Jean Delcourt

Théorie des groupes

2e ÉDITION

DUNOD

Illustration de couverture : © *tarapong-Fotolia.com*

11, rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-080781-9

À Michèle, Sophie et Marie

Préface

Ce livre est consacré aux groupes. Les ouvrages traitant de cette théorie sont nombreux, notamment en langue anglaise ; pour la langue française, on citera ceux de J. Calais ([6]), de N. Bouvier ([5]) entièrement consacrés aux groupes ; d'autres, comme le Cours d'algèbre de D. Perrin ([22]), et la « somme » de J.-M. Arnaudiès et J. Bertin ([3]) traitent une large part de la théorie, entre autres thèmes d'algèbre.

Notre livre vise à compléter ces textes, mais il prétend à une certaine originalité.

- C'est un livre de **cours par les exercices** qui tente de suivre une démarche d'auto-enseignement. Ainsi, l'étudiant devra lire cet ouvrage crayon en main, et sera amené à démontrer la plupart des théorèmes lui-même. Bien sûr, ces exercices sont corrigés de façon très détaillée.
- Nous y avons inclus un certain nombre de problèmes, également corrigés. Bien que d'une ampleur moindre qu'un problème de Capes ou d'Agrégation, ils visent à concrétiser, sur des exemples précis, les concepts de la théorie.
- Le plus souvent possible nous avons utilisé le langage de la géométrie qui donne un éclairage saisissant à des propriétés qui paraissent purement algébriques[1].
- Enfin l'ouvrage offre la palette la plus large possible d'exemples réels de groupes. Notre conviction est, en effet, qu'on ne comprend bien une théorie que lorsqu'on est assez familiarisé avec le domaine auquel elle s'applique, avec les êtres qui la peuplent... Et nous n'avons pas hésité à détailler au maximum les corrections, afin de ne laisser aucun point obscur ; enfin nous l'espérons.

Bien sûr, il a fallu faire des choix. Nous avons été amené à renoncer à toute présentation de la théorie de Galois, alors même que c'est l'origine historique de la théorie des groupes ; et nous n'avons pas abordé les développements passionnants que sont la théorie des extensions de groupes, ainsi que celle des représentations de groupes. Enfin, il n'est pas non plus question des propriétés topologiques des groupes.

1. Lire et relire l'excellent [21].

Quelques remarques sur les notations. Le groupe diédral est très présent dans les exercices, car suffisamment simple et compliqué pour être exemplaire. Ayant $2n$ éléments, avec n entier, il est parfois noté $\mathbb{D}_n$, car il est groupe de symétrie du polygone régulier à n éléments, et contient le groupe cyclique à n éléments... Nous avons choisi de le noter $\mathbb{D}_{2n}$, l'indice étant alors le cardinal ; cela nous paraît en effet plus conforme aux habitudes récentes. De la même façon, nous notons $\mathbb{Z}/n$ le groupe additif quotient de $\mathbb{Z}$ par le sous-groupe des multiples de n ; c'est un compromis entre la notation $\mathbb{Z}/n\mathbb{Z}$ un peu longue, et $\mathbb{Z}_n$ qui peut prêter à confusion (avec nombres p-adiques). Plus important, et discutable, nous faisons souvent jouer au groupe noté $\mathbb{Z}/n$ le rôle du prototype d'un groupe cyclique d'ordre n. Or, ce n'en est qu'une réalisation particulière, additive, avec un générateur privilégié (la classe de 1), de même que le groupe des racines n-ièmes de l'unité en représente une autre réalisation. Il aurait sans doute été préférable d'avoir une notation différente pour « le » groupe cyclique d'ordre n, compris comme le groupe engendré par un élément x d'ordre n, de présentation $\langle x \mid x^n \rangle$. On trouve parfois une écriture comme $\mathbf{C}_n$. Notre choix risque de dérouter, surtout qu'il nous arrive de jongler entre notation additive et multiplicative, mais ce type d'écriture « à isomorphisme près » est fréquent... et a des avantages. On nous pardonnera aussi, peut-être, certains « ssi » mis pour « si et seulement si ».

Pour terminer, parlons de notre public, enfin du public souhaité : les connaissances nécessaires pour nous suivre sont celles qu'a acquises un étudiant de Licence 2. Il lui est demandé une certaine familiarité avec l'algèbre linéaire, et avec les rudiments de l'algèbre générale. Ce livre devrait donc être utile aux étudiants de Master, ainsi, bien sûr, qu'aux candidats aux concours Capes et Agrégation. Espérons également qu'il saura plaire aux simples amateurs de mathématiques.

Ce livre ne serait pas ce qu'il est sans les conseils éclairés que m'ont donnés de nombreux collègues et amis, spécialistes ou non de la théorie des groupes. Je remercie en particulier Dong Ye pour sa relecture attentive, mais il va de soi que les nombreuses erreurs qui subsistent sont entièrement de mon fait. Merci également aux éditions Dunod pour la qualité de leur travail éditorial.

Cette troisième édition a permis de corriger certaines erreurs et d'ajouter des précisions : merci à François Digne pour ses remarques. Nous avons également proposé quelques problèmes supplémentaires.

Table des matières

CHAPITRE 1 • **GROUPES – GROUPES CYCLIQUES** 1

1.1 Groupes, sous-groupes, ordre 1

1.2 Morphismes, sous-groupes normaux, groupes quotients 13

1.3 Problèmes 20

CHAPITRE 2 • **EXEMPLES DE GROUPES** 25

2.1 Groupes produits 25

2.2 Groupes libres, générateurs et relations 33

2.3 Quelques groupes finis 40

2.4 Groupes de permutations 46

2.5 Problèmes 56

CHAPITRE 3 • **ACTIONS DE GROUPES - GROUPES DE SYLOW** 59

3.1 Action d'un groupe sur un ensemble 59

3.2 Les théorèmes de Sylow 71

3.3 Produits semi-directs 85

3.4 D'autres groupes finis 97

3.5 Problèmes 106

CHAPITRE 4 • **GROUPES COMMUTATIFS** 111
4.1 Groupes commutatifs finis 111
4.2 Groupes commutatifs de type fini 121
4.3 Groupes divisibles 128
4.4 Problèmes 132

