donc isomorphes à ${}^{\mathbb{Z}}\!/_{4\mathbb{Z}}$ mais aucun d'entre eux ne peut être un facteur semi-direct de $Q_8$ car l'autre facteur serait d'ordre 2 et d'intersection réduite à $\{\mathrm{Id}\}$ avec le facteur d'ordre 4. Or tous ces sous-groupes d'ordre 4 contiennent le sous-groupe d'ordre 2. Par conséquent $Q_8$ ne peut s'obtenir comme produit semi-direct de deux de ses sous-groupes propres.

**Exercice 20.**

Soit G un groupe fini. Soient H et K des sous-groupes de G. Supposons que

— H et K sont des sous-groupes distingués de G ;

— $\mathrm{H} \cap \mathrm{K} = \{e\}$.

Montrer que HK est un sous-groupe distingué de G d'ordre $|\mathrm{H}||\mathrm{K}|$.

**Éléments de solution 20.**

Montrons tout d'abord que HK est un sous-groupe de G. On définit l'application $\varphi$ par

$$\varphi\colon \mathrm{H} \times \mathrm{K} \to \mathrm{HK} \qquad (h, k) \mapsto hk.$$

Cette application est injective. En effet soient $h$, $h'$ dans H et $k$, $k'$ dans K tels que $f(h, k) = f(h', k')$, *i.e.* $hk = h'k'$. On en déduit que $hh'^{-1} = k'k^{-1}$ ; de plus $hh'^{-1} = k'k^{-1}$ appartient à $\mathrm{H} \cap \mathrm{K} = \{e\}$. Donc $hh'^{-1} = e$ et $kk'^{-1} = e$ c'est-à-dire $(h, k) = (h', k')$. Cette application est par définition surjective. Soient $h$, $h'$ dans H et soient $k$, $k'$ dans K. Puisque K est distingué il existe $k_1$ dans K tel que $hk = k_1h$. Comme H est distingué il existe $h_1$ dans H tel que $k_1h = h_1k_1$. Ainsi $hk = h_1k_1$. Mais $\varphi$ est injective d'où $h = h_1$, $k = k_1$ et $h$ et $k$ commutent ($hk = kh$). Donc $hkh'k' = hh'kk'$. On en déduit que

— HK est un sous-groupe de G : la loi est stable dans HK, $e$ appartient à HK et si $g \in$ HK, alors $g^{-1} \in$ HK ;
— $\varphi$ est un homomorphisme.

En particulier $\varphi$ est un isomorphisme de groupes.

Montrons que HK est distingué dans G. Soient $g \in G$, $h \in H$ et $k \in K$. Alors

$$ghkg^{-1} = (ghg^{-1})(gkg^{-1}) = h_1(gkg^{-1})$$

avec $h_1$ dans H car H est distingué dans G. Par ailleurs $h_1gkg^{-1} = h_1k_1$ avec $k_1$ dans K car K est distingué dans G. Donc $ghkg^{-1}$ appartient à HK et HK est distingué dans G.

Montrons que HK est d'ordre |H||K|. Comme $\varphi$ est un isomorphisme de groupes l'ordre de HK est celui de H $\times$ K, *i.e.* |H||K|.

**Exercice 21.**

Soit G un groupe de centre $Z(\mathrm{G})$.

a) Montrer que $Z(\mathrm{G})$ est un sous-groupe distingué de G.

b) Montrer que si $\mathrm{G}/Z(\mathrm{G})$ est monogène (*i.e.* $\mathrm{G}/Z(\mathrm{G})$ est engendré par un seul élément), alors G est abélien.

**Éléments de solution 21.**

a) Le centre de G est un sous-groupe de G. En effet si $x \in Z(\mathrm{G})$ et $y \in Z(\mathrm{G})$, alors $y^{-1} \in Z(\mathrm{G})$ et pour tout élément $g$ de G on a $xy^{-1}g = xgy^{-1} = gxy^{-1}$ ce qui implique que $xy^{-1}$ appartient à $Z(\mathrm{G})$.

Par ailleurs soit $g \in G$ et soit $c \in Z(\mathrm{G})$. Comme $c$ commute avec tous les éléments de G on a

$$gcg^{-1} = cgg^{-1} = c.$$

Donc $gZ(\mathrm{G})g^{-1} = C$ et $Z(\mathrm{G})$ est un sous-groupe distingué dans G.

b) Si G $= Z(\mathrm{G})$, alors G est abélien. Si G $\neq Z(\mathrm{G})$ et si $\mathrm{G}/Z(\mathrm{G})$ est monogène non trivial, alors il existe un élément $x$ de G tel que $x \notin C$ et $\mathrm{G}/Z(\mathrm{G}) = \langle xZ(\mathrm{G})\rangle$. Soit $y$ dans G. Ou bien $y \in Z(\mathrm{G})$ et $xy = yx$. Ou bien $y \notin Z(\mathrm{G})$ et il existe $n \in \mathbb{N}$ tel que $y \in (xZ(\mathrm{G}))^n = x^nZ(\mathrm{G})$, autrement dit $y = x^nc$ avec $c \in Z(\mathrm{G})$. Dans ce cas $xy = xx^nc = x^ncx = yx$. Ainsi $x$ commute avec tous les éléments de G, *i.e.* $x \in Z(\mathrm{G})$ : contradition. Ainsi G $= Z(\mathrm{G})$ et G est abélien.

