Feuille d'exercices n° 2 : Actions de groupes, sous-groupes distingués

Exercice 1 Soit $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ le groupe des matrices inversibles 2×2 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.

1. Quel est l'ordre de $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$?
2. Soit E un espace vectoriel de dimension 2 sur le corps $\mathbb{Z}/2\mathbb{Z}$. Définir une action non triviale de $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ sur E.
3. En déduire que $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est isomorphe au groupe $\mathcal{S}_3$ des permutations de l'ensemble $\{1, 2, 3\}$.

Solution 1

1. Les éléments de $\mathrm{G} = \mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ sont les matrices inversibles dans $\mathbb{Z}/2\mathbb{Z}$. En voici la liste

$$\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \quad \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \quad \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \quad \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix} \quad \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \quad \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}$$

   Il en résulte que G est un groupe d'ordre 6.
2. Soit E un espace vectoriel de dimension 2 sur le corps $\mathbb{Z}/2\mathbb{Z}$. Définissons une action non triviale de $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ sur E.

   À chaque base (v, w) de l'espace vectoriel E correspond une action de G sur E : pour $g \in \mathrm{G}$ et $u \in E$ on définit $g * u \in E$ comme l'image du vecteur u par l'application linéaire de matrice g dans la base (v, w).
3. Montrons que $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est isomorphe au groupe $\mathcal{S}_3$ des permutations de l'ensemble $\{1, 2, 3\}$.

   Fixons une base de E et considérons l'action correspondante de G sur E. Pour tout $g \in \mathrm{G}$ l'application $\varphi_g \colon u \mapsto g * u$ est définie par les images des vecteurs non nuls de E ; en effet le vecteur nul a toujours pour image lui-même.

   Ainsi à tout élément de G est associée une permutation de $E \smallsetminus \{0\}$. Or E compte $2^2 = 4$ éléments. Soient v_1, v_2 et v_3 les trois vecteurs non nuls de E. Alors

$$g \mapsto \big((v_1, v_2, v_3) \mapsto (g * v_1, g * v_2, g * v_3)\big)$$

   définit un homomorphisme de groupes de G dans $\mathcal{S}_3$. Cet homomorphisme est injectif. Par suite G est isomorphe à un sous-groupe de $\mathcal{S}_3$. Puisque G et $\mathcal{S}_3$ ont même ordre, G est isomorphe à $\mathcal{S}_3$.

Exercice 2 Soit p un nombre premier. Soit $n \geqslant 1$ un entier. Soient G un groupe d'ordre p^n et $Z(\mathrm{G})$ son centre. Considérons un sous-groupe distingué H de G non trivial.

1. Montrer que $\mathrm{H} \cap Z(\mathrm{G}) \neq \{e\}$.
2. Montrer que l'ordre de $Z(\mathrm{G})$ est > 1.

Indication : faire agir G par conjugaison sur H.

Solution 2 Soit p un nombre premier. Soit $n \geqslant 1$ un entier. Soient G un groupe d'ordre p^n et $Z(\mathrm{G})$ son centre. Considérons un sous-groupe distingué H de G non trivial.

1. Montrons que $\mathrm{H} \cap Z(\mathrm{G}) \neq \{e\}$. Faisons agir G par conjugaison sur H ; notons que c'est possible car H étant distingué dans G nous avons $\forall\, g \in \mathrm{G},\ g\mathrm{H}g^{-1} \subset \mathrm{H}$.
   L'ordre de H est une puissance de p soit p^β car $|\mathrm{H}|$ divise $|\mathrm{G}|$ qui est une puissance de p. L'ordre de H est aussi somme des cardinaux des orbites pour cette action ; chacune de ces orbites a pour cardinal un diviseur de $|\mathrm{G}|$, c'est-à-dire de p^n donc une puissance de p.
   Raisonnons par l'absurde : supposons que $Z(\mathrm{G}) \cap \mathrm{H} = \{e\}$; alors une seule des orbites est réduite à un seul élément : l'orbite de e. Nous avons alors
   $$|\mathrm{H}| = p^\beta = 1 + \text{ somme de puissances de } p$$
   contradiction. Par suite $Z(\mathrm{G}) \cap \mathrm{H} \neq \{e\}$.
2. Montrons que l'ordre de $Z(\mathrm{G})$ est > 1. Nous allons encore appliquer la formule des classes. Remarquons que les orbites de G pour l'action de G par conjugaison sur lui-même ont pour cardinal des puissances de p ; en effet ces cardinaux sont des diviseurs de $|\mathrm{G}| = p^n$.
   Raisonnons par l'absurde : supposons que $|Z(\mathrm{G})| = 1$, alors
   $$p^n = |\mathrm{G}| = 1 + \text{ somme de puissances de } p$$
   contradiction. Il en résulte que $|Z(\mathrm{G})| > 1$.

Exercice 3 Soient G un groupe fini et $Z(\mathrm{G})$ son centre. Considérons l'action de G sur lui-même par conjugaison.

1. Supposons G non abélien. Soit g un élément de $\mathrm{G} \smallsetminus Z(\mathrm{G})$; notons $\mathrm{Stab}(g)$ le stabilisateur de g.
   Montrer que $Z(\mathrm{G}) \subset \mathrm{Stab}(g) \subset \mathrm{G}$ (les inclusions sont strictes).
2. En déduire que si G n'est pas abélien, alors $Z(\mathrm{G})$ est un sous-groupe de G dont l'indice est strictement supérieur au plus petit nombre premier divisant l'ordre $|\mathrm{G}|$ de G.
3. Soit p un nombre premier. Soit n un entier.
   Quelles sont les valeurs possibles pour l'ordre du centre d'un groupe d'ordre p^n ?
   Quel est le centre d'un groupe d'ordre p^2 ?
   Quel est le centre d'un groupe non abélien d'ordre p^3 ?
4. Donner un exemple de groupe d'ordre p^3 non abélien.
5. Montrer que si G est d'ordre p^2, alors $\mathrm{G} \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Solution 3 Soient G un groupe fini et $Z(\mathrm{G})$ son centre. Considérons l'action de G sur lui-même par conjugaison.

