ENS Paris-Saclay 2025-2026
A. Bailleul

Préparation à l'agrégation
Cours-TD de théorie des groupes

Groupes, sous-groupes, quotients et morphismes

Quelques références bibliographiques pour la théorie des groupes :

- *Cours d'algèbre*, D. Perrin, Ellipses.
- *Algèbre - Le grand combat*, G. Berhuy, Calvage & Mounet.
- *Groupes finis et treillis de leurs sous-groupes*, A. Debreil, Calvage & Mounet.
- *Théorie des groupes*, F. Ulmer, Ellipses.
- *Théorie des groupes*, J. Delcourt, Ellipses.
- *An introduction to the theory of groups*, J. Rotman, Springer.

1 Généralités sur les groupes

Les groupes sont des structures mathématiques que l'on retrouve partout (algèbre commutative, algèbre linéaire, géométrie, topologie, théorie des nombres, combinatoire, etc.). La notion fut dégagée suite notamment aux travaux de Galois sur la résolution des équations algébriques par radicaux.

Définition 1.1. *Un* ***groupe*** *est un couple $(G, *)$ où G est un ensemble et :*

1. *$* : G \times G \to G$ est une loi de composition interne* ***associative*** *: $\forall x, y, z \in G, (x * y) * z = x * (y * z)$.*
2. *Il existe un élément* ***neutre*** *$e \in G$: $\forall x \in G, x * e = e * x = x$.*
3. *Tout élément admet un* ***inverse*** *: $\forall x \in G, \exists y \in G, x * y = y * x = e$. L'inverse de x est en général noté x^{-1}.*

Le groupe $(G, *)$ est dit ***abélien*** *(ou* ***commutatif****) lorsque la loi $*$ est commutative : $\forall x, y \in G, x * y = y * x$.*

Remarque 1.2.

1. Quand le groupe est abélien, on note traditionnellement sa loi $+$, son neutre 0 et l'inverse de x est noté $-x$. On omet souvent la loi $*$ quand le contexte est clair et on parle abusivement de G comme étant un groupe.

2. En l'absence d'inverses, on parle de **monoïde**, et en l'absence de neutre ou d'associativité on parle de **magma**.

Exemple 1.3.

1. $(\mathbb{Z}, -)$ est un magma qui n'est pas un monoïde, $(\mathbb{N}, +)$ est un monoïde qui n'est pas un groupe, $(\mathbb{Z}, +)$ est un groupe.

2. Pour $n \geq 1$ entier, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes de congruence modulo n muni de l'addition modulaire est un groupe de neutre $\overline{0}$.

3. Si E est un ensemble alors l'ensemble E^E des fonctions de E dans E est un monoïde muni de la composition qui n'est en général pas un groupe. L'ensemble $\mathrm{Bij}(E)$ des bijections de E dans E est un groupe pour la composition, noté $\mathfrak{S}(E)$, de neutre id_E, et appelé **groupe des permutations** de E.

4. Si A est un anneau, $(A, +)$ est un groupe de neutre 0 et $(A, \times)$ est un monoïde qui n'est pas un groupe. Cependant $(A^\times, \times)$ est un groupe de neutre 1.

Exercice 1. *Montrer que le neutre et l'inverse d'un élément sont uniques.*

2 Sous-groupes

Définition 2.1. *Soit $(G, *)$ un groupe. Une partie $H \subset G$ est un **sous-groupe** de G lorsque $(H, *_{H\times H})$ est un groupe. Il est équivalent d'avoir :*

1. $H \neq \emptyset$.
2. $\forall x, y \in H, x * y \in H$.
3. $\forall x \in H, x^{-1} \in H$.

Exemple 2.2.

1. $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.
2. Si E est un espace vectoriel alors $\mathrm{GL}(E)$ est un sous-groupe de $\mathfrak{S}(E)$.

Exercice 2. *Montrer que H est un sous-groupe de G si et seulement si $H \neq \emptyset$ et $\forall x, y \in H, x * y^{-1} \in H$.*

Exercice 3. *Montrer que les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{Z}$.*

Proposition 2.3. *Soit G un groupe et $\{H_i \mid i \in I\}$ un ensemble de sous-groupes de G. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.*

Définition 2.4. *Soit G un groupe et $S \subset G$ une partie de G. Le **sous-groupe engendré** par S est*

$$\langle S \rangle = \bigcap_{\substack{H \text{ sous-groupe de } G \\ S \subset H}} H.$$

C'est le plus petit (au sens de l'inclusion) sous-groupe de G contenant S.