CHAPITRE 5 • **GROUPE DÉRIVÉ, GROUPES NILPOTENTS, GROUPES RÉSOLUBLES** 135
5.1 Centre, groupe dérivé 135
5.2 Résolution de groupes 146
5.3 Groupes nilpotents, groupes résolubles 151

CHAPITRE 6 • **PROBLÈMES SUPPLÉMENTAIRES** 159
6.1 Les produits en couronne 159
6.2 Groupes polyédraux et binaires polyédraux 162
6.3 Transitivité, blocs, groupes primitifs 165
6.4 Sur les sous-groupes 167
6.5 Des groupes d'ordre 12 168
6.6 Un groupe d'ordre 168 168
6.7 Sous-groupes maximaux 169

SOLUTIONS DES PROBLÈMES 170
1.3.1 Sous-groupes caractéristiques, centre 170
1.3.2 Le groupe modulaire $\mathcal{M}$ 171
2.5.1 Les sous-groupes d'un produit 174
2.5.2 Les groupes de Prüfer 175
3.5.1 Les groupes $\mathbf{GL}(n,\mathbb{K})$, $\mathbf{PGL}(n,\mathbb{K})$, $\mathbf{SL}(n,\mathbb{K})$, $\mathbf{PSL}(n,\mathbb{K})$ 177
3.5.2 Produits semi-directs en géométrie 181
4.4.1 Groupes commutatifs définis par générateurs 186
6.1 Les produits en couronne 189
6.2 Groupes polyédraux et binaires polyédraux 193
6.3 Transitivité, blocs, groupes primitifs 203
6.4 Sur les sous-groupes 207
6.5 Des groupes d'ordre 12 208
6.6 Un groupe d'ordre 168 211
6.7 Sous-groupes maximaux 212

ANNEXES 215

I Table des notations 215

II Description des groupes ayant moins de 30 éléments 216

III Lexique 219

BIBLIOGRAPHIE 220

ADRESSES INTERNET 222

INDEX 223

Chapitre 1

Groupes
Groupes cycliques

1.1 GROUPES, SOUS-GROUPES, ORDRE

Un groupe $\mathbf{G}$ ou $(\mathbf{G}, *)$ est un ensemble muni d'une loi $*$ associative qui admet un élément neutre et pour laquelle tout élément a un symétrique. Cela s'écrit :

$$\forall x, y, z \in \mathbf{G},\ x * (y * z) = (x * y) * z$$
$$\exists e \in \mathbf{G},\ x * e = e * x = x$$
$$\forall x \in \mathbf{G},\ \exists x' \in \mathbf{G},\ x * x' = x' * x = e$$

Si, de plus :

$$\forall x, y \in \mathbf{G},\ x * y = y * x$$

on dit que la loi est **commutative**, $\mathbf{G}$ est commutatif ou **abélien**. On note la loi de composition par $*$, par $\times$, ou par... rien du tout. Si la loi est commutative, on écrit plutôt $+$. On montre facilement que l'élément neutre est unique, il est noté e, 1 ou 0 dans le cas d'une loi commutative ; le symétrique de x est également unique, il est noté x^{-1} ou $-x$ (cas commutatif). Il est parfois appelé inverse (x^{-1}) ou oppposé ($-x$).

Un sous-groupe de $\mathbf{G}$ est un sous-ensemble de $\mathbf{G}$ qui est lui-même un groupe (pour la même loi de composition). Ainsi $\{e\}$ et $\mathbf{G}$ lui-même sont des sous-groupes de $\mathbf{G}$, appelés **sous-groupes triviaux**. Si $\mathbf{H}$ est un sous-groupe de $\mathbf{G}$, on écrit : $\mathbf{H} \leqslant \mathbf{G}$.

Exercice 1.1.1

Montrer qu'un ensemble $\mathbf{G}$ muni d'une loi associative est un groupe si et seulement si

$$\exists e \in \mathbf{G},\ \forall a \in \mathbf{G},\ e * a = a$$
$$\forall a \in \mathbf{G},\ \exists b \in \mathbf{G},\ b * a = e$$

Autrement dit, il suffit qu'il existe un élément neutre à gauche et un symétrique à gauche.

Exercice 1.1.2

Soit **G** un groupe fini, $\mathbf{G} = \{e, x_1, x_2, \ldots, x_{n-1}\}$ où e est l'élément neutre. On appelle **table** du groupe la matrice $T = (a_{i,j})$ où $a_{i,j} = x_i * x_j$. Montrer que T est un « carré latin », c'est-à-dire que sur chaque ligne et sur chaque colonne il y a un et un seul élément de **G**. Réciproquement, est-ce que tout carré latin est la table d'un groupe ?

Exercice 1.1.3

Soit **G** un groupe et S un sous-ensemble. Pourquoi peut-on parler du « sous-groupe engendré par **la** partie S » ? On le note $\langle \mathrm{S} \rangle$ ou gr(S).

Exercice 1.1.4

Si **H** est un sous-ensemble **fini** d'un groupe **G**, **stable** pour la loi. Montrer que **H** est un sous-groupe de **G**. Contre-exemple dans le cas de cardinal infini.

Après ces généralités, nous arrivons au premier résultat important de la théorie des groupes, connu sous le nom de **théorème de Lagrange** : tout sous-groupe d'un groupe fini a pour cardinal un diviseur du cardinal du groupe. En démontrant ce théorème, on introduit des définitions très importantes, celle de l'ensemble quotient $\mathbf{G}/\mathbf{H}$, celle de l'indice d'un sous-groupe.

Exercice 1.1.5

Soit **G** un groupe, **H** un sous-groupe et x un élément de **G**. On note $x\mathbf{H}$ l'ensemble des éléments de **G** qui s'écrivent xh, avec $h \in \mathbf{H}$.