1. Supposons G non abélien. Soit g un élément de $\mathrm{G} \smallsetminus Z(\mathrm{G})$; notons $\mathrm{Stab}(g)$ le stabilisateur de g.
   Montrons que $Z(\mathrm{G}) \subset \mathrm{Stab}(g) \subset \mathrm{G}$ (les inclusions sont strictes).
   L'inclusion $Z(\mathrm{G}) \subseteq \mathrm{Stab}(g)$ est claire.
   Soit $g \in \mathrm{G} \smallsetminus Z(\mathrm{G})$ (un tel élément existe car G n'est pas abélien). Remarquons que g appartient à $\mathrm{Stab}(g)$; en effet $ggg^{-1} = g$. Par suite $Z(\mathrm{G})$ est strictement inclus dans $\mathrm{Stab}(g)$.
   Soit $g \in \mathrm{G} \smallsetminus Z(\mathrm{G})$ (un tel élément existe car G n'est pas abélien). Puisque $g \notin Z(\mathrm{G})$ il existe un élément $h \in \mathrm{G}$ qui ne commute pas avec g donc qui n'appartient pas à $\mathrm{Stab}(g)$. Il en résulte que $\mathrm{Stab}(g)$ est un sous-groupe propre de G.
2. Supposons que G ne soit pas abélien, montrons qu'alors $Z(\mathrm{G})$ est un sous-groupe de G dont l'indice est strictement supérieur au plus petit nombre premier p divisant l'ordre $|\mathrm{G}|$ de G.
   D'après 1. si G n'est pas abélien et si g appartient à $\mathrm{G} \smallsetminus Z(\mathrm{G})$, alors l'indice de $|\mathrm{G} : Z(\mathrm{G})| > |\mathrm{G} : \mathrm{Stab}(g)|$.
   Mais $|\mathrm{G} : \mathrm{Stab}(g)| \geqslant p$ car $|\mathrm{G} : \mathrm{Stab}(g)|$ divise $|\mathrm{G}|$. Par suite $|\mathrm{G} : Z(\mathrm{G})| > p$.
3. Soit p un nombre premier. Soit n un entier.
   Donnons les valeurs possibles pour l'ordre du centre d'un groupe d'ordre p^n.
   Si G est abélien, alors $|Z(\mathrm{G})| = p^n$.
   Si G n'est pas abélien, alors $|\mathrm{G} : Z(\mathrm{G})| > p$ donc $|Z(\mathrm{G})| < p^{n-1}$. L'exercice précédent assure que $Z(\mathrm{G})$ n'est pas réduit à l'élément neutre donc $|Z(\mathrm{G})| \geqslant p$. Finalement lorsque G n'est pas abélien, nous avons
   $$|Z(\mathrm{G})| \in \left\{p,\, p^2,\, \ldots,\, p^{n-2}\right\}$$
   Si $n = 2$, le groupe G est nécessairement abélien.
   Déterminons le centre d'un groupe d'ordre p^2. Le centre d'un groupe G d'ordre p^2 est donc G tout entier.
   Déterminons le centre d'un groupe non abélien d'ordre p^3. Le centre d'un groupe non abélien d'ordre p^3 est d'ordre p.

4. Donnons un exemple de groupe d'ordre p^3 non abélien.
   Le groupe des quaternions est un groupe d'ordre 2^3 (ici $p = 2$) et n'est pas abélien.
5. Montrons que si G est d'ordre p^2, alors $\mathrm{G} \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
   Soit G un groupe d'ordre p^2. Il est abélien. Nous avons l'alternative suivante :
   — ou bien G contient un élément d'ordre p^2 auquel cas G est cyclique et isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$;
   — ou bien tous les éléments de $\mathrm{G} \setminus \{e\}$ sont d'ordre p. Soient x et y deux éléments de $\mathrm{G} \setminus \{e\}$ tels que $y \notin \langle x \rangle$. Alors $\langle x \rangle \cap \langle y \rangle = \{e\}$. En effet le sous-groupe $\langle x \rangle \cap \langle y \rangle$ est d'ordre strictement inférieur à p et d'ordre divisant p donc d'ordre 1. Puisque tout sous-groupe du groupe abélien G est distingué G est isomorphe à $\langle x \rangle \times \langle y \rangle$ (Exercice 10). Or $\langle x \rangle \simeq \langle y \rangle \simeq \mathbb{Z}/p\mathbb{Z}$. Ainsi $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 4 Soient E un ensemble et G un groupe opérant sur E. Soient g et h des éléments de E appartenant à la même orbite.
Montrer que les stabilisateurs Stab_g et Stab_h sont des sous-groupes conjugués de G.
En déduire que Stab_g et Stab_h ont même ordre.

Solution 4 Soient E un ensemble et G un groupe opérant sur E. Soient g et h des éléments de E appartenant à la même orbite. Alors il existe x dans G tel que $h = x \cdot g$.
Soit $y \in \mathrm{Stab}_g$. Alors $y \cdot g = g$. De plus d'une part $y \cdot g = y \cdot (x^{-1}h)$ et d'autre part $g = x^{-1}h$. Par conséquent $y \cdot (x^{-1}h) = x^{-1}h$, soit $xyx^{-1} \cdot h = h$ c'est-à-dire xyx^{-1} appartient à Stab_h. Autrement dit $x\mathrm{Stab}_g x^{-1} \subset \mathrm{Stab}_h$.
Un raisonnement similaire conduit à $\mathrm{Stab}_h \subset x\mathrm{Stab}_g x^{-1}$.
Il s'en suit que $\mathrm{Stab}_h = x\mathrm{Stab}_g x^{-1}$.
L'application $y \mapsto xyx^{-1}$ est un automorphisme de G. C'est donc une bijection et l'image de Stab_g par cet automorphisme est Stab_h. Ces deux ensembles ont donc même cardinal.

Exercice 5 Soit E un ensemble fini. Soit G un groupe fini qui opère sur E. Pour tout g dans G on définit

$$E^g = \big\{ s \in E \,|\, gs = s \big\}.$$

Autrement dit E^g est l'ensemble des points fixes de E sous l'action de g. Pour $s \in E$, on note G_s le fixateur de s pour l'action de G sur E.

1. Construire la table de l'opération
$$\varphi \colon \mathrm{G} \times E \to \{ \text{ vrai=V, faux=F } \}$$
définie par
$$\begin{cases} \varphi(g,s) = V \text{ si } gs = s \\ \varphi(g,s) = F \text{ sinon} \end{cases}$$
dans le cas où $\mathrm{G} = \mathrm{D}_6$ et $E = \{A, B, C\}$ où ABC est un triangle équilatéral.
2. Démontrer que $\displaystyle\sum_{s \in E} |\mathrm{G}_s| = \sum_{g \in \mathrm{G}} \mathrm{card}(E^g)$.
3. En déduire la formule de Burnside
$$|\mathrm{G}| \times \text{ le nombre d'orbites } = \sum_{g \in \mathrm{G}} \mathrm{card}(E^g).$$

Solution 5

1. Construisons la table de l'opération
$$\varphi \colon \mathrm{G} \times E \to \{ \text{ vrai=V, faux=F } \}$$
définie par
$$\begin{cases} \varphi(g,s) = V \text{ si } gs = s \\ \varphi(g,s) = F \text{ sinon} \end{cases}$$
dans le cas où $\mathrm{G} = \mathrm{D}_6$ et $E = \{A, B, C\}$ où ABC est un triangle équilatéral.
Désignons par O le centre de gravité du triangle équilatéral ABC et par ρ la rotation de centre O et d'angle $\frac{2\pi}{3}$. Soient s_A, s_B et s_C les symétries d'axes respectifs AO, BO et CO.
Nous obtenons la table suivante

	A	B	C
id	V	V	V
ρ	F	F	F
ρ^2	F	F	F
s_A	V	F	F
s_B	F	V	F
s_C	F	F	V

En effet

(a) $\mathrm{id}(A) = A$, $\mathrm{id}(B) = B$ et $\mathrm{id}(C) = C$;

(b) $\rho(A) \in \{B, C\}$, $\rho(B) \in \{A, C\}$ et $\rho(C) \in \{A, B\}$;

(c) $\rho^2(A) \in \{B, C\}$, $\rho^2(B) \in \{A, C\}$ et $\rho^2(C) \in \{A, B\}$;

(d) $s_A(A) = A$, $s_A(B) = C$ et $s_A(C) = B$;

(e) $s_B(B) = B$, $s_B(A) = C$ et $s_B(C) = A$;

(f) $s_C(C) = C$, $s_C(A) = B$ et $s_C(B) = A$.

2. Montrons que $\displaystyle\sum_{s\in E} |\mathrm{G}_s| = \sum_{g\in \mathrm{G}} \mathrm{card}(E^g)$.

Posons $p = |\mathrm{G}|$. Notons g_1, g_2, …, g_p les éléments de G. Posons $q = \mathrm{card}(E)$. Notons s_1, s_2, …, s_q les éléments de E.