Exercice 4. *Montrer que*

$$\langle S\rangle = \{s_1^{\varepsilon_1}\dots s_n^{\varepsilon_n} \mid n\in\mathbb{N}, s_1,\dots,s_n\in S, \varepsilon_1,\dots,\varepsilon_n\in\{-1,1\}\}.$$

Définition 2.5. *Un groupe G engendré par un élément est appelé **monogène**. Si de plus il est fini, on dit que G est **cyclique**. Plus généralement si G est engendré par une partie finie on dit qu'il est **de type fini**.*

Définition 2.6. *Soit G un groupe et $g\in G$. S'il existe $n\in\mathbb{N}^*$ tel que $g^n = e$ on dit que g est d'**ordre fini**. Le plus petit entier $n\in\mathbb{N}^*$ tel que $g^n = e$ est appelé l'**ordre** de g.*

Exercice 5. *Montrer que si $g\in G$ est d'ordre fini alors son ordre est égal au cardinal de $\langle g\rangle$.*

3 Morphismes de groupes

Définition 3.1. *Soit $(G,\triangle)$ et $(H,\square)$ des groupes. Un **morphisme de groupes** est une application $f: G\to H$ telle que*

$$\forall x,y\in G, f(x\triangle y) = f(x)\square f(y).$$

*Un **endomorphisme** de G est un morphisme de groupes de G dans G, un **isomorphisme** est un morphisme de groupes bijectif et un **automorphisme** est un endomorphisme bijectif.*

Proposition 3.2. *Soit G, H des groupes et $f: G\to H$ un isomorphisme. Alors $f^{-1}: H\to G$ est un isomorphisme.*

Remarque 3.3. Quand deux groupes G et H sont isomorphes, on note $G\simeq H$, et on fait « comme s'ils étaient les mêmes », c'est-à-dire que toutes les propriétés exprimables en termes de théorie des groupes (abélien, centre trivial, résoluble, etc.) de l'un sont vraies pour l'autre.

Exercice 6. *Montrer qu'un groupe cyclique est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$ pour un unique entier n. Montrer qu'un groupe monogène non cyclique est isomorphe à $(\mathbb{Z},+)$.*

Définition 3.4. *Soit $f: G\to H$ un morphisme de groupes. Le **noyau** de f est*

$$\ker f = \{g\in G \mid f(g) = e_H\}.$$

*L'**image** de f est*

$$\operatorname{im} f = \{h\in H \mid \exists g\in G, f(g) = h\}.$$

Proposition 3.5. *Soit $f: G\to H$ un morphisme de groupes. Alors $\ker f$ est un sous-groupe de G et $\operatorname{im} f$ est un sous-groupe de H. De plus, f est injectif si et seulement si $\ker f = \{e_G\}$ et f est surjectif si et seulement si $\operatorname{im} f = H$.*

Démonstration. On a $f(g) = f(g') \Leftrightarrow f(gg'^{-1}) = e_H$. □

4 Quotient par un sous-groupe

Dans toute cette section, G est un groupe et H un sous-groupe de G.

Définition 4.1. *Les* ***classes à gauche*** *modulo H sont les $gH = \{gh \mid h \in H\} \subset G$ avec $g \in G$. L'****ensemble-quotient*** *G/H est $\{gH \mid g \in G\}$. Quand il est fini, on appelle* ***indice*** *de H dans G, noté $[G : H]$, le cardinal de G/H.*

⚠ Il n'y a pas de structure de groupe naturelle sur G/H en général.