1) Montrer que la relation $x\mathcal{R}y \iff y \in x\mathbf{H}$ est une relation d'équivalence.
2) Montrer que les classes d'équivalence sont de la forme $x\mathbf{H}$ et sont toutes en bijection avec **H**. L'ensemble quotient, c'est-à-dire l'ensemble des classes d'équivalence est noté $\mathbf{G}/\mathbf{H}$. Son cardinal s'appelle l'indice de **H** dans **G**, et il s'écrit $[\mathbf{G} : \mathbf{H}]$.
3) À quelle condition a-t-on $x\mathbf{H} = \mathbf{H}$? Quelles sont les classes d'équivalence qui sont des sous-groupes ?
4) Démontrer le **théorème de Lagrange**, si **H** est un sous-groupe d'un groupe fini **G**, alors le cardinal de **H** est un diviseur du cardinal de **G**.
5) On définit de même les classes d'équivalence à droite, de la forme $\mathbf{H}x$. Montrer que les classes à droite sont toutes en bijection avec **H**, et que l'ensemble quotient est en bijection avec l'ensemble des classes à gauche.

Exercice 1.1.6

Soit **H** un sous-groupe d'indice fini de **G**, et **K** un sous-groupe de **G** contenant **H**. Montrer qu'il est d'indice fini dans **G** et que :

$$[\mathbf{G} : \mathbf{H}] = [\mathbf{G} : \mathbf{K}][\mathbf{K} : \mathbf{H}]$$

Premiers exemples de groupes, les groupes cycliques. Ils apparaîtront sous différents aspects dans toute la théorie.

Exercice 1.1.7

On appelle **groupe monogène** un groupe engendré par un élément $\mathbf{G} = \langle x \rangle$. Montrer que $\mathbf{G}$ est infini, de la forme $\mathbf{G} = \{\ldots, x^{-1}, 1, x, x^2, x^3, \ldots\}$ ou fini de la forme $\mathbf{G} = \{1, x, x^2, \ldots, x^{n-1}\}$.[1] Un exemple du premier cas est $(\mathbb{Z},+)$, de générateur 1 ; le second cas est illustré par $(\mathbb{Z}/n\mathbb{Z},+)$, noté également $\mathbb{Z}/n$, ou par $\mathbb{U}_n$, groupe multiplicatif des racines n-ièmes de l'unité dans $\mathbb{C}$. Dans le cas fini, on dit que $\mathbf{G}$ est un **groupe cyclique**.

La notion d'**ordre** d'un élément est liée aux groupes cycliques. Rappelons qu'on appelle ordre d'un ensemble fini le nombre de ses éléments (on dit aussi cardinal). Il s'agit de deux emplois différents du mot ordre... Mais il y a quand même un lien.

Exercice 1.1.8

On appelle **ordre** d'un élément x d'un groupe $\mathbf{G}$ le plus petit entier $n > 0$ tel que $x^n = e$. Si n n'existe pas, on dit que x est d'ordre infini. L'ordre de x est souvent noté $|x|$ comme le cardinal d'un ensemble.

1) Montrer que l'ordre de x est l'ordre (i.e. le cardinal) du sous-groupe engendré par x.
2) Montrer que si l'ordre de x est n, alors $x^p = e \iff p \in n\mathbb{Z}$.
3) Si l'ordre de x est n, quel est l'ordre de x^k ?
4) Si a et b commutent, que peut-on dire de l'ordre de ab en fonction des ordres de a et de b ? On examinera le cas où les ordres de a et de b sont premiers entre eux.
5) Comparer les ordres de ab et de ba.
6) Dans un groupe fini, l'ordre de tout élément est fini. Réciproque ?

Exercice 1.1.9

Déterminer les sous-groupes d'un groupe cyclique. Traiter le cas infini, puis le cas d'un groupe cyclique d'ordre n ; il y a alors un sous-groupe de cardinal d pour chaque entier d divisant n. Que peut-on dire si n est premier ?

Exercice 1.1.10

Soit $\mathbf{G}$ un groupe cyclique d'ordre n engendré par x. On dit qu'un élément y de $\mathbf{G}$ est un **générateur** si $\mathbf{G} = \langle y \rangle$.
Montrer que les générateurs de $\mathbf{G}$ sont les éléments de la forme x^k où k est premier avec n. Détailler le cas où $n = 12$ puis où n est premier. On note $\phi(n)$ le nombre des générateurs d'un groupe cyclique d'ordre n ; c'est l'**indicateur d'Euler**.

Exercice 1.1.11

Calculer $\phi(p)$, $\phi(p^\alpha)$ (avec p premier). Démontrer que :

$$\forall x \in \mathbb{N}^*, \ \sum_{d|n} \phi(d) = n$$

1. On note x^k le produit de x par lui-même k fois, avec les conventions habituelles pour $x^0 = e$ et pour $x^k = (x^{-1})^{-k}$ si k est négatif.

Exercice 1.1.12

Montrer qu'un groupe fini de cardinal n est cyclique ssi pour tout d divisant n, il existe un seul sous-groupe de cardinal d. On utilisera l'exercice précédent. Montrer de même que tout sous-groupe fini (multiplicatif) d'un corps commutatif est cyclique.

Exercice 1.1.13

On suppose que $\mathbf{G}$ est un groupe tel que : $\forall x \in \mathbf{G},\ x^2 = e$; autrement dit, tous les éléments différents de e sont d'ordre 2. Montrer que $\mathbf{G}$ est commutatif.

Exercice 1.1.14

Montrer que si le cardinal d'un groupe $\mathbf{G}$ est pair, alors il existe dans $\mathbf{G}$ un élément d'ordre 2. Réciproque ? On verra une généralisation dans le chapitre 3 (lemme de Cauchy).

Exercice 1.1.15

Démontrer qu'un groupe est fini ssi il a un nombre fini de sous-groupes.

Nous sommes maintenant en mesure de classer tous les groupes finis ayant moins de sept éléments. Cette classification des groupes finis se poursuivra tout au long de cet ouvrage ; en annexe, un tableau regroupe les principaux résultats concernant ces groupes finis de petit cardinal.