D'une part

$$\begin{aligned}\varphi^{-1}(V) &= \big\{(g,s) \in \mathrm{G}\times E \,|\, gs = s\big\}\\ &= \big\{(g,s) \in \mathrm{G}\times E \,|\, s \in E^g\big\}\\ &= \{g_1\}\times E^{g_1} \cup \{g_2\}\times E^{g_2} \cup \ldots \cup \{g_p\}\times E^{g_p}\end{aligned}$$

ce qui conduit à

$$\mathrm{card}(\varphi^{-1}(V)) = \sum_{g\in \mathrm{G}} \mathrm{card}(E^g)$$

D'autre part

$$\begin{aligned}\varphi^{-1}(V) &= \big\{(g,s) \in \mathrm{G}\times E \,|\, gs = s\big\}\\ &= \big\{(g,s) \in \mathrm{G}\times E \,|\, g \in \mathrm{G}_s\big\}\\ &= \mathrm{G}_{s_1}\times \{s_1\} \cup \mathrm{G}_{s_2}\times \{s_2\} \cup \ldots \cup \mathrm{G}_{s_q}\times \{s_q\}\end{aligned}$$

ce qui entraîne

$$\mathrm{card}(\varphi^{-1}(V)) = \sum_{s\in E} |\mathrm{G}_s|.$$

Il en résulte que

$$\sum_{g\in \mathrm{G}} \mathrm{card}(E^g) = \sum_{s\in E} |\mathrm{G}_s|.$$

3. Si s est un élément de E, on désigne par $\mathcal{O}_s$ l'orbite de s sous l'action de G. On sait que $|\mathrm{G}_s| = \frac{|\mathrm{G}|}{\mathrm{card}(\mathcal{O}_s)}$. Par suite

$$\sum_{g\in \mathrm{G}} \mathrm{card}(E^g) = |\mathrm{G}| \left(\frac{1}{\mathrm{card}(\mathcal{O}_{s_1})} + \frac{1}{\mathrm{card}(\mathcal{O}_{s_2})} + \ldots + \frac{1}{\mathrm{card}(\mathcal{O}_{s_q})}\right)$$

Soient σ_1, σ_2, …, σ_r des éléments de E tels que E est la réunion disjointe des $\mathcal{O}_{\sigma_i}$ pour $1 \leqslant i \leqslant r$. Nous avons

$$\sum_{s\in \mathcal{O}_{\sigma_i}} \frac{1}{\mathrm{card}(\mathcal{O}_s)} = \sum_{s\in \mathcal{O}_{\sigma_i}} \frac{1}{\mathrm{card}(\mathcal{O}_{\sigma_i})} = \frac{1}{\mathrm{card}(\mathcal{O}_{\sigma_i})} \sum_{s\in \mathcal{O}_{\sigma_i}} 1 = \frac{1}{\mathrm{card}(\mathcal{O}_{\sigma_i})} \times \mathrm{card}(\mathcal{O}_{\sigma_i}) = 1$$

d'où la formule de Burnside.

Exercice 6 Soit G un groupe. Soient H et K deux sous-groupes distingués de G.
Montrer que le sous-groupe de G engendré par $\mathrm{H} \cup \mathrm{K}$ est aussi distingué dans G.

Solution 6 Soient $g \in \mathrm{G}$ et $x \in \langle \mathrm{H} \cup \mathrm{K} \rangle$. Il existe donc y_1, y_2, …, y_m dans $\mathrm{H} \cup \mathrm{K}$ tels que $x = y_1 y_2 \dots y_m$ et

$$gxg^{-1} = gy_1y_2 \dots y_m g^{-1}.$$

Si y_1 appartient à H alors puisque H est distingué dans G il existe $y_1' \in \mathrm{H}$ tel que $gy_1 = y_1'g$. Si y_1 appartient à K alors puisque K est distingué dans G il existe $y_1'' \in \mathrm{K}$ tel que $gy_1 = y_1''g$. Ainsi il existe $z_1 \in \mathrm{H} \cup \mathrm{K}$ tel que $gy_1 = z_1 g$.

En fait pour tout $1 \leqslant i \leqslant m$ il existe $z_i \in \mathrm{H} \cup \mathrm{K}$ tel que $gy_i = z_i g$.

Nous obtenons donc

$$\begin{aligned} gxg^{-1} &= gy_1y_2 \dots y_m g^{-1} \\ &= z_1 g y_2 \dots y_m g^{-1} \\ &= z_1 z_2 g \dots y_m g^{-1} \\ &= \dots \\ &= z_1 z_2 \dots z_m g g^{-1} \\ &= z_1 z_2 \dots z_m \end{aligned}$$

Or $z_1 z_2 \dots z_m$ appartient à $\mathrm{H} \cup \mathrm{K}$ donc gxg^{-1} appartient à $\mathrm{H} \cup \mathrm{K}$. Ainsi $\langle \mathrm{H} \cup \mathrm{K} \rangle$ est distingué dans G.

Exercice 7 Soit G un groupe. Rappelons que le centralisateur d'un élément de G est l'ensemble des éléments de G qui commutent avec lui.

1. Montrer que le centralisateur d'un élément de G est un sous-groupe de G.
2. Dans $\mathcal{S}_4$ quel est le centralisateur de $(1\ 2)$? Est-ce un sous-groupe distingué de $\mathcal{S}_4$?

Solution 7

1. Soit G un groupe. Montrons que le centralisateur C_g d'un élément g de G est un sous-groupe de G.
   Notons que e appartient à C_g.
   Soit x dans C_g. Alors $gx = xg$ d'où $x^{-1}gxx^{-1} = x^{-1}xgx^{-1}$ c'est-à-dire $x^{-1}g = gx^{-1}$, autrement dit x^{-1} appartient à C_g.
   Soient x et y dans C_g. Alors

   $$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$$

   i.e. xy appartient à C_g.
   Il en résulte que C_g est un sous-groupe de G.
2. Déterminons le centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$.
   Soit σ un élément de $\mathcal{S}_n$. Si $(i\ j)$ est une transposition quelconque alors $\sigma(i\ j)\sigma^{-1} = (\sigma(i)\ \sigma(j))$. En effet soit $y \in \{1, 2, \dots, n\}$;
   - si $y = \sigma(i)$, alors $\big(\sigma(i\ j)\sigma^{-1}\big)(y) = \sigma(j)$;
   - si $y = \sigma(j)$, alors $\big(\sigma(i\ j)\sigma^{-1}\big)(y) = \sigma(i)$;
   - si $y \notin \{\sigma(i), \sigma(j)\}$, alors $\big((i\ j)\sigma^{-1}\big)(y) = \sigma^{-1}(y)$ et $\big(\sigma(i\ j)\sigma^{-1}\big)(y) = y$.

   Ainsi le centralisateur de $(i\ j)$ est constitué des permutations $\sigma \in \mathcal{S}_n$ qui laisse l'ensemble $\{i, j\}$ invariant, *i.e.* des permutations $\sigma \in \mathcal{S}_n$ telles que $\sigma(i) = i$ ou j et $\sigma(j) = j$ ou i. En particulier le centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$ est $\{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$.
   Considérons la permutation $(3\ 4)$ qui appartient au centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$. Conjuguons là par la transposition $(2\ 3)$. Nous obtenons $(2\ 4)$, *i.e.* $(2\ 3)(1\ 2)(2\ 3) = (2\ 4)$. En particulier $(2\ 3)(1\ 2)(2\ 3)$ n'appartient pas au centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$. Le centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$ n'est donc pas un sous-groupe distingué de $\mathcal{S}_4$.