**Exercice 22.** [Simplicité de $SO_3$, Francinou, Gianella, Nicolas, exercices de mathématiques, oraux x-ens, algèbre tome 3, pages 67-70]

Rappelons que $SO_3$ est le groupe des rotations de l'espace euclidien canonique $\mathbb{R}^3$. Soit G un sous-groupe de $SO_3$. On désigne par $\mathrm{G}_0$ la composante connexe par arcs de Id dans G.

Le groupe $SO_3$ est une partie de l'espace vectoriel $\mathcal{L}(\mathbb{R}^3)$ muni de sa topologie d'espace normé. Un chemin de G est une application $\gamma\colon [0,1] \to \mathrm{G}$ continue, $\gamma(0)$ est l'origine du chemin et $\gamma(1)$ son extrémité.

a) On considère sur G la relation $\mathcal{R}$ définie par $g\mathcal{R}h$ s'il existe un chemin de G d'origine $g$ et d'extrémité $h$. Montrer que cette relation est une relation d'équivalence.

b) Montrer que $\mathrm{G}_0$ est un sous-groupe de G.

c) Montrer que si G est distingué dans $SO_3$, alors $\mathrm{G}_0$ est distingué dans $SO_3$.

d) Supposons que G soit un sous-groupe de $SO_3$ connexe par arcs, distingué et non réduit à {Id}. Montrer qu'alors G contient une rotation d'angle $\pi$.

e) Montrer que les retournements, c'est-à-dire les rotations d'angle $\pi$, engendrent $SO_3$.

f) Supposons que G soit un sous-groupe de $SO_3$ connexe par arcs, distingué et non réduit à {Id}. Montrer que G $= SO_3$.

g) Montrer que le groupe $SO_3$ est simple.

**Éléments de solution 22.**

a) Si $g \in \mathrm{G}$, alors $g\mathcal{R}g$ comme on le voit en considérant $\gamma\colon t \mapsto g$.

Si $\gamma$ est un chemin d'origine $g$ et d'extrémité $h$, l'application $t \mapsto \gamma(1-t)$ est un chemin d'origine $h$ et d'extrémité $g$.

Si $g\mathcal{R}h$ et $h\mathcal{R}k$ et si $\gamma$ (resp. $\gamma'$) est un chemin de G d'orgine $g$ (resp. $h$) et d'extrémité $h$ (resp. $k$) l'application $\gamma''\colon [0,1] \to \mathrm{G}$ définie par

$$\gamma''(t) = \begin{cases} \gamma(2t) \text{ si } 0 \leq t \leq 1/2 \\ \gamma'(2t-1) \text{ si } 1/2 \leq t \leq 1 \end{cases}$$

est un chemin d'origine $g$ et d'extrémité $k$.

Les classes d'équivalence pour cette relation sont les composantes connexes par arcs de G.

b) Par définition $\mathrm{G}_0$ contient Id. Soient $g$ et $h$ deux éléments de $\mathrm{G}_0$. Soit $\gamma$ (resp. $\gamma'$) un chemin de $\mathrm{G}_0$ reliant Id à $g$ (resp. $h$). Considérons l'application

$$\gamma''\colon t \mapsto \gamma(t)\big(\gamma'(t)\big)^{-1}.$$

Pour tout $t \in [0,1]$ $\gamma(t)$ et $\gamma'(t)$ appartiennent à G donc $\gamma(t)\gamma'(t)$ appartient à G (en effet G est un sous-groupe de $\mathrm{SO}_3$). Enfin l'application $g \mapsto g^{-1}$ est continue sur $\mathrm{SO}_3$ : si on identifie un élément de $\mathrm{SO}_3$ à sa matrice dans la base canonique les coefficients de $g^{-1}$ dépendent polynomialement des coefficients de $g$. De plus $\gamma''(0) = \mathrm{IdId} = \mathrm{Id}$ et $\gamma''(1) = gh^{-1}$. Ainsi $\gamma''$ est un chemin de Id à $gh^{-1}$ et $gh^{-1}$ appartient à $\mathrm{G}_0$. Il en résulte que $\mathrm{G}_0$ est un sous-groupe de G.