Exercice 1.1.16

Montrer que tout groupe ayant p éléments, où p est premier, est un groupe cyclique. Ainsi, nous connaissons les groupes à 2, 3, 5 et 7 éléments. Ainsi, bien sûr, que le groupe à 1 seul élément, que l'on notera souvent e, 1, ou même 0 dans un contexte commutatif.

Exercice 1.1.17

Montrer qu'il y a deux groupes à quatre éléments, tous les deux commutatifs. Celui qui n'est pas cyclique se note $\mathcal{V}$ et s'appelle **groupe de Klein**, ou **groupe du rectangle**.

Exercice 1.1.18

Démontrer qu'il y a deux groupes à six éléments, dont l'un n'est pas commutatif.

Après les groupes cycliques et nos petits groupes, nous allons construire de nouveaux exemples à l'aide de l'algèbre linéaire.

Exercice 1.1.19 (Des sous-groupes de matrices)

On note $\mathcal{M}(n, \mathbb{K})$ l'espace vectoriel des matrices carrées à coefficients dans le corps $\mathbb{K}$. Montrer que les ensembles suivants sont des groupes pour la multiplication :

1) L'ensemble des matrices de déterminant non nul, $\mathbf{GL}(n, \mathbb{K})$ (groupe linéaire).

2) L'ensemble des matrices de déterminant égal à 1, $\mathbf{SL}(n, \mathbb{K})$ (groupe spécial linéaire).

3) L'ensemble des matrices triangulaires supérieures, $\mathbf{T}(n, \mathbb{K})$ (matrices inversibles dont tous les coefficients d'indice $i > j$ sont nuls) ou des matrices triangulaires unipotentes, $\mathbf{TU}(n, \mathbb{K})$, c'est-à-dire les matrices triangulaires supérieures n'ayant que des 1 sur la diagonale.

Exercice 1.1.20

L'ensemble des matrices symétriques inversibles est-il un sous-groupe de l'ensemble des matrices inversibles ? Montrer que l'ensemble des matrices qui s'écrivent $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ avec $a^2 \neq b^2$ est un groupe pour le produit.

Exercice 1.1.21

Trouver les sous-groupes engendrés par les matrices suivantes (la loi est le produit des matrices) :

1) $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

2) $B = \begin{pmatrix} j & 0 \\ 0 & j^2 \end{pmatrix}$ avec $j = e^{\frac{2i\pi}{3}}$

3) Étudier le groupe engendré par A et B. On vérifiera qu'il a douze éléments, et l'on en cherchera les sous-groupes.

Exercice 1.1.22

Soient $\mathbb{E}$ un $\mathbb{K}$-espace vectoriel et $\mathbb{F}$ un sous-espace vectoriel. Montrer que $\mathbb{F}$ est un sous-groupe additif de $\mathbb{E}$. Réciproquement, est-ce que tout sous-groupe additif de $\mathbb{E}$ est un sous-espace vectoriel ? Donner des contre-exemples, mais examiner aussi le cas où $\mathbb{K}$ est un corps fini.

L'exercice suivant est important. Il montre comment construire un groupe à l'aide de deux autres. Nous rencontrerons à nouveau, et à plusieurs reprises, ce genre de construction.

Exercice 1.1.23

Soit $\mathbf{G}$ un groupe et $\mathbf{H} \leqslant \mathbf{G}$, $\mathbf{K} \leqslant \mathbf{G}$ deux sous-groupes. On s'intéresse à l'ensemble des éléments de la forme hk où $h \in \mathbf{H}$, $k \in \mathbf{K}$, ensemble que l'on note $\mathbf{HK}$.

1) Démontrer que $\mathbf{HK}$ est un sous-groupe si et seulement si $\mathbf{HK} = \mathbf{KH}$.

2) Quel est le cardinal de $\mathbf{HK}$ quand les deux groupes $\mathbf{H}$ et $\mathbf{K}$ sont finis ?

3) Montrer que si $\mathbf{H} \cap \mathbf{K} = \{e\}$, alors tout élément de $\mathbf{HK}$ s'écrit de façon unique comme produit hk.

4) Soit $\mathbf{G} = \mathbb{Z}/6$ et $\mathbf{H} = \langle\overline{2}\rangle$, $\mathbf{K} = \langle\overline{3}\rangle$. Vérifier que $\mathbf{G} = \mathbf{HK}$ et qu'il y a unicité de l'écriture comme dans la question précédente.

SOLUTIONS

1.1.1 Si b est inverse à gauche de a, montrons qu'il est aussi inverse à droite, $b*(a*b) = (b*a)*b = e*b = b$; si c est l'inverse à gauche de b, $(c*b)*(a*b) = e*(a*b) = a*b = c*b = e$, donc $a*b = e$. Montrons maintenant que e est aussi neutre à droite : $a*e = a*b*a = e*a = a$.

1.1.2 La ligne i de la matrice est l'ensemble des images des éléments de **G** par l'application $x \mapsto x_i * x$. Or cette application, que l'on nomme translation à gauche, et qu'on note L_{x_i}, est bijective, puisque l'équation $x_i * x = y$ a pour seule solution $x = x_i^{-1} * y$. On traite de même les colonnes de la matrice.
Tous les carrés latins ne sont pas des tables de groupe, même si l'on impose que la première ligne et la première colonne correspondent à l'élément neutre :

$*$	e	a_1	a_2	a_3	a_4
e	e	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_4	e	a_3
a_2	a_2	a_3	a_1	a_4	e
a_3	a_3	a_4	e	a_2	a_1
a_4	a_4	e	a_3	a_1	a_2

Sur ce tableau on constate par exemple que : $(a_1*a_2)*a_3 = a_4*a_3 = a_1$ et que $a_1*(a_2*a_3) = a_1*a_4 = a_3$. La loi n'est pas associative.

1.1.3 Tout repose sur la propriété suivante. L'intersection de groupes est un groupe. Si donc S est un sous-ensemble de **G**, l'intersection des sous-groupes de **G** qui contiennent S est un sous-groupe, le plus petit contenant S. Comme **G** lui-même est un sous-groupe contenant S, cette intersection est bien définie et est non vide. Il est ensuite facile de montrer que ce sous-groupe est l'ensemble des produits de la forme : $s_1^{e_1} s_2^{e_2} \dots s_k^{e_k}$ où les s_i sont dans S et $e_i = \pm 1$. Comparer cette notion avec celle de « sous-espace vectoriel engendré par une partie ».