Exercice 8 Soit G un groupe. Soient H et K deux groupes de G. Considérons un sous-groupe L de $\mathrm{H} \cap \mathrm{K}$ qui est distingué dans H et dans K.
Montrer que L est distingué dans le sous-groupe de G engendré par $\mathrm{H} \cup \mathrm{K}$.

Solution 8 Le sous-groupe L est un sous-groupe de $\langle \mathrm{H} \cup \mathrm{K} \rangle$. Soit z un élément de $\langle \mathrm{H} \cup \mathrm{K} \rangle$. Nous pouvons écrire z sous la forme $z_1 z_2 \dots z_m$ les z_i, $1 \leqslant i \leqslant m$, appartenant à $\mathrm{H} \cup \mathrm{K}$.

Soit $\ell \in \mathrm{L}$; alors

$$z\ell z^{-1} = z_1 z_2 \dots (z_m \ell z_m^{-1}) \dots z_2^{-1} z_1^{-1}.$$

L'élément $z_m \ell z_m^{-1}$ appartient à L ; en effet si z_m appartient à H (resp. K), nous utilisons le fait que L est distingué dans H (resp. K).

Nous en déduisons de la même façon que $z_{m-1} z_m \ell z_m^{-1} z_{m-1}^{-1}$ appartient à L. Par récurrence $z\ell z^{-1}$ appartient à L ce qui prouve que L est distingué dans $\langle \mathrm{H} \cup \mathrm{K} \rangle$.

Exercice 9 Montrer que dans un groupe tout sous-groupe d'indice 2 est distingué.

Solution 9 Soit G un groupe. Soit H un sous-groupe d'indice 2 de G. Nous avons donc ${}^{\mathrm{G}}\!/_{\mathrm{H}} = \{\mathrm{H}, x\mathrm{H}\}$ où $x \neq \mathrm{H}$ et $\mathrm{G} = \mathrm{H} \cup x\mathrm{H}$ avec $\mathrm{H} \cap x\mathrm{H} = \emptyset$.

Soit $g \in \mathrm{G}$. Ou bien $g \in \mathrm{H}$ et $g\mathrm{H}g^{-1} = \mathrm{H}$. Ou bien $g \notin \mathrm{H}$ et $g \in x\mathrm{H}$; il existe donc $h_0 \in \mathrm{H}$ tel que $g = xh_0$. Soit alors $h \in \mathrm{H}$; nous avons

$$ghg^{-1} = xh_0 h h_0^{-1} x^{-1} = xh'x^{-1}$$

où $h' = h_0 h h_0^{-1} \in \mathrm{H}$. Si $xh'x^{-1}$ n'appartient pas à H, alors $xh'x^{-1}$ appartient à $x\mathrm{H}$, *i.e.* $xh'x^{-1}$ s'écrit xh_1 avec h_1 dans H. Ceci implique que x appartient à H : contradiction. Par conséquent $xh'x^{-1}$ appartient à H, *i.e.* ghg^{-1} appartient à H. Autrement dit H est un sous-groupe distingué de G.

Exercice 10 Soit G un groupe. Soient H et K des sous-groupes de G. Supposons que

- H et K sont des sous-groupes distingués de G ;
- $\mathrm{H} \cap \mathrm{K} = \{e\}$;
- $\mathrm{HK} = \mathrm{G}$.

Considérons l'application

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

1. Montrer que φ est une application injective.
2. Montrer que φ est un isomorphisme de groupes.

Solution 10

1. Montrons que φ est une application injective.
   Soient h et h' dans H, soient k et k' dans K. Supposons que $\varphi(h,k) = \varphi(h',k')$, *i.e.* $hk = h'k'$ ce que nous pouvons réécrire $h'^{-1}h = k'k^{-1}$. D'une part $h'^{-1}h$ appartient à H, d'autre part $k'^{-1}k$ appartient à K. Il en résulte que $h'^{-1}h = k'k^{-1}$ appartient à $\mathrm{H} \cap \mathrm{K} = \{e\}$. Ainsi $h = h'$, $k = k'$ et φ est injective.
2. Montrons que φ est un isomorphisme de groupes.
   Par hypothèse $\mathrm{HK} = \mathrm{G}$ donc φ est surjective.
   Soient h, h' dans H et k, k' dans K. Le groupe K étant distingué dans G nous avons $hk = k_1 h$ pour un certain k_1 dans K. Comme H est distingué nous avons $k_1 h = h_1 k_1$ pour un certain h_1 dans H. Or φ est injective donc $h = h_1$, $k = k_1$ et h et k commutent. Par conséquent $hkh'k')hh'kk'$ d'où
   - HK est un sous-groupe de G : la loi est stable dans HK, e appartient à HK et g^{-1} appartient à HK si g appartient à HK ;
   - φ est un morphisme de groupes.

   Par suite φ est un isomorphisme de groupes.

Exercice 11 Soit G un groupe. Soient H et K deux sous-groupes propres de G. Supposons que

- H et K sont des sous-groupes d'indice 2 dans G ;
- $\mathrm{H} \cap \mathrm{K} = \{e\}$.

Montrer que G est isomorphe à ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$.

Solution 11 Les groupes H et K sont d'indice 2 dans G ils sont donc distingués dans G (Exercice 9).

De plus $\mathrm{H} \cap \mathrm{K} = \{e\}$ donc HK est un sous-groupe distingué de G. En effet

- Soient h, h' dans H et k, k' dans K. Le groupe K étant distingué dans G nous avons $hk = k_1 h$ pour un certain k_1 dans K. Comme H est distingué nous avons $k_1 h = h_1 k_1$ pour un certain h_1 dans H. Or φ est injective donc $h = h_1$, $k = k_1$ et h et k commutent. Par conséquent $hkh'k')hh'kk'$. Ainsi HK est un sous-groupe de G : la loi est stable dans HK, e appartient à HK et g^{-1} appartient à HK si g appartient à HK.
- Le groupe HK est distingué dans G ; en effet soient $g \in \mathrm{G}$, $h \in \mathrm{H}$ et $k \in \mathrm{K}$. Comme H est distingué dans G l'élémeent $ghkg^{-1}$ s'écrit aussi $h_1 gkg^{-1}$ avec h_1 dans H. Par ailleurs $h_1 gkg^{-1} = h_1 k_1 gg^{-1} = h_1 k_1$ avec k_1 dans K car K est distingué dans G. Il s'en suit que $ghkg^{-1}$ appartient à HK.
- Montrons que H et K sont d'ordre 2. Nous avons $\mathrm{G} = \mathrm{H} \cup x\mathrm{H}$ avec $x \notin \mathrm{H}$. Comme K est d'indice 2 il est d'ordre au moins 2 et contient donc au moins un élément k qui n'est pas dans H (en particulier $k \neq e$). Nous pouvons donc prendre pour x cet élément k. Ainsi $\mathrm{G} = \mathrm{H} \cup k\mathrm{H}$ avec $\mathrm{H} \cap k\mathrm{H} = \emptyset$. Soit $k' \in \mathrm{K} \setminus \{e\}$. Ainsi k' n'appartient pas à H et $k' \in k\mathrm{H}$. Il existe donc $h \in \mathrm{H}$ tel que $k' = kh$. Par suite $h = k^{-1}k'$ est aussi dans K donc $h = e$ et $k = k'$. Le groupe K contient donc seulement deux éléments : e et k.
  De même nous obtenons que H est d'ordre 2.
  Ainsi H et K sont isomorphes à $\mathbb{Z}/2\mathbb{Z}$.
- Montrons que $\mathrm{G} = \mathrm{KH}$. Soit $g \in \mathrm{G}$. Alors ou bien g appartient à H et donc g appartient à HK, ou bien g appartient à kH, *i.e.* $g = kh$ avec $h \in \mathrm{H}$. Or $\mathrm{HK} = \mathrm{KH}$ donc g appartient à HK.

