Feuille d'exercices 3

Morphismes et quotients

Exercice 1. Soient $\varphi\colon G \to H$ et $\psi\colon H \to K$ deux morphismes de groupes. Alors la composition $\psi \circ \varphi\colon G \to K$ est encore un morphisme.

Exercice 2. Montrer qu'un morphisme injectif $\varphi\colon G \to H$ est la même chose qu'un isomorphisme entre G et un sous-groupe de H.

Un tel morphisme met en évidence une copie isomorphe de G dans H : on dit qu'il *plonge* G dans H. Ainsi, un morphisme injectif s'appelle aussi un *plongement*.

Exercice 3. Soit $\pi\colon G \to H$ un morphisme surjectif et soit $S \subseteq G$ tel que $\langle S\rangle = G$. Montrer que $\langle \pi(S)\rangle = H$.

Exercice 4. Montrer que :

(a) $Z(G) \trianglelefteq G$.

(b) Plus généralement, si $H \leq Z(G)$ alors $H \trianglelefteq G$.

Exercice 5. Soit G un groupe. Alors tout sous-groupe d'indice 2 de G est distingué.

Exercice 6. Soit G un groupe et $H \leq G$ un sous-groupe. On suppose que H est d'ordre n, et que c'est l'unique sous-groupe de G d'ordre n. Montrer que H est distingué dans G.

Exercice 7. Soient K et H deux sous-groupes distingués de G, et supposons que $K \cap H = \{e\}$. Montrer que $kh = hk$ pour tout $k \in K$ et $h \in H$.

(Est-ce la même chose que dire que $KH = KH$?)

Exercice 8. Montrer que $K \trianglelefteq H \trianglelefteq G$ n'implique pas nécessairement $H \trianglelefteq G$.
Indication : penser au groupe diédral D_8 et à ses sous-groupes.

Exercice 9 (Le groupe quaternionique)**.** Dans $G = \mathrm{GL}(2, \mathbf{C})$, posons :

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

Pour ne pas confondre avec I, notons aussi la matrice identité I_2 par 1.

(a) Calculer leurs carrés, ainsi que les produits IJ, JK, KI.

(b) En déduire les produit JI, KJ, IK.

(c) Déduire que

$$\langle I, J\rangle = \{\pm 1, \pm I \pm J, \pm K\}.$$

Ce groupe s'appelle le *groupe quaternionique*, noté parfois Q_8.

(d) Dresser la liste des sous-groupes de Q_8. Pour chacun, déterminer s'il est distingué ou non.

Exercice 10. Soit $(G, +)$ un groupe abélien.

(a) Montrer que l'application $\pi\colon G \times G \to G$, définie par $\pi(x, y) = x + y$ est un morphisme de groupes.

(b) Dans le cas $G = \mathbf{R}$, décrire les fibres de π géométriquement.

Exercice 11. Soit F un corps.

(a) Considérons le groupe $G \leq \mathrm{GL}(2,F)$ défini par

$$G = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a,b,c \in F, ac \neq 0\}.$$

Démontrer que l'application $\phi \colon G \to F^\times$ définie par

$$\phi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}) = a$$

est un morphisme surjectif. Calculer son noyau.

(b) Soit $G \leq \mathrm{GL}(2,F)$ défini par

$$G = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in F\}.$$

Montrer que G est isomorphe au groupe additif de F.

Exercice 12. Montrer que si G est abélien alors tout sous-groupe de G est distingué.

Donner un exemple d'un groupe non-abélien dont tous les sous-groupes sont distingués.

Exercice 13. Soit $G = \mathrm{GL}(2,\mathbf{Q})$ et soient

$$H = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbf{Z}\}, \quad g = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

Montrer que $gHg^{-1} \subseteq H$ mais que g ne normalise pas H.

Exercice 14. Trouver tous les sous-groupes distingués de D_8 et le type d'isomorphisme du quotient de D_8 par chacun d'entre eux.

Exercice 15. Soit F un corps. Montrer que $\mathrm{SL}(n,F) \trianglelefteq \mathrm{GL}(n,F)$ et calculer le type d'isomorphisme du quotient.

Exercice 16. Soit G un groupe. Montrer que si $G/Z(G)$ est cyclique, alors G est abélien.

Exercice 17. Montrer que $(\mathbf{Q},+)$ n'a pas de sous-groupes propres d'indice fini.