Exercice 7. *Déterminer une bijection entre les classes à gauche et les classes à droite modulo H. En particulier, l'indice $[G : H]$ ne dépend pas de si on considère les classes à gauche ou à droite.*

Proposition 4.2. *Les classes à gauche modulo H forment une partition de G.*

Remarque 4.3. En particulier, on dispose d'une relation d'équivalence sur G correspondant à la partition selon les classes à gauche modulo H, donnée par

$$x \sim y \Leftrightarrow \exists g \in G, x, y \in gH,$$

ou de manière équivalente

$$x \sim y \Leftrightarrow \exists h \in H, y = xh,$$

ou encore

$$x \sim y \Leftrightarrow x^{-1}y \in H.$$

Corollaire 4.4 (Théorème de Lagrange)**.** *Si G est fini alors $|G| = |H|[G : H]$. En particulier, $|H|$ et $[G : H]$ divisent $|G|$ et l'ordre d'un élément de G divise $|G|$.*

Démonstration. On utilise la partition selon les classes à gauche et le fait que $|gH| = |H|$. □

Corollaire 4.5. *Soit p un nombre premier. Si G est fini d'ordre p, alors $G \simeq \mathbb{Z}/p\mathbb{Z}$ est cyclique.*

Exercice 8. *Soit $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$. Déterminer l'ordre de $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$.*

Exercice 9. *Montrer le petit théorème de Fermat à l'aide du théorème de Lagrange.*

Proposition 4.6. *Les propriétés suivantes sont équivalentes :*

1. *Pour tout $g \in G, gHg^{-1} = H$.*
2. *Pour tout $g \in G, gH = Hg$ (i.e. les classes à gauche sont les classes à droite).*
3. *Pour tout $g_1, g_2 \in G$, $g_1Hg_2H = g_1g_2H$.*

Définition 4.7. *Si l'une des conditions ci-dessus est vérifiée, on dit que H est* ***distingué*** *dans G, et on note $H \triangleleft G$.*

Exercice 10. *Montrer que si H est d'indice 2 dans G alors $H \triangleleft G$.*

Exercice 11. *Montrer qu'il suffit de montrer que $\forall g \in G, gHg^{-1} \subset H$ pour obtenir que $H \triangleleft G$.*

Proposition 4.8. *L'image réciproque d'un sous-groupe distingué par un morphisme de groupes est distingué.*

Remarque 4.9.

1. En particulier, le noyau d'un morphisme de groupes est toujours distingué.
   ⚠ L'image d'un morphisme de groupes n'est en général pas distinguée dans le groupe d'arrivée.

2. Si $K \triangleleft H$ et $H \triangleleft G$ on n'a pas forcément $K \triangleleft G$. Contre-exemple à venir dans la feuille suivante.

3. Si G est abélien, tous ses sous-groupes sont distingués.
   ⚠ La réciproque est fausse, voir les exercices.

Définition 4.10. *Un groupe G est dit **simple** lorsqu'il est non trivial et que ses seuls sous-groupes distingués sont $\{e\}$ et G.*

Exercice 12. *Soit p un nombre premier. Montrer que $\mathbb{Z}/p\mathbb{Z}$ est simple. Réciproquement, montrer que si un groupe abélien fini est simple alors il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.*

Remarque 4.11. Les groupes finis simples forment les « briques de base » qui permettent de comprendre la structure des groupes finis, nous expliquerons pourquoi dans les exercices. Leur liste complète est connue seulement depuis les années 80, résultats de décennies et de milliers de pages de recherche.

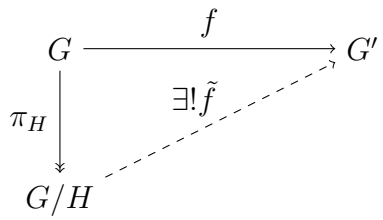
Théorème 4.12. *Si H est distingué dans G, il existe une unique loi de groupe sur G/H telle que la projection canonique $g \mapsto gH$ de G dans G/H soit un morphisme de groupes.*

Démonstration. On pose la loi $(g_1H) * (g_2H) = (g_1g_2)H$, qui est bien définie car $H \triangleleft G$. On a immédiatement que le neutre de cette loi est H, et l'inverse de gH est $g^{-1}H$. □

⚠ Il n'y a aucune raison pour que $G \simeq H \times G/H$ en général, voir les exercices.