Finalement G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 12 Pour a et b réels on définit l'application

$$\tau_{a,b} \colon \mathbb{R} \to \mathbb{R} \qquad\qquad x \mapsto ax + b.$$

1. Soit $\mathrm{G} = \{\tau_{a,b} \mid a \neq 0\}$.
   Montrer que G est un groupe pour la composition des applications.
2. Soit $\mathrm{H} = \{\tau_{a,b} \mid a \neq 0,\ a \in \mathbb{Q}\}$.
   Montrer que H est un sous-groupe de G.
3. Décrire les classes à droite de H dans G.
   Montrer que toute classe à gauche (modulo H) est classe à droite (modulo H). (Indication : considérer l'application qui à l'élément $\tau_{a,b}$ de G associe la classe de a dans $\mathbb{R}^*/\mathbb{Q}^*$)
4. Donner un exemple d'un sous-groupe K de G tel qu'une classe à gauche ne soit pas classe à droite.
5. Soit $\mathrm{N} = \{\tau_{a,b} \mid a = 1\}$.
   Montrer que N est un sous-groupe distingué de G.

Solution 12

1. Soit $\mathrm{G} = \{\tau_{a,b} \mid a \neq 0\}$.
   Montrons que G est un groupe pour la composition des applications.
   Soient $\tau_{a,b}$ et $\tau_{a',b'}$ deux éléments de G. Alors $\tau_{a,b}^{-1} = \tau_{1/a,-b/a}$ (notons que $a \neq 0$). De plus $\tau_{a',b'} \circ \tau_{a,b}^{-1} = \tau_{a'/a,-a'b/a+b'}$. Par suite G est un sous-groupe du groupe des bijections de $\mathbb{R}$ dans $\mathbb{R}$.
2. Soit $\mathrm{H} = \{\tau_{a,b} \mid a \neq 0,\ a \in \mathbb{Q}\}$.
   Montrons que H est un sous-groupe de G.
   Soient $\tau_{a,b}$ et $\tau_{a',b'}$ deux éléments de H. Alors $\tau_{a,b}^{-1} = \tau_{1/a,-b/a}$ (notons que $a \neq 0$). De plus $\tau_{a',b'} \circ \tau_{a,b}^{-1} = \tau_{a'/a,-a'b/a+b'}$. Par suite H est un sous-groupe de G.
3. Décrivons les classes à droite de H dans G et montrons que toute classe à gauche (mod H) est classe à droite (modulo H).
   La classe à droite de l'élément $\tau_{\alpha,\beta}$ de G est l'ensemble des $\tau_{\alpha a,\alpha b+\beta}$ où $a \in \mathbb{Q}$.
   Pour montrer que toute classe à gauche est une classe à droite il suffit de montrer que H est distingué dans G. Considérons le morphisme de groupes

   $$\varphi \colon \mathrm{G} \to \mathbb{R}^*/\mathbb{Q}^* \qquad\qquad \tau_{a,b} \mapsto \text{ la classe de } a \text{ dans } \mathbb{R}^*/\mathbb{Q}^*$$

   Son noyau est H qui est donc distingué dans G.
4. Donnons un exemple d'un sous-groupe K de G tel qu'une classe à gauche ne soit pas classe à droite.
   Soit K le sous-groupe de G des éléments $\tau_{a,b}$ où a et b sont rationnels. Les classes à gauche et à droite de K dans G ne coïncident pas.

5. Soit $\mathrm{N} = \{\tau_{a,b} \,|\, a = 1\}$.
   Montrons que N est un sous-groupe distingué de G.
   L'identité appartient à N. Soient $\tau_{1,b}$ et $\tau_{1,b'}$ deux éléments de N. Nous avons $\tau_{1,b} \circ \tau_{1,b'}^{-1} = \tau_{1,b-b'}$; en particulier $\tau_{1,b} \circ \tau_{1,b'}^{-1}$ appartient à N. Ainsi N est un sous-groupe de G.
   Soit $\tau_{\alpha,\beta}$ un élément quelconque de G et soit $\tau_{1,b}$ un élément quelconque de N. Alors

$$\tau_{\alpha,\beta} \circ \tau_{1,b} \circ \tau_{\alpha,\beta}^{-1} = \tau_{\alpha,\beta} \circ \tau_{1,b} \circ \tau_{1/\alpha,-\beta/\alpha} = \tau_{1,\alpha b};$$

   ainsi $\tau_{\alpha,\beta} \circ \tau_{1,b} \circ \tau_{\alpha,\beta}^{-1}$ appartient à N ce qui prouve que N est un sous-groupe distingué de G.

Exercice 13 Soit H un sous-groupe d'un groupe G tel que toute classe à gauche modulo H soit classe à droite modulo H. Le sous-groupe H est-il distingué ?

Solution 13 Supposons que H ne soit pas distingué dans G. Cela signifie qu'il existe $g \in \mathrm{G} \setminus \{e\}$ tel que $g\mathrm{H} \neq \mathrm{H}g$ ou encore qu'il existe $h \in \mathrm{H}$ tel que gh n'appartient pas à $\mathrm{H}g$.

Ainsi gh appartient à une autre classe à droite que nous noterons $\mathrm{H}g'$ ($\mathrm{H}g' \neq \mathrm{H}g$). Puisque toute classe à gauche est une classe à droite et que les classes à droite forment une partition de G la classe à droite qui est égale à $g\mathrm{H}$ est nécessairement $\mathrm{H}g'$.

Donc g appartient à $g\mathrm{H}$ et $\mathrm{H}g$. Comme $g\mathrm{H} = \mathrm{H}g'$ l'élément g appartient aussi à $\mathrm{H}g'$. Autrement dit g appartient à $\mathrm{H}g \cap \mathrm{H}g'$. Ceci n'est possible que si $g = e$ ou $\mathrm{H}g = \mathrm{H}g'$. Mais par hypothèse $g \neq e$ et $\mathrm{H}g \neq \mathrm{H}g'$.

Il en résulte que H est distingué dans G.

Exercice 14 Soit G un groupe fini. Soit H un sous-groupe de G. Soit N un sous-groupe distingué de G.
Montrer que si $|\mathrm{H}|$ et $[\mathrm{G} : \mathrm{N}]$ sont premiers entre eux, alors H est un sous-groupe de N.

Solution 14 Raisonnons par l'absurde : supposons que H ne soit pas un sous-groupe de N. Alors il existe $h \in \mathrm{H}$ qui n'est pas un élément de N. Il s'en suit que $h\mathrm{N}$ est un élément différent de l'élément neutre N de G/N.

