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.

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 dc tous les coefficients d'indice $i > j$ sont nuls) ou des matrices triangulaires unipotente $\mathbf{TU}(n, \mathbb{K})$, c'est-à-dire les matrices triangulaires supérieures n'ayant que des 1 sur diagonale.

Exercice 1.1.20

L'ensemble des matrices symétriques inversibles est-il un sous-groupe de l'ensemble c matrices inversibles ? Montrer que l'ensemble des matrices qui s'écrivent $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ av $a^2 \neq b^2$ 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 m trices) :

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 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 sou groupe additif de $\mathbb{E}$. Réciproquement, est-ce que tout sous-groupe additif de $\mathbb{E}$ est un sou espace vectoriel ? Donner des contre-exemples, mais examiner aussi le cas où $\mathbb{K}$ est un co 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 d 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 ?

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. La seule chose à vérifier est qu'elle est non vide ; parmi les sous-groupes contenant S, il y a au moins **G** et l'intersection contient au moins S. 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 (un antécédent de y est $x^{-1}y$). 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 $x = yh$, $y = zh'$ donc $x = zh'h$ et $x \in \mathbf{H}$. 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

4) Comme pour toute relation d'équivalence, les classes d'équivalence forment une partitio du groupe **G**. Leur ensemble s'écrit **G**/**H** son cardinal, [**G** : **H**] s'appelle l'indice de dans **G**. Il peut être fini quand **G** et **H** sont infinis : c'est le cas de l'indice de $n\mathbb{Z}$ dans (qui vaut n). Quand **G** est fini, toutes les classes d'équivalence ont autant d'éléments qu **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'u groupe de cardinal fini n est un diviseur de n.

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

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

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 droite, il y a bijection entre les deux ensembles quotients par :

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

1.1.6 Supposons que les classes de **G** modulo **K** aient pour représentants $g_1, \dots, g_n$, et qu les classes de **K** modulo **H** aient pour représentants $k_1, \dots, k_m$. Alors **G** est l'union des $g_i\mathbf{K}$ **K** est l'union des $k_j\mathbf{H}$ et donc **G** est l'union des $g_i k_j \mathbf{H}$.

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 distinct (par exemple $i > j$) tels que $x^i = x^j$. On en déduit $x^{i-j} = e$. Définissons maintenant n comm étant le plus petit des entiers strictement positifs tels que $x^n = e$. Alors :

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

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 d n. On vérifie que les éléments indiqués sont distincts, sinon on aurait une égalité de la form $x^{i-j} = e$ avec $0 < i - j < n$. De plus, **G** ainsi décrit est bien un groupe, l'inverse de x^i es x^{n-i}.
Dans le cas infini, toutes les puissances de x sont distinctes, sinon l'argumentation ci-dessu conduirait à **G** fini. Alors, l'ensemble $\{\dots, x^{-2}, x^{-1}, e, x, x^2, x^3, \dots\}$ est bien un groupe.

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

1) Si x est d'ordre n, alors le sous-groupe engendré par x est $\{e, x, x^2, x^3, \dots, x^{n-1}\}$. Ce éléments sont distincts, au nombre de n. On a bien $|x| = |\langle x \rangle|$. Si x n'est pas d'ordre fini

qui donne $k\ell = \text{ppcm}(k,\ell)$; 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, $\mathbf{H} = < n^k >$ 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

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

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

1.1.12 On sait déjà qu'un groupe cyclique a cette propriété. Réciproquement, soit **G** d'or n un groupe ayant un seul sous-groupe d'ordre d pour tout d diviseur de n. On note $\psi(d)$ nombre des éléments de **G** qui sont d'ordre d, nombre qui peut être éventuellement nul. S 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 est cyclique, et tout élément d'ordre d engendre ce même groupe ; on a donc $\psi(d) = \phi($ chaque fois que $\psi(d)$ est non nul. Mais, en classant les éléments de **G** suivant leur ordre, obtient une partition de **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, $\psi(d) = \phi(d)$, particulier $\psi(n) = \phi(n)$, et est non nul, il existe un élément d'ordre n et **G** est cyclique.
Avec les mêmes notations, supposons maintenant que **G** soit un sous-groupe fini du grou multiplicatif d'un corps. Soit g un élément d'ordre d, s'il en existe, et $\mathbf{H} = \langle g \rangle$. Alors tc élément d'ordre d vérifie l'égalité $x^d = 1$, et les d éléments de **H** vérifient aussi cette égali Mais dans un corps, une équation de degré d admet au plus d solutions ; tous les éléme d'ordre d sont donc dans **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 **G** en deux sous-ensembles, l'ensemble des éléments égaux leur inverse, et l'ensemble de ceux qui sont différents de leur inverse. Le cardinal de ce derni ensemble est pair (on regroupe par paires x et x^{-1}) ; le premier ensemble contient au moi l'élément neutre. Si donc le cardinal **G** est pair, ce premier ensemble contient au moins élément $x \neq e$, tel que $x = x^{-1}$ soit $x^2 = e$, x est d'ordre 2. La réciproque est contenue da le théorème de Lagrange : si x est d'ordre 2 dans un groupe fini, son ordre divise le cardin du groupe.