Corollaire 4.13. *Soit H un sous-groupe de G. Alors $H \triangleleft G$ si et seulement s'il existe un groupe G' et un morphisme de groupes $f : G \to G'$ tel que $H = \ker f$.*

Théorème 4.14 (Propriété universelle du quotient)**.** *Soit $f : G \to G'$ un morphisme de groupes. Pour qu'il existe un morphisme de groupes $\tilde{f} : G/H \to G'$ tel que $f = \tilde{f} \circ \pi_H$, il faut et il suffit que $H \subset \ker f$. De plus, $\tilde{f}$ est unique. Autrement dit, le diagramme suivant commute :*



Démonstration. La condition est clairement nécessaire car si $f = \tilde{f} \circ \pi_H$ alors f est trivial sur H. Réciproquement, si f est trivial sur H, posons, pour tout $g \in G$,

$$\tilde{f}(gH) = f(g).$$

$\tilde{f}(gH)$ ne dépend pas du représentant g de gH car si $gH = g'H$ alors il existe $h \in H$ tel que $g = g'h$ et alors $f(g) = f(g')f(h) = f(g')$. On vérifie immédiatement que $\tilde{f}$ est bien un morphisme de groupes, d'où le résultat. □

Corollaire 4.15 (Premier théorème d'isomorphisme)**.** *Soit $f : G \to G'$ un morphisme de groupes. Alors*

$$G/\ker f \simeq \operatorname{im} f.$$

Démonstration. On vérifie que le $\tilde{f}$ ci-dessus a la même image que f. De plus, si $\tilde{f}(g \ker f) = e_{G'}$ c'est que $g \in \ker f$ et donc $g \ker f = \ker f$, donc $\tilde{f}$ est injectif. □

Théorème 4.16 (Théorème chinois)**.** *Soit $m, n \geq 1$ des entiers premiers entre eux. Alors*

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Démonstration. Considérons le morphisme de groupes $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ défini par $f(k) = (k \bmod m, k \bmod n)$. Comme m et n sont premiers entre eux, il existe une relation de Bézout $mu + nv = 1$ avec $m, n \in \mathbb{Z}$. Alors $f(um) = (\overline{0}, \overline{1})$ et $f(vn) = (\overline{1}, \overline{0})$. Comme $\{(\overline{1}, \overline{0}), (\overline{0}, \overline{1})\}$ engendre $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, f est surjectif. De plus, le noyau de f est $mn\mathbb{Z}$. En effet, il est clair que $mn\mathbb{Z} \subset \ker f$, et si $f(k) = (\overline{0}, \overline{0})$, c'est que $m \mid k$ et $n \mid k$. En écrivant $k = md$, le lemme de Gauss donne que n divise d, d'où $mn \mid k$. On conclut avec le premier théorème d'isomorphisme. □

Remarque 4.17. On peut aussi directement montrer que $k \bmod mn \mapsto (k \bmod m, k \bmod n)$ est un morphisme de groupes bien défini, injectif comme ci-dessus et conclure par égalité des cardinaux des deux groupes.

5 Produits directs et semi-directs internes

Une question naturelle est la suivante : étant donné un groupe G engendré par deux sous-groupes H et K, peut-on reconstruire la structure de groupe de G à partir de celles de H et K ? La réponse dépend de comment H et K sont « agencés » dans G. On présente ici deux situations abordables à l'agrégation.

Définition 5.1. *Soit $(G_1, *_1)$ et $(G_2, *_2)$ des groupes. Leur **produit direct** (externe) est le groupe d'ensemble sous-jacent $G_1 \times G_2$ et de loi donnée par*

$$(g_1, g_2) * (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2).$$

Remarque 5.2. On vérifie facilement que, si on note $H_1 = G_1 \times \{e_{G_2}\}$ et $H_2 = \{e_{G_1}\} \times G_2$ alors $H_1 \simeq G_1, H_2 \simeq G_2, H_1, H_2 \triangleleft G_1 \times G_2, H_1H_2 = G_1 \times G_2$ et $H_1 = H_2 = e_{G_1 \times G_2}$.

Les conditions ci-dessus caractérisent en fait les produits directs.

Proposition 5.3. *Soit G un groupe, H_1 et H_2 des sous-groupes de G. Supposons que*

1. *$H_1 \triangleleft G, H_2 \triangleleft G$.*
2. *$G = H_1H_2 = \{h_1h_2 \mid h_1 \in H_1, h_2 \in H_2\}$.*
3. *$H_1 \cap H_2 = \{e\}$.*

*Alors G est isomorphe à $H_1 \times H_2$ et on dit que G est **produit direct interne** de H_1 et H_2.*

Démonstration. Il s'agit de vérifier que $g_1 g_2 \mapsto (g_1, g_2)$ est un isomorphisme de groupes bien défini. Le point-clé est que les éléments de H_1 et de H_2 commutent entre eux car $h_1 h_2 h_1^{-1} h_2^{-1}$ est simultanément dans H_1 et H_2, donc trivial. □

Considérons maintenant la situation suivante : on dispose d'un groupe G et de deux sous-groupes H et K de G tels que $G = HK$. Peut-on retrouver la structure de groupe de G à l'aide de cette information ?