Soit q l'ordre de $h\mathrm{N}$ dans G/N. On sait que $q \neq 1$ et que q divise $|\mathrm{G}/\mathrm{N}| = [\mathrm{G} : \mathrm{N}]$. Par ailleurs $h^{|\mathrm{H}|} = e$ donc $(h\mathrm{K})^{|\mathrm{H}|} = \mathrm{H}$. Par suite q divise $|\mathrm{H}|$. Ainsi $q \neq 1$ est un diviseur commun à $[\mathrm{G} : \mathrm{N}]$ et $|\mathrm{H}|$ qui sont premiers entre eux : contradiction. Il en résulte que H est un sous-groupe de N.

Exercice 15 Soit G un groupe qui ne contient qu'un seul sous-groupe H d'ordre n.
Montrer que H est distingué.

Solution 15 Nous allons montrer que H est un sous-groupe caractérisque de G. Soit φ un automorphisme de G et $\varphi_{|\mathrm{H}} \colon \mathrm{H} \to \varphi(\mathrm{H})$ la restriction de φ à H et à son image. Comme φ est un automorphisme de G, $\varphi_{|\mathrm{H}}$ est bijective. C'est donc un isomorphisme de groupes. Étant donné que H est fini d'ordre n, $\varphi(\mathrm{H})$ est fini d'ordre n. Or H est l'unique sous-groupe de G d'ordre n donc $\varphi(\mathrm{H}) = \mathrm{H}$.

Puisque H est un sous-groupe caractéristique de G c'est un sous-groupe distingué de G.

Exercice 16 Soit H un sous-groupe de G tel que le produit de deux classes à gauche modulo H soit une classe à gauche modulo H.
Le sous-groupe H est-il distingué ?

Solution 16 Comme le produit de deux classes à gauche est une classe à gauche pour tout couple (g, g') d'éléments de G il existe $g'' \in \mathrm{G}$ tel que $g\mathrm{H}g'\mathrm{H} = g''\mathrm{H}$. En particulier il existe g'' tel que $g\mathrm{H}g^{-1}\mathrm{H} = g''\mathrm{H}$. Et pour tout élément h de H il existe h' et h'' dans H tels que $ghg^{-1}h' = g''h''$. En particulier puisque e appartient à H il existe h'' dans H tel que $geg^{-1}e = g''h''$ ce qui se réécrit $e = g''h''$. Ainsi $g'' = h''^{-1} \in \mathrm{H}$ et $g\mathrm{H}g^{-1}\mathrm{H} = \mathrm{H}$, c'est-à-dire $g\mathrm{H}g^{-1} = \mathrm{H}$. Le sous-groupe H est donc distingué dans G.

Exercice 17 Soit G un groupe. Soit H un sous-groupe distingué de G.
Montrer que si H est cyclique tout sous-groupe de H est distingué dans G.

Solution 17 Soit h un générateur de H. Soit K un sous-groupe du groupe cyclique distingué H. Alors tous les éléments de K sont égaux à une puissance de h et K est lui-même cyclique engendré par une puissance de h.

Posons $p_0 = \inf\{p \in \mathbb{N}^* \,|\, h^p \in \mathrm{K}\}$. Soit h^p un élément de K. Nous avons $p = qp_0 + r$ avec $0 \leqslant r < p_0$. Par suite $h^p = (h^{p_0})^q h^r$ et $h^r = h^p (h^{-p_0})^q$ appartient à K. Puisque $p_0 = \inf\{p \in \mathbb{N}^* \,|\, h^p \in \mathrm{K}\}$ nous avons nécessairement $r = 0$ et $\mathrm{K} = \langle h^{p_0} \rangle$.

Puisque H est distingué dans G pour tout $g \in \mathrm{G}$ il existe q tel que $ghg^{-1} = h^q$. Par conséquent $gh^{p_0}g^{-1} = h^{qp_0}$ et K est distingué dans G.

Exercice 18 Soient A un groupe et C un sous-groupe distingué de A. Soient B un groupe et D un sous-groupe distingué de B.

Montrer que $^{\mathrm{A}\times\mathrm{B}}\!/_{\mathrm{C}\times\mathrm{D}} \simeq {}^{\mathrm{A}}\!/_{\mathrm{C}} \times {}^{\mathrm{B}}\!/_{\mathrm{D}}$.

Solution 18 Considérons l'homomorphisme de groupes entre $\mathrm{A}\times\mathrm{B}$ et $^{\mathrm{A}}\!/_{\mathrm{C}} \times {}^{\mathrm{B}}\!/_{\mathrm{D}}$ donné par

$$\varphi((a,b)) = (a\mathrm{C}, b\mathrm{D}).$$

Le noyau de φ est égal à

$$\begin{aligned}\ker\varphi &= \big\{(a,b)\in\mathrm{A}\times\mathrm{B}\,|\,a\mathrm{C}=\mathrm{C}\text{ et }b\mathrm{D}=\mathrm{D}\big\}\\ &= \big\{(a,b)\in\mathrm{A}\times\mathrm{B}\,|\,a\in\mathrm{C}\text{ et }b\in\mathrm{D}\big\}\\ &= \mathrm{C}\times\mathrm{D}.\end{aligned}$$

Par ailleurs $(a\mathrm{C}, b\mathrm{D})$ est l'image de (a,b) par φ donc φ est surjectif. Il en résulte que φ induit un isomorphisme entre $^{\mathrm{A}\times\mathrm{B}}\!/_{\mathrm{C}\times\mathrm{D}}$ et $^{\mathrm{A}}\!/_{\mathrm{C}} \times {}^{\mathrm{B}}\!/_{\mathrm{D}}$.

Exercice 19 Soient G_1 et G_2 deux groupes non isomorphes.

1. Montrer que $Z(\mathrm{G}_1)\times Z(\mathrm{G}_2)$ est isomorphe à $Z(\mathrm{G}_1\times\mathrm{G}_2)$.
2. Supposons que G_1 et G_2 sont des groupes simples.
   (a) Montrer que $\mathrm{G}_1\times\mathrm{G}_2$ contient un sous-groupe distingué H_1 isomorphe à G_1 et un sous-groupe distingué H_2 isomorphe à G_2.
   (b) Montrer que si H est un sous-groupe distingué de $\mathrm{G}_1\times\mathrm{G}_2$, alors $\mathrm{H}\cap\mathrm{H}_1$ est distingué dans H_1 et $\mathrm{H}\cap\mathrm{H}_2$ est distingué dans H_2.
   (c) En déduire que H_1 et H_2 sont les seuls sous-groupes distingués de $\mathrm{G}_1\times\mathrm{G}_2$.