1.1.4 Soit $x \in \mathbf{H}$ et $\phi : g \mapsto xg$. Par hypothèse, si l'on restreint ϕ à **H**, l'ensemble d'arrivée est bien **H**. De plus, ϕ est injective ($xg = xg' \Rightarrow g = g'$ en multipliant par l'inverse de x dans **G**). Comme **H** est fini, elle est bijective, et donc e admet un antécédent, x est inversible dans **H**. **H** est donc bien un sous-groupe de **G**. Pour un contre-exemple, regarder $\mathbb{N}$, stable pour la somme, mais qui n'est pas un sous-groupe de $\mathbb{Z}$.

1.1.5 1) $x\mathcal{R}x$ pour tout x, car $x = xe \in x\mathbf{H}$; si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $y = xh$, $z = yh'$ donc $z = zhh'$ et $z \in x\mathbf{H}$. Enfin si $x = yh$ alors $y = xh^{-1}$. On a montré que la relation est réflexive, transitive et symétrique lorsque **H** est un sous-groupe. Remarquons que la relation $\mathcal{R}$ peut aussi être définie par : $x\mathcal{R}y \iff x^{-1}y \in \mathbf{H}$.

2) La définition même de la relation montre que les éléments en relation avec x sont tous dans $x\mathbf{H}$; de plus, l'application de **H** dans $x\mathbf{H}$ définie par $h \mapsto xh$ est bijective, surjective par définition de $x\mathbf{H}$ et injective car $xh = xh' \Rightarrow h = h'$, en composant à gauche par l'inverse de x.

3) $x\mathbf{H} = \mathbf{H}$ équivaut à x est en relation avec e, soit $x \in \mathbf{H}$. Si une classe est un sous-groupe, alors elle contient l'élément neutre e. C'est donc la classe de e, c'est-à-dire **H**. Toutes les autres classes ne sont pas des sous-groupes.

4) Comme pour toute relation d'équivalence, les classes d'équivalence forment une partition du groupe **G**. Leur ensemble s'écrit $\mathbf{G}/\mathbf{H}$ son cardinal, $[\mathbf{G} : \mathbf{H}]$ s'appelle l'indice de **H**

dans **G**. Il peut être fini quand **G** et **H** sont infinis : c'est le cas de l'indice de $n\mathbb{Z}$ dans $\mathbb{Z}$ (qui vaut n). Quand **G** est fini, toutes les classes d'équivalence ont autant d'éléments que **H** et :

$$\text{card}(\mathbf{G}) = [\mathbf{G} : \mathbf{H}]\ \text{card}(\mathbf{H})$$

En particulier, on en déduit le **théorème de Lagrange** : le cardinal d'un sous-groupe d'un groupe de cardinal fini n est un diviseur de n.

5) On peut, pour définir les classes à droite, considérer la relation d'équivalence :

$$x\mathcal{S}y \iff y \in \mathbf{H}x \iff yx^{-1} \in \mathbf{H}$$

La relation $\mathcal{R}$ et la relation $\mathcal{S}$ sont alors reliées par :

$$x\mathcal{R}y \iff x^{-1}\mathcal{S}y^{-1}$$

Si donc on note, comme cela se fait parfois, $\mathbf{G} \setminus \mathbf{H}$ l'ensemble des classes d'équivalence à droite, il y a bijection entre les deux ensembles quotients par :

$$x\mathbf{H} \mapsto \mathbf{H}x^{-1}$$

1.1.6 Supposons que la famille $(g_i)_{i\in I}$ soit une famille de représentants des classes de **G** modulo **K** et que $(k_j)_{j\in J}$ soit une famille de représentants des classes de **K** modulo **H**. Alors,

$$\mathbf{G} = \bigcup_{i\in I} g_i\mathbf{K} = \bigcup_{(i,j)\in I\times J} g_ik_j\mathbf{H}$$

Par ailleurs, si $g_ik_j\mathbf{H} = g_{i'}k_{j'}\mathbf{H}$, il vient $g_i^{-1}g_{i'} \in \mathbf{K}$ puisque $\mathbf{H} \subset \mathbf{K}$, et donc $g_i\mathbf{K} = g_{i'}\mathbf{K}$, soit $g_i = g_{i'}$. On a alors $k_j\mathbf{H} = k_{j'}\mathbf{H}$ d'où $k_j = k_{j'}$. On en déduit que les $(g_ik_j)_{(i,j)\in I\times J}$ constituent une famille de représentants des classes de **G** modulo **H**. Et donc, si l'indice $[\mathbf{G} : \mathbf{H}]$ est fini, le cardinal de $I \times J$ est fini, I et J sont finis et

$$[\mathbf{G} : \mathbf{H}] = [\mathbf{G} : \mathbf{K}]\,[\mathbf{K} : \mathbf{H}]$$

1.1.7 $\langle x\rangle$ contient tous les éléments de la forme $x^i, i \in \mathbb{Z}$. S'il est fini, il existe i et j distincts (par exemple $i > j$) tels que $x^i = x^j$. On en déduit $x^{i-j} = e$. Définissons maintenant n comme étant le plus petit des entiers strictement positifs tels que $x^n = e$. Alors :

- $x^p = e \iff p \in n\mathbb{Z}$
- $\mathbf{G} = \{e, x, x^2, \ldots, x^{n-1}\}$

En effet, si $x^p = e$ et si $p = nq + r$ est la division euclidienne de p par n, alors $x^r = (x^p)(x^n)^{-q} = e$; au vu de la définition de n, on doit avoir $r = 0$, donc p est un multiple de n. On vérifie que les éléments indiqués sont distincts, sinon on aurait une égalité de la forme $x^{i-j} = e$ avec $0 < i - j < n$. De plus, **G** ainsi décrit est bien un groupe, l'inverse de x^i est x^{n-i}.
Dans le cas infini, toutes les puissances de x sont distinctes, sinon l'argumentation ci-dessus conduirait à **G** fini. Alors, l'ensemble $\{\ldots, x^{-2}, x^{-1}, e, x, x^2, x^3, \ldots\}$ est bien un groupe.