Si $g_1 = h_1 k_1$ et $g_2 = h_2 k_2$ avec $h_1, h_2 \in H$ et $k_1, k_2 \in K$, alors on a

$$g_1 g_2 = h_1 k_1 h_2 k_2 \stackrel{?}{=} h_3 k_3.$$

Il n'y a *a priori* aucune manière de retrouver h_3 et k_3. Cependant, si (par exemple) $H \triangleleft G$, alors on peut écrire

$$h_1 k_1 h_2 k_2 = h_1 (k_1 h_1 k_1^{-1}) k_1 k_2$$

ce qui permet de voir que $h_3 = h_1 (k_1 h_1 k_1^{-1}) \in H$ et $k_3 = k_1 k_2 \in K$ conviennent.

L'unicité d'une telle écriture est équivalente à $H \cap K = \{e\}$ car $h_1 k_1 = h_2 k_2 \Leftrightarrow h_2^{-1} h_1 = k_2 k_1^{-1}$.

Définition 5.4. *On dit que G est **produit semi-direct interne** de H et K, et on note $G = H \rtimes K$, lorsque :*

1. *$G = HK$.*
2. *$H \cap K = \{e\}$.*
3. *$H \triangleleft G$.*

On a vu plus haut que lorsque de plus $K \triangleleft G$ alors $G \simeq H \times K$ et donc les notions de produits direct interne et externe coïncident. Dans l'Exercice 32 on fait le lien entre le produit semi-direct interne et la structure de produit semi-direct externe $H \rtimes_\varphi K$, qui dépend d'un morphisme de groupes $\varphi : K \to \mathrm{Aut}(H)$.

6 Groupes et sous-groupes remarquables

Dans toute cette section, G est un groupe.

Définition 6.1. *Le **centre** de G est*

$$Z(G) = \{g \in G \mid \forall h \in G, gh = hg\}.$$

Proposition 6.2. *On a $Z(G) \triangleleft G$. Le groupe G est abélien si et seulement si $Z(G) = G$.*

Définition 6.3. *Si $x, y \in G$, leur **commutateur** est*

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

*Le **sous-groupe dérivé** de G est*

$$D(G) = \langle \{[x, y] \mid x, y \in G\} \rangle.$$

⚠ $D(G)$ n'est en général pas égal à l'ensemble $\{[x, y] \mid x, y \in G\}$ des commutateurs de G car ce dernier n'est pas toujours un sous-groupe de G.

Proposition 6.4. *On a $D(G) \triangleleft G$. Le groupe G est abélien si et seulement si $D(G) = \{e\}$.*

Proposition 6.5. *L'ensemble des automorphismes de groupes de G, noté $\mathrm{Aut}(G)$, est un groupe pour la composition.*

Exercice 13. *Déterminer $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ pour $n \in \mathbb{N}^*$.*

7 Exercices

Exercice 14. *Soit $(G, *)$ un groupe. Le **groupe opposé** est $(G, \bullet)$ où la loi $\bullet$ est définie par*

$$x \bullet y = y * x.$$

Montrer que $(G, \bullet)$ est un groupe isomorphe à $(G, *)$.

Exercice 15. *Soit G un groupe tel que $\forall g \in G, g^2 = e$. Montrer que G est abélien. Montrer la même conclusion en supposant que $g \mapsto g^{-1}$ est un endomorphisme de G.*

Exercice 16. *Soit G un groupe et H un sous-groupe strict de G. Montrer que $\langle G \setminus H \rangle = G$.*

Exercice 17. *Soit G un groupe, $x, y \in G$ qui commutent entre eux et d'ordres respectifs m et n premiers entre eux. Montrer que xy est d'ordre mn.*

Exercice 18. *Soit G un groupe abélien fini. Exprimer*

$$\prod_{g \in G} g.$$

*En déduire le **théorème de Wilson** : Si p est un nombre premier alors*

$$(p-1)! \equiv -1 \mod p.$$

(On pourra admettre que $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$ est un groupe pour la multiplication.)