Solution 19

1. Montrons que $Z(\mathrm{G}_1)\times Z(\mathrm{G}_2)$ est isomorphe à $Z(\mathrm{G}_1\times\mathrm{G}_2)$.
   Soit $(x_1,x_2)\in\mathrm{G}_1\times\mathrm{G}_2$; alors (x_1,x_2) appartient à $Z(\mathrm{G}_1\times\mathrm{G}_2)$ si et seulement si
   $$\forall\,(y_1,y_2)\in\mathrm{G}_1\times\mathrm{G}_2 \qquad (x_1,x_2)(y_1,y_2)=(y_1,y_2)(x_1,x_2)$$
   si et seulement si
   $$\forall\,(y_1,y_2)\in\mathrm{G}_1\times\mathrm{G}_2 \qquad (x_1y_1,x_2y_2)=(y_1x_1,y_2x_2)$$
   si et seulement si
   $$\forall\,(y_1,y_2)\in\mathrm{G}_1\times\mathrm{G}_2 \qquad x_1y_1=y_1x_1 \text{ et } x_2y_2=y_2x_2.$$
   Par conséquent (x_1,x_2) appartient à $Z(\mathrm{G}_1\times\mathrm{G}_2)$ si et seulement si x_1 appartient à $Z(\mathrm{G}_1)$ et x_2 appartient à $Z(\mathrm{G}_2)$. Ainsi
   $$Z(\mathrm{G}_1\times\mathrm{G}_2)\simeq Z(\mathrm{G}_1)\times Z(\mathrm{G}_2).$$
2. Supposons que G_1 et G_2 sont des groupes simples.
   (a) Montrons que $\mathrm{G}_1\times\mathrm{G}_2$ contient un sous-groupe distingué H_1 isomorphe à G_1 et un sous-groupe distingué H_2 isomorphe à G_2.
   Soit $\mathrm{H}_1=\mathrm{G}_1\times\{e_2\}$ où e_2 est l'élément neutre de G_2. Le groupe H_1 est un sous-groupe de $\mathrm{G}_1\times\mathrm{G}_2$ isomorphe à G_1. De plus H_1 est distingué dans $\mathrm{G}_1\times\mathrm{G}_2$ car pour tout $(x_1,x_2)\in\mathrm{G}_1\times\mathrm{G}_2$, pour tout $(x,e_2)\in\mathrm{H}_1$ nous avons
   $$(x_1,x_2)(x,e_2)(x_1,x_2)^{-1}=(x_1,x_2)(x,e_2)(x_1^{-1},x_2^{-1})=(x_1xx_1^{-1},x_2x_2^{-1})=(x_1xx_1^{-1},e_2)$$
   et $(x_1,x_2)(x,e_2)(x_1,x_2)^{-1}$ appartient à H_1.
   De même $\mathrm{H}_2=\{e_1\}\times\mathrm{G}_2$ est un sous-groupe distingué de $\mathrm{G}_1\times\mathrm{G}_2$.

(b) Montrons que si H est un sous-groupe distingué de $G_1 \times G_2$, alors $H \cap H_1$ est distingué dans H_1 et $H \cap H_2$ est distingué dans H_2.
Soit $(x_1, e_2) \in H_1$ et soit $(x, e_2) \in H \cap H_1$; nous avons

$$(x_1, e_2)(x, e_2)(x_1, e_2)^{-1} = (x_1, e_2)(x, e_2)(x_1^{-1}, e_2) = (x_1 x x_1^{-1}, e_2)$$

donc $(x_1, e_2)(x, e_2)(x_1, e_2)^{-1}$ appartient à H_1. Par ailleurs H est un sous-groupe distingué de $G_1 \times G_2$ donc $(x_1, e_2)(x, e_2)(x_1, e_2)^{-1}$ appartient à H. Finalement $(x_1, e_2)(x, e_2)(x_1, e_2)^{-1}$ appartient à $H \cap H_1$ et $H \cap H_1$ est un sous-groupe distingué de H_1.
De même $H \cap H_2$ est un sous-groupe distingué de H_2.

(c) Les sous-groupes H_1 et H_2 sont isomorphes à G_1 et G_2 respectivement. Les groupes G_1 et G_2 étant simples les groupes H_1 et H_2 sont aussi simples. Il y a donc quatre cas possibles qui sont les suivants :

i) $H \cap H_1 = H_1$ et $H \cap H_2 = H_2$ auquel cas $H = G_1 \times G_2$.

ii) $H \cap H_1 = H_1$ et $H \cap H_2 = \{(e_1, e_2)\}$ auquel cas $H = H_1$.

iii) $H \cap H_1 = \{(e_1, e_2)\}$ et $H \cap H_2 = H_2$ auquel cas $H = H_2$.

iv) $H \cap H_1 = \{(e_1, e_2)\}$ et $H \cap H_2 = \{(e_1, e_2)\}$ auquel cas $H = \{(e_1, e_2)\}$. En effet $^{HH_1}\!/_{H_1}$ (qui est isomorphe à H) est distingué dans $^{G}\!/_{H_1}$, groupe qui est lui-même isomorphe à G_2.
De la même façon nous obtenons que si H n'est pas trivial il est isomorphe à G_1.
Ainsi si H n'est pas trivial, il est isomorphe à G_1 et à G_2 et G_1 et G_2 sont isomorphes : contradiction.
Par conséquent $H = \{(e_1, e_2)\}$.

Ainsi les seuls sous-groupes distingués propres de $G_1 \times G_2$ sont H_1 et H_2.

Exercice 20 Soient G un groupe et H un sous-groupe de G.

(a) Montrer qu'en posant $g \cdot aH = (ga)H$, où a, $g \in G$, on définit une action de G sur l'ensemble $^{G}\!/_{H}$ des classes à gauche modulo H.

(b) Montrer que cette action est transitive.
Déterminer le stabilisateur de aH.

(c) On suppose G fini. Calculer le cardinal d'une orbite et retrouver un théorème classique.

Solution 20

(a) Posons $X = {}^{G}\!/_{H}$. Soient g dans G et x dans X. Désignons par a, a' deux représentants de la classe à gauche x. On a $aH = a'H = x$ ou encore $a^{-1}a' \in H$. Or

$$(ga)^{-1} ga' = a^{-1} g^{-1} ga' = a^{-1} a' \in H$$

donc $gaH = ga'H$.
Si on remplace a par un autre représentant a' de la classe $x = aH$, alors $ga'H = gaH$. La formule a donc bien un sens et définit une application de $G \times X \to X$.
C'est bien une action de G sur X puisque

- $\forall\, x = aH \in X$ nous avons $e \cdot x = eaH = aH = x$,
- $\forall\, x = aH \in X$, $\forall\, g \in G$, $\forall\, g' \in G$ nous avons

$$g \cdot (g' \cdot x) = g \cdot (g'aH) = g(g'a)H = (gg')aH = gg' \cdot x$$

(b) Pour tous $x = aH \in X$ et $y = bH \in X$ il existe $g \in G$ tel que $g \cdot x = y$ (prendre $g = ba^{-1}$). Il existe donc une seule orbite, égale à X.
Le stabilisateur de $x = aH$ est aHa^{-1} car :

$$g \in G_x \iff gaH = aH \iff a^{-1}gaH = H \iff a^{-1}ga \in H \iff g \in aHa^{-1}.$$

(c) Comme $G_x = aHa^{-1} = \mathrm{Ad}_a(H) \simeq H$, on retrouve le théorème de Lagrange

$$[G : H] = \mathrm{card}\left({}^{G}\!/_{H}\right) = \mathrm{card}(\mathrm{orb}(x)) = \frac{[G : 1]}{[G_x : 1]} = \frac{[G : 1]}{[H : 1]}.$$

Exercice 21 Soient p un nombre premier et $a > 1$. En utilisant une action de groupe que l'on précisera montrer que tout groupe G d'ordre p^a admet un élément central (*i.e.* qui commute avec tout élément de G) d'ordre p.

Solution 21 Faisons agir G sur lui-même par conjugaison. Les orbites sont ou bien de cardinal 1 (pour chaque élément du centre), ou bien de cardinal une puissance de p non égale à 1. En écrivant G comme une union d'orbites on a donc $|Z(\mathrm{G})| \equiv 0 \bmod p$, ce qui interdit à $Z(\mathrm{G})$ d'être trivial. Soit $g \in Z(\mathrm{G}) \smallsetminus \{1\}$, alors g est d'ordre p^b pour un certain $1 \leqslant b \leqslant a$. Alors $g^{p^{b-1}}$ appartient à $Z(\mathrm{G})$ et est d'ordre p.