1.1.8 Cet exercice ressemble beaucoup au précédent. On ne reprendra pas le détail des arguments.

1) Si x est d'ordre n, alors le sous-groupe engendré par x est $\{e, x, x^2, x^3, \ldots, x^{n-1}\}$. Ces éléments sont distincts, au nombre de n. On a bien $|x| = |\langle x\rangle|$. Si x n'est pas d'ordre fini, le sous-groupe engendré par x est en bijection avec $\mathbb{Z}$, il a une infinité d'éléments.

2) Déjà vu dans l'exercice précédent.

3) Soit ℓ l'ordre de x^k. Alors, $\left(x^k\right)^\ell = e$, donc $\exists\lambda \in \mathbb{Z}/\ k\ell = n\lambda$. Ce nombre est donc un multiple commun de k et de n, la plus petite valeur positive de ℓ est par conséquent celle

qui donne $k\ell = \text{ppcm}(k, n)$; or, on sait que :

$$\text{ppcm}(k, n) = k \vee n = \frac{kn}{k \wedge n}$$

On en déduit que

$$|x^k| = \frac{n}{k \wedge n}$$

Remarquons que x^k est de même ordre que x lorsque k et n sont premiers entre eux.

4) Le fait que a et b commutent permet d'écrire : $(ab)^k = a^k b^k$. Soient alors n et m les ordres respectifs de a et b. On a bien sûr $(ab)^{mn} = a^{mn}b^{mn} = e$. Supposons maintenant que $(ab)^\ell = a^\ell b^\ell = e$. Élevons cette égalité à l'exposant n, $a^{\ell n}b^{\ell n} = b^{\ell n} = e$. On en déduit que ℓn est un multiple de m. Comme n et m sont premiers entre eux, il vient, par le théorème de Gauss, que ℓ est un multiple de m. De même, on montre que ℓ est un multiple de n, et ℓ est un multiple du ppcm de m et n, c'est-à-dire de mn. Si m et n ne sont pas premiers entre eux, l'ordre de ab peut être plus petit que le ppcm des ordres ; si a est d'ordre 4, alors a^3 est d'ordre 4 et leur produit est d'ordre... 1.

5) Si ab est d'ordre n, alors :

$$(ba)^n = b(ab)^{n-1}a = b(ab)^{-1}a = bb^{-1}a^{-1}a = e$$

et ba est d'ordre m inférieur à n. Le même calcul montre que n est inférieur à m d'où l'égalité des ordres.

6) La réciproque est fausse. Autrement dit, il existe des groupes infinis dont tout élément est d'ordre fini. Nous aurons l'occasion d'en rencontrer plusieurs, mais voici un premier exemple. Soit **G** le groupe des suites à valeurs dans $\mathbb{Z}/2$; il est muni d'une structure de groupe additif en posant $(u + v)_n = u_n + v_n$, et tout élément est d'ordre fini égal à 2 (1 pour la suite constante nulle).

1.1.9 On reprend le même genre d'arguments que dans l'exercice précédent. Soit **H** un sous-groupe (autre que $\{e\}$) et $x^k \in \mathbf{H}$ tel que $k > 0$ (il y a de tels k car **H** est stable pour la prise d'inverse) soit minimum. Alors, $x^p \in \mathbf{H} \iff p \in k\mathbb{Z}$ par division euclidienne de p par k. Si **G** est infini, $\mathbf{H} = \langle x^k \rangle$ est alors un sous-groupe de **G**, et est aussi cyclique infini. Si **G** est fini d'ordre n, le théorème de Lagrange (1.1.5) permet d'affirmer que card(**H**) est un diviseur d de n.
Soit alors d un diviseur quelconque de n. Alors $\langle x^{\frac{n}{d}} \rangle$ est un sous-groupe d'ordre d (puisque $x^{\frac{n}{d}}$ est exactement d'ordre d, cf. 1.1.8). Donc il existe toujours un sous-groupe d'ordre d. Montrons maintenant qu'il n'y en a qu'un seul, si $\langle x^k \rangle$ est un sous-groupe d'ordre d, alors $x^{kd} = e$, donc $n|kd$ et $\frac{n}{d}|k$. Cela montre que x^k appartient à $\langle x^{\frac{n}{d}} \rangle$. On a donc $\langle x^k \rangle \subset \langle x^{\frac{n}{d}} \rangle$. Mais comme ces deux groupes ont même ordre, ils coïncident.
Il y a donc un seul sous-groupe d'ordre d. Si n est premier, il n'y a donc aucun sous-groupe autre que e et **G** lui-même.

1.1.10 On peut utiliser l'exercice 1.1.8 pour trouver les générateurs de $\langle x \rangle$ où x est d'ordre n : l'ordre de x^k est $\frac{n}{k \wedge n}$, il faut et suffit que k soit premier à n pour que x^k soit d'ordre n et donc générateur de **G**. Le nombre des générateurs de **G** est donc le nombre des entiers k plus petit que n et premiers à n, noté $\phi(n)$. Ainsi, pour $n = 12$, sont générateurs x, x^5, x^7, x^{11} et $\phi(12) = 4$. Si $n = p$ est un nombre premier, tous les $k \neq 0$ conviennent et $\phi(p) = p - 1$.