Exercice 18 (Théorème de Cauchy)**.** Le but de cet exercice est de démontrer le théorème suivant : si G est un groupe fini et p est un nombre premier qui divise $|G|$, alors G a un élément d'ordre p.
Soit

$$S = \{(x_1,\dots,x_p) \in G^p : x_1 x_2 \cdots x_p = 1\}.$$

(a) Montrer que $|S| = |G|^{p-1}$ et qu'en particulier p divise $|S|$.

(b) Soit $\sim$ la relation sur S définie par $\alpha \sim \beta$ ssi α est une permutation cyclique de β. Montrer qu'une permutation cyclique d'un élément de S est aussi un élément de S.

(c) Montrer que $\sim$ est une relation d'équivalence.

(d) Montrer qu'une classe d'équivalence contient un seul élément ssi elle est de la forme $\{(x,\dots,x)\}$ où $x^p = 1$.

(e) Montrer que toute classe d'équivalence est de cardinal 1 ou p. En déduire que $|G|^{p-1} = k + pd$ où d est le nombre de classes de cardinal p et k est le nombre de classes de cardinal 1.

(f) Observer que $\{(1,\dots,1)\}$ est une classe de cardinal 1 et en déduire qu'il y en a au moins une autre.
(g) Conclure.

Exercice 19. Montrer que S_4 n'a pas de sous-groupe isomorphe à Q_8.

Exercice 20. Soit G un groupe. Soit $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G, muni de la loi de composition d'applications. Alors $\mathrm{Aut}(G)$ est un groupe, nommé le *groupe d'automorphismes* de G.

On pourrait le montrer ou bien directement, ou bien en montrant que $\mathrm{Aut}(G) \leq S_G$.

Exercice 21. Soit G un groupe et $x, y \in G$. On appelle xyx^{-1} le *conjugué* de y par x. Pour $x \in G$ fixé, définissons $\varphi_x \colon G \to G$ par

$$\varphi_x(y) = xyx^{-1}.$$

Cette application est la *conjugaison par* x.

(a) Montrer que pour tout $x \in G$, l'application $\varphi_x \colon G \to G$ est un morphisme.
(b) Montrer que pour tout $x, y \in G$, on a $\varphi_x \circ \varphi_y = \varphi_{xy}$.
(c) Montrer que $\varphi_e = \mathrm{id}_G$.
(d) En déduire que $\varphi_x \in \mathrm{Aut}(G)$ pour tout $x \in G$.

Exercice 22. Soit G un groupe, $N \leq G$. Soient $S \subseteq G$, $T \subseteq N$ tels que $G = \langle S \rangle$, $N = \langle T \rangle$.
(a) Montrer que si pour tout $s \in S$, $sTs^{-1} \subseteq N$ et $s^{-1}Ts \subseteq N$, alors $N \trianglelefteq G$.
(b) Si N est fini il suffit de demander que $sTs^{-1} \subseteq N$ pour tout $s \in S$.

Exercice 23. Grâce à l'Exercice 21, on peut définir une application

$$\Phi \colon G \to \mathrm{Aut}(G), \qquad \Phi(x) = \varphi_x.$$

(a) Montrer que Φ est un morphisme de groupes.
(b) Montrer que $\ker \Phi = Z(G)$.
(c) Soit $\psi \in \mathrm{Aut}(G)$ et $x \in G$. Montrer que $\psi \circ \varphi_x \circ \psi^{-1} = \varphi_{\psi(x)}$. En déduire que

$$\mathrm{img}\,\Phi \trianglelefteq \mathrm{Aut}(G).$$

Remarque. Un automorphisme de G qui peut s'écrire sous la forme φ_x s'appelle un automorphisme *intérieur*. L'ensemble des automorphismes intérieurs est notée $\mathrm{Inn}(G)$:

$$\mathrm{Inn}(G) = \{\varphi_x : x \in G\} = \mathrm{img}\,\Phi.$$

Nous avons montré que $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. Le groupe quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ est noté $\mathrm{Out}(G)$, et ses membres s'appellent des automorphismes *extérieurs* (bien que ce ne soient pas des automorphismes).

Exercice 24. Continuant l'Exercice 23, montrer que G est abélien si et seulement si Φ est le morphisme trivial.