c) Soient $g \in \mathrm{G}_0$, $\gamma$ un chemin de G de Id à $g$ et $h \in \mathrm{SO}_3$. Considérons l'application

$$\gamma'\colon [0,1] \to \mathrm{SO}_3 \qquad\qquad t \mapsto h\gamma(t)h^{-1}.$$

Pour tout $t \in [0,1]$ $\gamma(t)$ appartient à G et G étant distingué $h\gamma(t)h^{-1}$ appartient à G. L'application $\gamma$ est continue de même que la multiplication à gauche ou à droite par un élément de $\mathrm{SO}_3$ ; par conséquent $\gamma'$ est continue. De plus

$$\gamma'(0) = h\mathrm{Id}h^{-1} = \mathrm{Id} \qquad\qquad \gamma'(1) = hgh^{-1}.$$

L'applcation $\gamma'$ est donc un chemin de Id à $hgh^{-1}$ et $hgh^{-1}$ appartient à $\mathrm{G}_0$. Autrement dit $\mathrm{G}_0$ est distingué dans $\mathrm{SO}_3$.

d) Si $\theta$ est l'angle d'une rotation $g$ de $\mathbb{R}^3$ (si on change l'orientation de l'axe de la rotation l'angle est changé en son opposé donc $\theta$ est défini au signe près), alors il existe une base orthonormale dans laquelle sa matrice est

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

si bien que $\operatorname{Tr} g = 2\cos\theta + 1$ et donc l'application

$$\mathrm{SO}_3 \to [-1,1] \qquad\qquad g \mapsto \cos\theta = \frac{\operatorname{Tr} g - 1}{2}$$

est une application continue. Il suffit de montrer que cette application prend la valeur $-1$ pour avoir une rotation $g \in G$ d'angle $\pi$.

Montrons que G contient une rotation $r$ d'angle $\pm\frac{\pi}{2}$, alors $r^2$ sera une rotation de G d'angle $\pi$. Par hypothèse G contient un élément $g$ distinct de Id. Quitte à considérer $g^{-1}$ on peut supposer qu'une mesure $\theta$ de son angle appartient à $]0,\pi]$. Si $\cos\theta \leq 0$ on pose $s = g$. Si $\cos\theta > 0$, alors $\theta \in \left]0, \frac{\pi}{2}\right]$. Notons $N$ la partie entière de $\frac{\pi}{2\theta}$, *i.e.* $N = E\left(\frac{\pi}{2\theta}\right)$. Alors

$$N\theta \leq \frac{\pi}{2} < (N+1)\theta < 2 \times \frac{\pi}{2} = \pi.$$

En particulier $g^{N+1}$ est une rotation d'angle $(N+1)\theta \in \left[\frac{\pi}{2}, \pi\right[$. On pose alors $s = g^{N+1}$. Ainsi G contient une rotation $s$ d'angle $\theta$ avec $\cos\theta \leq 0$.

Le groupe G étant connexe par arcs il existe un chemin $\gamma$ de Id à $s$. L'application

$$\varphi\colon [0,1] \to [-1,1] \qquad\qquad t \mapsto \frac{\mathrm{Tr}(\gamma(t)) - 1}{2}$$

est continue car Tr et $\gamma$ le sont. Par ailleurs $\varphi(0) = \cos 0 = 1$ et $\varphi(1) = \frac{\mathrm{Tr}(s)-1}{2} \leq 0$. Le théorème des valeurs intermédiaires assure donc l'existence de $t_0 \in [0,1]$ tel que $\varphi(t_0) = 0$. La rotation $r = \gamma(t_0)$ a un angle de $\pm\frac{\pi}{2}$. Par conséquent $R = r^2$ est une rotation d'angle $\pi$, *i.e.* un retournement.

e) Tout élément de $\mathrm{SO}_3$ est la composition d'un nombre pair de réflexions. Il suffit donc de montrer que la composée de deux réflexions est une composée de deux retournements.

Soient $x$ et $y$ deux points de $\mathbb{R}^3 \smallsetminus \{0\}$. On désigne par $\tau_x$ et $\tau_y$ les réflexions respectives par rapport à $x^\perp$ et $y^\perp$. On a

$$\tau_x \circ \tau_y = (-\tau_x) \circ (-\tau_y)$$

et $-\tau_x$ et $-\tau_y$ sont des retournements.