1.1.15 Dans un sens, pas de problème... Pour l'autre sens, une idée est de se ramener au groupes monogènes. Supposons que **G** ait un nombre fini de sous-groupes, il y a alors nombre fini de sous-groupes de la forme $\langle x \rangle$. Si **G** avait une infinité d'éléments, parmi c sous-groupes un serait monogène infini, ce qui est absurde car un tel groupe a une infinité sous-groupes.

$x \neq e$. Son ordre est un diviseur de p différent de 1, c'est p. Le groupe **G** est donc engendré par p 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 yx. 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	x	$\boldsymbol{xy}$	$\boldsymbol{xy^2}$	$\boldsymbol{x}$
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	$\boldsymbol{y^2}$	$\boldsymbol{e}$	$\boldsymbol{y}$

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	x	$\boldsymbol{xy^2}$	$\boldsymbol{x}$	$\boldsymbol{xy}$
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 d centre O et d'angle $\frac{2\pi}{3}$, x est la réflexion d'axe Ox. On vérifie alors qu'on a bien $xy = y^2x$. C groupe, que l'on peut appeler groupe du triangle équilatéral, va réapparaître sous de nouveau déguisements[1], on le notera $\mathcal{S}_3$.

1.1.19 Les connaissances classiques d'algèbre linéaire donnent la réponse aux deux pre mières questions. $\mathbf{GL}(n, \mathbb{K})$ est un groupe, car une matrice est inversible ssi son déterminan est non nul. $\mathbf{SL}(n, \mathbb{K})$ en est un sous-groupe, car le produit de deux matrices de déterminant est une matrice de déterminant 1. Il en va de même pour l'inverse. Pour la dernière questio utilisons une méthode « géométrique » ; si une matrice de $\mathbf{T}(n, \mathbb{K})$ est interprétée comme l matrice d'un automorphisme u de $\mathbb{K}^n$ dans la base canonique, celui-ci est caractérisé parc qu'il conserve les espaces engendrés par e_1, par $e_1, e_2, \ldots$, par $e_1, e_2, \ldots, e_n$. L'ensemble d tels automorphismes est stable pour la composition et pour l'inverse. On peut aussi montre la stabilité de cet ensemble par le calcul ; on vérifie alors que si $A, B \in \mathbf{T}(n, \mathbb{K})$ alors, $C = AB$, 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 **ad ditif** de l'ensemble des matrices carrées. En revanche, elles ne forment pas un sous-group multiplicatif en se restreignant à celles qui sont inversibles. En effet, le produit de deux ma trices 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 pa 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 fau en particulier vérifier que le produit de deux matrices de cet ensemble est encore une matric de la même forme.

1.1.21 1) Le groupe engendré par A est cyclique ; comme A est d'ordre 4, c'est le group 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 êt assez compliqué... Ici, le théorème de Lagrange prouve que le groupe engendré a au moi douze éléments, car il contient deux sous-groupes ayant quatre et trois éléments. Le calcu

montre que $AB = B^2A$, ce qui permet rapidement de voir que le groupe obtenu a bien douze éléments qui sont :

$$I,\ A,\ A^2,\ A^3,\ B,\ B^2,\ AB,\ A^2B,\ A^3B,\ AB^2,\ A^2B^2,\ A^3B^2$$

Le groupe obtenu est non commutatif, nous aurons l'occasion d'en donner d'autres descriptions. Disons tout de suite qu'on le note T, et qu'il fait partie des « groupes dicycliques ». Il contient un élément d'ordre 2, deux éléments d'ordre 3, six éléments d'ordre 4, et deux d'ordre 6.
On trouve alors six sous-groupes non triviaux qui contiennent tous le groupe à deux éléments. Pour une suite, voir l'exercice 3.3.6