1.1.11 Dans l'exercice précédent, on a montré que $\phi(p) = p - 1$. Cherchons maintenant les entiers inférieurs à p^α qui sont non premiers à p^α. Ce sont les nombres divisibles par p de la forme kp pour $0 \leqslant k < p^{\alpha-1}$. Il y en a donc $p^{\alpha-1}$, et l'on en déduit $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Pour la dernière formule, on considère $\mathbf{G} = \langle x \rangle$ un groupe cyclique d'ordre n et on classe ses éléments suivant leur ordre, c'est un entier d diviseur de n, et chaque élément d'ordre d est un générateur du (seul) sous-groupe d'ordre d. Le nombre des éléments d'ordre d est donc le nombre des générateurs d'un groupe cyclique d'ordre d, soit $\phi(d)$. Cette partition donne donc l'égalité :

$$n = \sum_{d|n} \phi(d)$$

1.1.12 On sait déjà qu'un groupe cyclique a cette propriété. Réciproquement, soit $\mathbf{G}$ d'ordre n un groupe ayant un seul sous-groupe d'ordre d pour tout d diviseur de n. On note $\psi(d)$ le nombre des éléments de $\mathbf{G}$ qui sont d'ordre d, nombre qui peut être éventuellement nul. Soit d tel que $\psi(d) \neq 0$ et x un élément d'ordre d. Alors $\langle x \rangle$ est le seul sous-groupe d'ordre d, il est cyclique, et tout élément d'ordre d engendre ce même groupe : on a donc $\psi(d) = \phi(d)$ chaque fois que $\psi(d)$ est non nul. Mais, en classant les éléments de $\mathbf{G}$ suivant leur ordre, on obtient une partition de $\mathbf{G}$ et :

$$n = \sum_{d|n} \psi(d) = \sum_{d|n} \phi(d)$$

il est donc impossible que pour un d, $\psi(d)$ soit nul ; on a, pour tout d, $\psi(d) = \phi(d)$, en particulier $\psi(n) = \phi(n)$, et est non nul, il existe un élément d'ordre n et $\mathbf{G}$ est cyclique.
Avec les mêmes notations, supposons maintenant que $\mathbf{G}$ soit un sous-groupe fini du groupe multiplicatif d'un corps. Soit g un élément d'ordre d, s'il en existe, et $\mathbf{H} = \langle g \rangle$. Alors tout élément d'ordre d vérifie l'égalité $x^d = 1$, et les d éléments de $\mathbf{H}$ vérifient aussi cette égalité. Mais dans un corps, une équation de degré d admet au plus d solutions ; tous les éléments d'ordre d sont donc dans $\mathbf{H}$ et en sont des générateurs. On termine comme ci-dessus.

1.1.13 Suppposons que tout carré soit égal à l'élément neutre :

$$(xy)^2 = xyxy = e \Rightarrow x(xyxy)y = x(e)y \Rightarrow yx = xy$$

Le groupe est donc commutatif.

1.1.14 On peut partitionner $\mathbf{G}$ en deux sous-ensembles, l'ensemble des éléments égaux à leur inverse, et l'ensemble de ceux qui sont différents de leur inverse. Le cardinal de ce dernier ensemble est pair (on regroupe par paires x et x^{-1}) ; le premier ensemble contient au moins l'élément neutre. Si donc le cardinal $\mathbf{G}$ est pair, ce premier ensemble contient au moins un élément $x \neq e$, tel que $x = x^{-1}$ soit $x^2 = e$, x est d'ordre 2. La réciproque est contenue dans le théorème de Lagrange : si x est d'ordre 2 dans un groupe fini, son ordre divise le cardinal du groupe.

1.1.15 Dans un sens, pas de problème... Pour l'autre sens, une idée est de se ramener aux groupes monogènes. Supposons que $\mathbf{G}$ ait un nombre fini de sous-groupes, les sous-groupes de la forme $\langle x \rangle$ sont en nombre fini et leur réunion est $\mathbf{G}$. Si $\mathbf{G}$ avait une infinité d'éléments, parmi ces sous-groupes un serait monogène infini, ce qui est absurde car un tel groupe a une infinité de sous-groupes.

1.1.16 Nous avons déjà remarqué qu'un groupe cyclique ayant p éléments, p premier, n'a aucun sous-groupe non trivial. Pour un groupe $\mathbf{G}$ quelconque, d'ordre p premier, c'est la

même idée. Soit $x \neq e$. Son ordre est un diviseur de p différent de 1, c'est p. Le groupe **G** est donc engendré par x et est cyclique. Un groupe à 2 éléments sera cyclique, de modèle $\mathbb{Z}/2 = \{\overline{0}, \overline{1}\}$ s'il est noté additivement, ou $\{1, -1\}$ s'il est multiplicatif. De même, un groupe à trois éléments sera $\mathbb{Z}/3$ ou $\{1, j, j^2\}$, avec $j = e^{\frac{2i\pi}{3}}$, racine cubique de l'unité. De même pour cinq ou sept éléments. La suite nous prouvera que p premier n'est pas le seul cas où il existe un seul type de groupe ayant p éléments ; voir le tableau dans l'annexe B2.

1.1.17 Parmi les groupes ayant quatre éléments, il y a le groupe cyclique $\mathbb{Z}/4$ ou en version multiplicative $\{1, -1, i, -i\}$. Si **G** a quatre éléments et n'est pas cyclique, tous les éléments différents de e ont pour ordre 2. **G** est donc commutatif d'après l'exercice 1.1.13. Soit x et y deux éléments distincts et différents de e. Alors $x^2 = y^2 = e$ et $xy \neq x, xy \neq y$ car ni x ni y ne sont neutres. Comme le groupe est d'ordre 4, il n'y a pas d'autre élément. La table suivante s'en déduit, compte-tenu de la commutativité et de l'ordre 2 de xy :

$*$	e	x	y	xy
e	e	x	y	xy
x	x	e	xy	y
y	y	xy	e	x
xy	xy	y	x	e

C'est un carré latin. Reste à vérifier, il n'y a pas beaucoup de cas, l'associativité... Une autre méthode pour vérifier cette associativité est de trouver un « modèle » : dans le plan euclidien, (Oxy) repère orthogonal, on prend pour x la réflexion d'axe Ox, pour y la réflexion d'axe Oy. xy est alors la symétrie de centre O et le groupe obtenu est le groupe des isométries qui conservent un rectangle centré en O et d'axes de symétrie Ox et Oy. D'où le nom de **groupe du rectangle** pour ce groupe $\mathcal{V}$ (de l'allemand « vier », quatre). On le nomme également **groupe de Klein**[1].