Exercice 19. *Déterminer les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ pour $n \in \mathbb{N}^*$.*

Exercice 20. *Soit $m, n \in \mathbb{N}^*$. Déterminer tous les morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.*

Exercice 21. *Déterminer* $\mathrm{Aut}(\mathbb{Z})$.

Exercice 22. *Soit G un sous-groupe de $(\mathbb{R}, +)$. Montrer que G est monogène ou dense dans $\mathbb{R}$. Indication : Considérer* $\inf G \cap \mathbb{R}^{+*}$.

Exercice 23. *Justifier si les paires de groupes suivantes sont isomorphes :*

1. $\mathbb{Z}/n\mathbb{Z}$ *et* $\mathbb{Z}/m\mathbb{Z}$ *avec* $m \neq n$.
2. $((\mathbb{Z}/2\mathbb{Z})^2, +)$ *et* $(\mathbb{Z}/4\mathbb{Z}, +)$.
3. $(\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z}, +)$ *et* $(\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}, +)$.
4. $(\mathbb{R}, +)$ *et* $(\mathbb{R}^{+*}, \times)$.
5. $(\mathbb{Q}, +)$ *et* $(\mathbb{Q}^{+*}, \times)$.
6. $(\mathbb{Q}, +)$ *et* $(\mathbb{R}, +)$.
7. $(\mathbb{Z}[X], +)$ *et* $(\mathbb{Q}^{+*}, \times)$.
8. $(\mathbb{R}, +)$ *et* $(\mathbb{C}, +)$. *(Bonus)*

Exercice 24. 1. *Montrer que si G et G' sont des groupes, $f : G \to G'$ est un morphisme de groupes et $H \triangleleft G$ alors $f(H)$ n'est pas forcément distingué dans G'.*

2. *Montrer que si f est surjectif alors $f(H) \triangleleft G'$.*
Remarque. *En général, $f(H)$ est distingué dans $f(G)$.*

Exercice 25. 1. *Soit G un groupe, H et K des sous-groupes de G avec $H \triangleleft G$.*

(a) *Montrer que le sous-groupe engendré par K et H est égal à KH.*

(b) *Montrer que $K \cap H \triangleleft K$ et*

$$K/(K \cap H) \simeq KH/H. \quad (\textit{Second théorème d'isomorphisme})$$

2. *Soit G un groupe, H et K des sous-groupes distingués de G avec $K \subset H$. Montrer que*

$$(G/K)/(H/K) \simeq G/H. \quad (\textit{Troisième théorème d'isomorphisme})$$

Exercice 26. *Soit G un groupe. Montrer que $G/D(G)$ est le plus grand quotient abélien de G, au sens où si $H \triangleleft G$ alors G/H est abélien si et seulement si $D(G) \subset H$, et dans ce cas on a un morphisme surjectif*

$$G/D(G) \twoheadrightarrow G/H.$$

Exercice 27. *Notons l'ensemble $\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}$ à 8 éléments muni de la loi vérifiant :*

- *1 est neutre.*
- *$i^2 = j^2 = k^2 = -1$ commute avec tous les éléments de $\mathbb{H}_8$.*
- *$ij = -ji = k, jk = -kj = i, ki = -ik = j$.*

On admettra (c'est l'associativité qui est fatigante) qu'il s'agit d'une loi de groupe sur $\mathbb{H}_8$.

1. *Déterminer $Z(\mathbb{H}_8)$ et $D(\mathbb{H}_8)$.*
2. *Montrer que tous les sous-groupes de $\mathbb{H}_8$ sont distingués. $\mathbb{H}_8$ est-il abélien ?*
3. *Montrer que $\mathbb{H}_8 \not\simeq D(\mathbb{H}_8) \times \mathbb{H}_8/D(\mathbb{H}_8)$.*
4. *Montrer que $\mathbb{H}_8$ ne peut s'écrire comme un produit direct de groupes simples.*

Exercice 28. *Soit G un groupe abélien et p un nombre premier tel que pour tout $g \in G, g^p = e$. Montrer que l'on peut munir G d'une structure de $\mathbb{F}_p$-espace vectoriel. Si G est fini, quel peut être la forme de son cardinal ?*