Exercice 25. Soit G un groupe fini tel que $x^2 = e$ pour tout $x \in G$.
(a) Rappeler pourquoi G est abélien.
(b) Montrer que $|G|$, l'ordre de G, est une puissance de 2.
Indication : pour $x \in G \setminus \{e\}$, considérer le quotient $G/\langle x \rangle$.

Exercice 26. Soit G un groupe et $x, y \in G$. On appelle

$$[x, y] = xyx^{-1}y^{-1}$$

le *commutateur* de x et y.

Montrer que $[x, y] = e$ si et seulement si $xy = yx$ (d'où son nom).

Exercice 27. Soit G un groupe. Le sous-groupe engendré par tous les commutateurs, noté G', s'appelle le *groupe dérivé* de G :

$$G' = \langle [x, y] : x, y \in G \rangle.$$

(a) Montrer que $G' \trianglelefteq G$.

(b) Montrer que G/G' est abélien.

(c) Montrer que si H est un groupe abélien quelconque et $\varphi\colon G \to H$ un morphisme, alors $G' \leq \ker\varphi$ et il existe un unique morphisme $\psi\colon G/G' \to H$ tel que $\psi \circ \pi_{G'} = \varphi$. Autrement dit, il existe un unique ψ qui rend le diagramme suivant commutatif :

$$\begin{tikzcd} G \arrow[r, "\pi_{G'}"] \arrow[dr, "\varphi"'] & G/G' \arrow[d, dashed, "\psi"] \\ & H \end{tikzcd}$$

Exercice 28. Nous proposons de calculer le groupe $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}, +)$, pour $n \geq 2$. Pour cela, nous allons utiliser la structure d'anneau $(\mathbf{Z}/n\mathbf{Z}, +, \cdot)$. Un membre de $\mathbf{Z}/n\mathbf{Z}$ sera noté $\overline{k} = k + n\mathbf{Z}$, avec $k \in \mathbf{Z}$. Nous avons déjà (ou nous le montrerons en amont) que $\mathbf{Z}/n\mathbf{Z}$ admet deux opérations, $+$ et $\cdot$, définies par

$$\overline{k} + \overline{\ell} = \overline{k + \ell}, \qquad \overline{k} \cdot \overline{\ell} = \overline{k \cdot \ell}.$$

En particulier, ces deux opération sont bien définies, et $+$ est simplement la loi du groupe quotient $\mathbf{Z}/n\mathbf{Z}$ (pour la multiplication, voir l'**??**).

(a) Montrer que la multiplication sur $\mathbf{Z}/n\mathbf{Z}$ est associative, avec neutre $\overline{1}$.

(b) Un élément $x \in \mathbf{Z}/n\mathbf{Z}$ est dit *inversible* s'il existe $y \in \mathbf{Z}/n\mathbf{Z}$ tel que $xy = yx = \overline{1}$. L'ensemble des membres inversibles de $\mathbf{Z}/n\mathbf{Z}$ sera noté $(\mathbf{Z}/n\mathbf{Z})^\times$. Montrer que $\big((\mathbf{Z}/n\mathbf{Z})^\times, \cdot\big)$ est un groupe.

(c) Soit $\varphi \in \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$, et posons $\widehat{\varphi} = \varphi(\overline{1}) \in \mathbf{Z}/n\mathbf{Z}$. Montrer que $\varphi(x) = x\widehat{\varphi}$ tout $x \in \mathbf{Z}/n\mathbf{Z}$.

(d) Montrer que si $\varphi, \psi \in \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$, alors $\widehat{\varphi \circ \psi} = \widehat{\varphi}\widehat{\psi}$, et que $\widehat{\mathrm{id}} = \overline{1}$.

(e) En déduire que pour tout $\varphi \in \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}, +)$, $\widehat{\varphi}$ est inversible, et que l'application $\varphi \mapsto \widehat{\varphi}$ est un morphisme $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}, +) \to \big((\mathbf{Z}/n\mathbf{Z})^\times, \cdot\big)$.

(f) Montrer que c'est un isomorphisme, d'où notre conclusion :

$$\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}, +) \cong \big((\mathbf{Z}/n\mathbf{Z})^\times, \cdot\big).$$

Exercice 29. Utilisant les mêmes idée que dans Exercice 28, montrer que $\mathrm{Aut}(\mathbf{Z}, +) \cong (\mathbf{Z}^\times, \cdot) = \big(\{\pm 1\}, \cdot\big)$.