1.1.18 Il y a le groupe cyclique. Soit **G** non cyclique d'ordre 6 et x un élément d'ordre 2. Il en existe d'après l'exercice 1.1.14. Si tous les éléments différents de e étaient d'ordre 2, on retrouverait un sous-groupe d'ordre 4 comme dans l'exercice précédent, ce qui est absurde (théorème de Lagrange). Il existe un élément y d'ordre 3. **G** contient donc déjà e, x, y, y^2, et $y^2 \neq x$ car il est d'ordre 3. Soit alors l'élément xy. Il est différent de e, car l'inverse de x est lui-même, de x et de y, car x et y sont différents de e. Il est différent de y^2 car x est différent de y. Enfin, les mêmes arguments montrent que xy^2 est distinct des précédents. Reste à définir les autres produits : yx ne peut être égal à e, x, y, y^2, il peut être xy ou xy^2. Compte-tenu de l'associativité, on voit rapidement que chacune des hypothèses permet de remplir la table ; dans le premier cas, on obtient :

$\times$	e	y	y^2	x	xy	xy^2
e	e	y	y^2	x	xy	xy^2
y	y	y^2	e	$\boldsymbol{xy}$	$\boldsymbol{xy^2}$	$\boldsymbol{x}$
y^2	y^2	e	y	$\boldsymbol{xy^2}$	$\boldsymbol{x}$	$\boldsymbol{xy}$
x	x	xy	xy^2	e	y	y^2
xy	xy	xy^2	x	$\boldsymbol{y}$	$\boldsymbol{y^2}$	$\boldsymbol{e}$
xy^2	xy^2	x	xy	$\boldsymbol{y^2}$	$\boldsymbol{e}$	$\boldsymbol{y}$

1. Dans le chapitre suivant, nous retrouverons ce groupe sous la forme $\mathbb{Z}/2 \times \mathbb{Z}/2$.

On « reconnaît » le groupe cyclique à six éléments ; il est commutatif et les puissances de xy, par exemple, redonnent tous les éléments du groupe. Dans le second cas, on obtient :

$\times$	e	y	y^2	x	xy	xy^2
e	e	y	y^2	x	xy	xy^2
y	y	y^2	e	$\boldsymbol{xy^2}$	$\boldsymbol{x}$	$\boldsymbol{xy}$
y^2	y^2	e	y	$\boldsymbol{xy}$	$\boldsymbol{xy^2}$	$\boldsymbol{x}$
x	x	xy	xy^2	e	y	y^2
xy	xy	xy^2	x	$\boldsymbol{y^2}$	$\boldsymbol{e}$	$\boldsymbol{y}$
xy^2	xy^2	x	xy	$\boldsymbol{y}$	$\boldsymbol{y^2}$	$\boldsymbol{e}$

C'est un groupe non commutatif ; il a deux éléments d'ordre 3, y et y^2, et trois d'ordre 2, x, xy, xy^2. Pour vérifier l'associativité, on peut prendre le modèle suivant, y est la rotation de centre O et d'angle $\frac{2\pi}{3}$, x est la réflexion d'axe Ox. On vérifie alors qu'on a bien $xy = y^2x$. Ce groupe, que l'on peut appeler groupe du triangle équilatéral, va réapparaître sous de nouveaux déguisements[1], on le notera $\mathcal{S}_3$.

1.1.19 Les connaissances classiques d'algèbre linéaire donnent la réponse aux deux premières questions. $\mathbf{GL}(n, \mathbb{K})$ est un groupe, car une matrice est inversible ssi son déterminant est non nul. $\mathbf{SL}(n, \mathbb{K})$ en est un sous-groupe, car le produit de deux matrices de déterminant 1 est une matrice de déterminant 1. Il en va de même pour l'inverse. Pour la dernière question, utilisons une méthode « géométrique » ; si une matrice de $\mathbf{T}(n, \mathbb{K})$ est interprétée comme la matrice d'un automorphisme u de $\mathbb{K}^n$ dans la base canonique, celui-ci est caractérisé parce qu'il conserve les espaces engendrés par e_1, par e_1, e_2,..., par $e_1, e_2, \ldots, e_n$. L'ensemble de tels automorphismes est stable pour la composition et pour l'inverse. On peut aussi montrer la stabilité de cet ensemble par le calcul ; on vérifie alors que si $A, B \in \mathbf{T}(n, \mathbb{K})$ alors, si $C = AB$ on a $c_{ii} = a_{ii}b_{ii}$. Cette observation montre que $\mathbf{TU}(n, \mathbb{K})$ est un sous-groupe.

1.1.20 Les matrices symétriques forment un sous-espace vectoriel donc un sous-groupe **additif** de l'ensemble des matrices carrées. En revanche, elles ne forment pas un sous-groupe multiplicatif en se restreignant à celles qui sont inversibles. En effet, le produit de deux matrices symétriques est symétrique ssi ces matrices commutent :

$$ {}^t(AB) = AB \iff {}^tB{}^tA = AB \iff BA = AB $$

et dès la dimension 2, on trouve des matrices symétriques inversibles qui ne commutent pas. Pour les mêmes raisons, l'inverse d'une matrice symétrique est une matrice symétrique.
Les matrices de la forme indiquée commutent et forment un sous-groupe de $\mathbf{GL}(n, \mathbb{K})$; il faut en particulier vérifier que le produit de deux matrices de cet ensemble est encore une matrice de la même forme.

1.1.21 1) Le groupe engendré par A est cyclique ; comme A est d'ordre 4, c'est le groupe cyclique à quatre éléments ou $\mathbb{Z}/4$.

2) Le groupe engendré par B est cyclique d'ordre 3.

3) La question est plus délicate. Un groupe engendré par deux éléments d'ordre fini peut être assez compliqué... Ici, le théorème de Lagrange prouve que le groupe engendré a au moins douze éléments, car il contient deux sous-groupes ayant quatre et trois éléments. Le calcul

1. Voir dans le chapitre 2, le paragraphe Groupes de permutations.