Exercice 29. *Soit G un groupe.*

1. *Pour tout $g \in G$, on note $\mathrm{Int}(g) : x \mapsto gxg^{-1}$. Montrer que $\mathrm{Int}(g) \in \mathrm{Aut}(G)$.*
2. *On note $\mathrm{Int}(G) = \{\mathrm{Int}(g) \mid g \in G\}$. Montrer que $\mathrm{Int}(G)$ est un sous-groupe distingué dans $\mathrm{Aut}(G)$.*
3. *Montrer que $\mathrm{Int}(G) \simeq G/Z(G)$.*
4. *On appelle **sous-groupe caractéristique** de G tout sous-groupe H tel que $\forall \varphi \in \mathrm{Aut}(G), \varphi(H) = H$. Montrer qu'un sous-groupe caractéristique est distingué.*
5. *Montrer que $Z(G)$ et $D(G)$ sont caractéristiques dans G.*

6. *Donner un exemple de sous-groupe distingué qui n'est pas caractéristique.*

Exercice 30. *Montrer que $\mathbb{Q}$ n'est pas de type fini, c'est-à-dire qu'il n'existe pas de partie finie $S \subset \mathbb{Q}$ telle que $\mathbb{Q} = \langle S \rangle$.*

Exercice 31. *Soit G un groupe et $H \triangleleft G$. Montrer que les sous-groupes de G/H correspondent bijectivement aux sous-groupes K de G tels que $H \subset K$, et de même pour les sous-groupes distingués. En déduire que tout groupe fini G admet une **décomposition de Jordan-Hölder** : une suite de sous-groupes $\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$ avec $G_{i+1} \triangleleft G_i$ et G_i/G_{i+1} simple.*
Remarque. *C'est cette décomposition de Jordan-Hölder qui justifie l'importance de la connaissance des groupes finis simples. On peut « dévisser » n'importe quel groupe fini par quotients successifs qui sont simples.*

Exercice 32.

1. *Soit H et K des groupes, et supposons qu'il existe un morphisme de groupes $\varphi : K \to \mathrm{Aut}(H)$. Montrer que la loi donnée par*

$$(h_1, k_1) * (h_2, k_2) = (h_1 \varphi(k_1)(h_2), k_1 k_2)$$

sur l'ensemble $H \times K$ est une loi de groupe, et identifier son élément neutre.

*On note $H \rtimes_\varphi K$ ce groupe, appelé **produit semi-direct** de H par K (relativement à φ).*

2. *Montrer que $H \rtimes_\varphi K$ contient un sous-groupe distingué isomorphe à H et un sous-groupe isomorphe à K, d'intersection réduite à (e_H, e_K).*

3. *Soit P un groupe possédant des sous-groupes H et K vérifiant :*

   (a) $H \triangleleft P$.
   (b) $P = HK$.
   (c) $H \cap K = \{e_P\}$.

   Montrer qu'il existe $\varphi : K \to \mathrm{Aut}(H)$ tel que $P \simeq H \rtimes_\varphi K$. Indication : Identifier φ dans le cadre de la question précédente.

4. *Identifier tous les produits semi-directs de la forme*

$$\mathbb{Z}/3\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}.$$

5. *Montrer que si G est un groupe et $H \triangleleft G$ alors G n'est pas forcément isomorphe à un produit semi-direct $G/H \rtimes_\varphi H$ ou $H \rtimes_\varphi G/H$. Indication : Penser à $\mathbb{H}_8$.*

6. *Supposons que $H \rtimes_\varphi K$ soit un produit semi-direct. On identifie abusivement H à $H \times \{e_K\} \subset H \rtimes_\varphi K$ et K à $\{e_H\} \times K \subset H \rtimes_\varphi K$. Montrer que $(H \rtimes_\varphi K)/H \simeq K$ et qu'il existe une **section** $s : K \to H \rtimes_\varphi K$, c'est-à-dire un morphisme de groupes tel que pour tout $k \in K, \pi_H(s(k)) = k$, où π_H est la projection dans le quotient par H.*

7. *Réciproquement, soit G un groupe, $H \triangleleft G$ et $K = G/H$. Supposons qu'il existe une section $s : K \to G$. Montrer que G est isomorphe à un produit semi-direct de H par K.*