Exercice 22 Soit G un groupe. Soient H et K deux sous-groupes de G tels que $\mathrm{K} \subset \mathrm{H} \subset \mathrm{G}$.

a) Supposons que G soit fini. Montrer que

$$|\mathrm{G} : \mathrm{K}| = |\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}| .$$

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

$$|\mathrm{G} : \mathrm{K}| = |\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}| .$$

Solution 22

a) Comme G est fini, on a

$$|\mathrm{G}| = |\mathrm{G} : \mathrm{H}|\,|\mathrm{H}| \qquad |\mathrm{H}| = |\mathrm{H} : \mathrm{K}|\,|\mathrm{K}| \qquad |\mathrm{G}| = |\mathrm{G} : \mathrm{K}|\,|\mathrm{K}|$$

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

$$|\mathrm{G} : \mathrm{K}| = \frac{|\mathrm{G}|}{|\mathrm{K}|} = \frac{|\mathrm{G} : \mathrm{H}|\,|\mathrm{H}|}{|\mathrm{K}|} = |\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}| .$$

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

$$|\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}| = |\mathrm{G} : \mathrm{K}| .$$

Exercice 23 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 $\langle \mathrm{H} \cup \mathrm{K} \rangle = \mathrm{HK}$.

Solution 23

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

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

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 $\{\mathrm{id}\}$ 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,
— le 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 $\mathrm{G} = \mathrm{GL}(2, \mathbb{Q})$, $g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. L'élément g est d'ordre 2, l'élément h est d'ordre 3 mais $gh = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 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 24 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.

Solution 24

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 $C(S) \lhd N(S)$.

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 $g \in \mathrm{G}$ nous avons $g^{-1}Sg \subset S$ donc en multipliant par g et g^{-1} à gauche et à droite respectivement nous avons $S \subset gSg^{-1} \subset S$ 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. Nous avons

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

puisque H est distingué dans G nous savons 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 nous avons $k\mathrm{H}k^{-1} = \mathrm{H}$ 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 25 Soit G un groupe. Désignons par Aut(G) le groupe des automorphismes de G. Si a appartient à G, notons $\varphi(a)$ l'application

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

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

b) Montrer que $\varphi\colon \mathrm{G} \to \mathrm{Aut}(G)$, $g \mapsto \varphi(g)$ 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 $Z(\mathrm{G})$ le centre de G. Montrer que $\mathrm{Int}(\mathrm{G}) \simeq {}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$.

Solution 25

a) Il faut montrer que $\varphi(a)$ est un homomorphisme de G dans G ; bien sûr $\varphi(a)(e) = e$. Il reste donc à montrer 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 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 φ est un homomorphisme de groupes de G dans Aut(G).

c) Int(G) est l'image de G par l'homomorphisme de groupes φ ; c'est donc un sous-groupe de Aut(G).
Soit τ 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 $\mathrm{Im}\,\varphi$. 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 $\mathrm{Im}\,\varphi = \mathrm{Int}(\mathrm{G})$. Le théorème d'isomorphisme assure que $\mathrm{Int}(\mathrm{G}) \simeq {}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$.

Exercice 26 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

$$\mathrm{G}/\mathrm{H}\,/\,\mathrm{K}/\mathrm{H} \simeq \mathrm{G}/\mathrm{K}$$

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

iii) Montrer que H est distingué dans HK.

iv) Montrer que

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

Solution 26 Soit G un groupe et soit $H \triangleleft \mathrm{G}$ un sous-groupe distingué.

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

b) Soit K un sous-groupe de G.

i) Supposons que K soit distingué dans G et que K contienne H. Montrons que

$$\mathrm{G}/\mathrm{H}\,/\,\mathrm{K}/\mathrm{H} \simeq \mathrm{G}/\mathrm{K}$$

Le morphisme $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{H}$ composé avec la projection $\pi'\colon \mathrm{G}/\mathrm{H} \to (\mathrm{G}/\mathrm{H})/(\mathrm{K}/\mathrm{H})$ induit un morphisme surjectif $q\colon \mathrm{G} \to (\mathrm{G}/\mathrm{H})/(\mathrm{K}/\mathrm{H})$. 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 $(\mathrm{G}/\mathrm{H})/(\mathrm{K}/\mathrm{H})$.

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 27 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 $|\mathrm{H}||\mathrm{K}|$.

Solution 27 Montrons tout d'abord que HK est un sous-groupe de G. On définit l'application φ par

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

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 $\mathrm{H}\cap K = \{e\}$. 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 $hk = k_1 h$. Comme H est distingué il existe h_1 dans H tel que $k_1 h = h_1 k_1$. Ainsi $hk = h_1 k_1$. Mais φ 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 $g \in \mathrm{HK}$, alors $g^{-1} \in \mathrm{H}K$;
— φ est un homomorphisme.

En particulier φ est un isomorphisme de groupes.

Montrons que HK est distingué dans G. Soient $g \in \mathrm{G}$, $h \in \mathrm{H}$ et $k \in \mathrm{K}$. 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 φ est un isomorphisme de groupes l'ordre de HK est celui de $\mathrm{H} \times \mathrm{K}$, *i.e.* |H||K|.

Exercice 28 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.

Solution 28

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 $g \in \mathrm{G}$ et soit $c \in Z(\mathrm{G})$. Comme c commute avec tous les éléments de G nous avons

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

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

b) Si $\mathrm{G} = Z(\mathrm{G})$, alors G est abélien. Si $\mathrm{G} \neq Z(\mathrm{G})$ et si $\mathrm{G}/Z(\mathrm{G})$ est monogène non trivial, alors il existe un élément x de G tel que $x \notin Z(\mathrm{G})$ 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.* $x \in Z(\mathrm{G})$: contradiction. Ainsi $\mathrm{G} = Z(\mathrm{G})$ et G est abélien.

Exercice 29 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 D_8 ?

Solution 29

1. On vérifie que

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

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 D_8 compte 5 éléments d'ordre 2 donc n'est pas isomorphe à $\mathbb{H}_8$ qui n'en compte qu'un.

Exercice 30 Soit Q_8 le groupe des matrices 2×2 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 $\mathbb{Z}/2\mathbb{Z}$?

Solution 30 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 31 Soit G un groupe d'ordre 55 possédant deux sous-groupes distingués d'ordre 5 et 11 respectivement. Montrer que G est isomorphe à $\mathbb{Z}/55\mathbb{Z}$.

Solution 31 Si H et K sont d'ordre respectif 5 et 11, alors $\mathrm{H}\cap\mathrm{K} = \{e\}$ (en effet tous les éléments de $\mathrm{H}\smallsetminus\{e\}$ sont d'ordre 5 et tous les éléments de $\mathrm{K}\smallsetminus\{e\}$ sont d'ordre 11.

L'exercice assure que HK est un sous-groupe de G d'ordre $5\times 11 = 55$ qui est l'ordre de G. Il en résulte que $\mathrm{G} = \mathrm{HK}$. Alors HK est isomorphe à $\mathrm{H}\times\mathrm{K}$. Par suite G est isomorphe à $\mathrm{H}\times\mathrm{K}$. Or H est isomorphe à $\mathbb{Z}/5\mathbb{Z}$ et K est isomorphe à $\mathbb{Z}/11\mathbb{Z}$ donc G est isomorphe à $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/11\mathbb{Z} = \mathbb{Z}/55\mathbb{Z}$ (théorème chinois).