f) D'après d) le groupe G contient un retournement. Puisque G est distingué pour tout $g$ dans $\mathrm{SO}_3$ $gRg^{-1}$ appartient à G. Par ailleurs $\mathrm{Tr}(gRg^{-1}) = \mathrm{Tr}(R)$ donc $gRg^{-1}$ est aussi un retournement. Si le vecteur $u$ appartient à l'axe $\Delta$ de $R$ on a $(gRg^{-1})(g(u)) = g(u)$, c'est-à-dire $gRg^{-1}$ est un retournement d'axe $g(\Delta)$. Étant donnée une droite $D$ de $\mathbb{R}^3$ on peut trouver une rotation $g$ de $\mathbb{R}^3$ telle que $D = g(\Delta)$ en prenant un axe orthogonal à $D$ et $\Delta$ et un angle ad hoc (*i.*e. $\mathrm{SO}_3$ agit transitivement sur les droites de $\mathbb{R}^3$). Le groupe G contient donc tous les retournements. On conclut en invoquant le e) qui assure que les retournements engendrent $\mathrm{SO}_3$.

g) Soit G un sous-groupe distingué de $\mathrm{SO}_3$. Montrons que $\mathrm{G} = \{\mathrm{Id}\}$ ou $\mathrm{G} = \mathrm{SO}_3$. Désignons par $\mathrm{G}_0$ la composante connexe par acrs de Id. D'après b) et c) $\mathrm{G}_0$ est un sous-groupe distingué de $\mathrm{SO}_3$ ; par définition $\mathrm{G}_0$ est connexe par arcs. Si $\mathrm{G}_0 \neq \{\mathrm{Id}\}$, alors $\mathrm{G}_0 = \mathrm{SO}_3$ par f) et donc $\mathrm{G} = \mathrm{SO}_3$.

Supposons que $\mathrm{G}_0 = \{\mathrm{Id}\}$ et montrons que $\mathrm{G} = \{\mathrm{Id}\}$. Remarquons que toutes les composantes connexes par arcs de G sont des singletons ; en effet si $g'$ est dans la composante de $g$, relié par le chemin $\gamma$, alors $t \mapsto g^{-1}\gamma(t)$ est un chemin de G reliant Id à $g^{-1}g'$. Par suite $g^{-1}g'$ appartient à $\mathrm{G}_0 = \{\mathrm{Id}\}$ et $g' = g$.

Raisonnons par l'absurde : supposons que G contienne un élément $g$ distinct de Id. Soit $h$ une rotation quelconque non triviale. Soit $\theta$ une mesure de l'angle de $h$. Pour tout $t \in [0,1]$ on désigne par $h_t$ la rotation de même axe et d'angle $t\theta$. L'application $t \mapsto h_t$ est continue car elle se traduit matriciellement dans une certaine base orthonormale par

$$t \mapsto \begin{pmatrix} \cos(t\theta) & -\sin(t\theta) & 0 \\ \sin(t\theta) & \cos(t\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

L'application

$$[0,1] \to \mathrm{G} \qquad\qquad t \mapsto h_t g h_t^{-1}$$

est un chemin de G (car G est distingué) d'origine $g$ et d'extrémité $hgh^{-1}$. Il s'en suit que $hgh^{-1}$ appartient à la composante connexe par arcs de $g$. Cette dernière étant réduite à un singleton on obtient $hgh^{-1} = g$. Or si $g$ est une rotation d'axe $\Delta$, $hgh^{-1}$ est une rotation d'axe $h(\Delta)$. Par conséquent $h(\Delta) = \Delta$ ce qui est impossible (une droite ne peut pas être invariante par toutes les rotations de l'espace).

**Exercice 23.**

On note $\mathbb{H}_8$ le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$, appelé *groupe des quaternions* engendré par les trois matrices

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad J = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix} \qquad K = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix}$$

1. Calculer l'ordre de $\mathbb{H}_8$.
2. Exhiber les sous-groupes de $\mathbb{H}_8$.
3. Exhiber les sous-groupes distingués de $\mathbb{H}_8$.
4. Est-il isomorphe au groupe diédral $\mathrm{D}_8$ ?

**Éléments de solution 23.**

1. On vérifie que

$$I^2 = J^2 = K^2 = -\mathrm{id} \qquad\qquad IJ = K.$$

   Par conséquent le groupe des quaternions est

$$\mathbb{H}_8 = \{\mathrm{id}, -\mathrm{id}, I, -I, J, -J, K, -K\}.$$

   En particulier il est d'ordre 8.
2. D'après le théorème de Lagrange les sous-groupes propres de $\mathbb{H}_8$ sont d'ordre 2 ou 4. Il y a un seul sous-groupe d'ordre 2 : $\langle -\mathrm{id}\rangle$ et trois sous-groupes d'ordre 4 : $\langle I\rangle$, $\langle J\rangle$, $\langle K\rangle$.
3. Tous les sous-groupes de $\mathbb{H}_8$ sont distingués.
4. Le groupe diédral $\mathrm{D}_8$ compte 5 éléments d'ordre 2 donc n'est pas isomorphe à $\mathbb{H}_8$ qui n'en compte qu'un.