Exercice 33. *Soit G un groupe. On dit que G est **résoluble** lorsque la suite $(D^n(G))_{n\in\mathbb{N}}$, définie par $D^0(G)$ et $D^{n+1}(G) = D(D^n(G))$ pour tout $n \in \mathbb{N}$, stationne à $\{e\}$.*

1. *Montrer qu'un groupe abélien est résoluble. Montrer que $\mathbb{H}_8$ est résoluble. Montrer qu'un groupe simple non abélien n'est pas résoluble (c'est par exemple le cas des groupes alternés $\mathfrak{A}_n$ pour $n \geq 5$).*

2. *Montrer que G est résoluble si et seulement s'il existe une famille finie de sous-groupes $(G_i)_{0 \leq i \leq n}$ telle que $G_0 = G, G_n = \{e\}$ et pour $0 \leq i < n, G_{i+1} \triangleleft G_i$ et G_i/G_{i+1} est abélien.*

3. *Soit H un sous-groupe distingué de G. Montrer que G est résoluble si et seulement si H et G/H le sont.*

Exercice 34. *Soit F un groupe. On dit que F est un **groupe libre** de rang $n \in \mathbb{N}^*$ lorsqu'il existe $a_1, \ldots, a_n \in F$ vérifiant la propriété universelle suivante : pour tout groupe G et tout $g_1, \ldots, g_n \in G$, il existe un unique morphisme de groupes $f : F \to G$ tel que pour tout $i \in \{1, \ldots, n\}$, $f(a_i) = g_i$. Dans cet exercice, un groupe sera dit libre s'il est libre de rang n pour un certain entier $n \geq 1$.*

1. *Montrer que $\mathbb{Z}$ est un groupe libre mais que $\mathbb{Z}^2$ ne l'est pas.*

2. *Un groupe fini peut-il être libre ?*

3. *Montrer que si F est un groupe libre de rang n et $a_1, \ldots, a_n \in F$ sont des éléments vérifiant la propriété universelle ci-dessus, alors $\{a_1, \ldots, a_n\}$ engendre F.*

4. *Montrer que si F est un groupe libre de rang n et un groupe libre de rang m alors $n = m$. On pourra considérer les morphismes de groupes $F \to \mathbb{Z}/2\mathbb{Z}$.*

5. *En admettant l'existence, montrer que pour tout $n \in \mathbb{N}^*$, il n'existe qu'un seul groupe libre de rang n à isomorphisme près.*

6. *Construire un groupe libre de rang 2. Indication : Considérer quatre symboles a, b, a^{-1}, b^{-1} et l'ensemble $\mathcal{M}$ des mots en a, b, a^{-1}, b^{-1}. C'est un monoïde pour la concaténation. Quotienter ce monoïde par le monoïde engendré par $aa^{-1}, a^{-1}a, bb^{-1}$ et $b^{-1}b$.*

Exercice 35. *Soit G un groupe admettant une partie génératrice finie S. On définit le **graphe de Cayley** $\mathcal{G}$ associé comme étant le graphe ayant pour sommets les éléments de G, et il existe une arête de g à g' si et seulement s'il existe $s \in S$ tel que $g' = gs$.*

1. *Montrer qu'on peut supposer que S est symétrique et fini, c'est-à-dire que pour tout $s \in S, s^{-1} \in S$. On le supposera dans la suite.*

2. *Dessiner les graphes de Cayley de $(\mathbb{Z}/n\mathbb{Z}, \{\overline{1}, -\overline{1}\}), (\mathbb{Z}^2, \{(1,0), (0,1), (-1,0), (0,-1)\})$ et $(F_2, \{a, b, a^{-1}, b^{-1}\})$ (où F_2 est le groupe libre à deux générateurs a et b).*

3. *Montrer que $\mathcal{G}$ est connexe et régulier (c'est-à-dire que tout sommet est relié au même nombre d'arêtes).*

4. *Si $g, g' \in G$, on définit $d_S(g, g')$ comme étant la longueur du plus court chemin reliant g à g' dans $\mathcal{G}$. Montrer que d_S est une distance sur G, invariante à gauche, au sens où $d(hg, hg') = d(g, g')$ pour tout $g, g', h \in G$.*