1.1.22 Par définition même, un sous-espace vectoriel doit être lui-même un espace vectoriel, donc doit être un sous-groupe pour l'addition. En revanche, un sous-groupe additif de l'espace vectoriel $\mathbb{E}$ n'est pas forcément un $\mathbb{K}$-sous-espace vectoriel de $\mathbb{E}$. C'est par exemple le cas de $\mathbb{Q}$, sous-groupe additif du $\mathbb{R}$-espace vectoriel $\mathbb{R}$.
Si néanmoins $\mathbb{K} = \mathbb{F}_p$ est un corps fini à p éléments[1] où p est premier, alors les deux notions coïncident. En effet, la multiplication par un scalaire est, en ce cas, une addition répétée ; si $\mathbb{F}$ est un sous-groupe additif de $\mathbb{E}$,

$$\forall \lambda \in \mathbb{F}_p,\ \forall x \in \mathbb{F},\ \lambda.x = (1+1+1+\ldots+1).x = x+x+\ldots+x \in \mathbb{F}$$

On a noté 1 la classe de 1 et utilisé que $\mathbb{F}_p$ est additivement cyclique.

1.1.23 1) Utilisons pour résoudre cette question le « lemme » : $\mathbf{H}$ non vide est un sous-groupe de $\mathbf{G}$ ssi $\mathbf{HH} = \mathbf{H}$ et $\mathbf{H}^{-1} = \mathbf{H}$. On rédigera alors ainsi $\mathbf{HKHK} = \mathbf{HHKK} = \mathbf{HK}$ et $(\mathbf{HK})^{-1} = \mathbf{K}^{-1}\mathbf{H}^{-1} = \mathbf{KH} = \mathbf{HK}$ pour démontrer une implication. Pour l'autre, on dira :

$$\mathbf{K} \subset \mathbf{HK},\ \mathbf{H} \subset \mathbf{HK} \Rightarrow \mathbf{KH} \subset \mathbf{HK}, \qquad \mathbf{HK} = (\mathbf{HK})^{-1} \subset \mathbf{K}^{-1}\mathbf{H}^{-1} = \mathbf{KH}$$

ce qui prouve que $\mathbf{HK}$ est un sous-groupe de $\mathbf{G}$ implique $\mathbf{HK} = \mathbf{KH}$.

2) Supposons que $[\mathbf{H} : \mathbf{H} \cap \mathbf{K}] = n$, alors il existe $x_1, \ldots, x_n$ dans $\mathbf{H}$ tels que :

$$\mathbf{H} = \bigcup_{i=1..n} x_i \mathbf{H} \cap \mathbf{K}$$

ces classes étant disjointes. On en déduit :

$$\mathbf{HK} = \bigcup_{i=1..n} x_i(\mathbf{H} \cap \mathbf{K})\mathbf{K} = \bigcup_{i=1..n} x_i \mathbf{K}$$

car $(\mathbf{H} \cap \mathbf{K})\mathbf{K} = \mathbf{K}$. De plus, ces ensembles sont disjoints, car si $x_i\mathbf{K}$ et $x_j\mathbf{K}$ se rencontrent, il existe $k \in \mathbf{K}$ tel que $x_i = x_j k$ et $k \in \mathbf{H} \cap \mathbf{K}$ puisque x_i et x_j sont dans $\mathbf{H}$, donc $x_i = x_j$. Ainsi, le cardinal de $\mathbf{HK}$ vaut $n \times |\mathbf{K}|$, d'où la formule :

$$|\mathbf{HK}| = \frac{|\mathbf{H}||\mathbf{K}|}{|\mathbf{H} \cap \mathbf{K}|}$$

3)

$$hk = h'k' \Rightarrow kk'^{-1} = h^{-1}h' \in \mathbf{H} \cap \mathbf{K} = \{e\}$$

donc $k = k'$ et $h = h'$.

1.2 MORPHISMES, SOUS-GROUPES NORMAUX, GROUPES QUOTIENTS

Un **morphisme de groupes** est une application ϕ d'un groupe $\mathbf{G}$ dans un groupe $\mathbf{H}$ qui respecte les opérations :

$$\forall g, g' \in \mathbf{G},\ \phi(gg') = \phi(g)\phi(g')$$

Tout morphisme transporte l'élément neutre en l'élément neutre, le symétrique de l'image de x est l'image du symétrique de x. De plus, ϕ et ϕ^{-1} transportent les sous-groupes en des sous-groupes.
Comme en algèbre linéaire, on appelle **noyau** d'un morphisme ϕ, noté $\mathrm{Ker}(\phi)$, l'ensemble des antécédents de l'élément neutre. Un morphisme est injectif ssi son noyau est réduit au neutre.
Si un morphisme de $\mathbf{G}$ vers $\mathbf{G}'$ est bijectif, son application réciproque est aussi un morphisme. Les deux groupes sont dits **isomorphes**, et l'on écrit :

$$\mathbf{G} \cong \mathbf{G}'$$

Un isomorphisme d'un groupe dans lui-même s'appelle un **automorphisme**. L'ensemble des automorphismes de $\mathbf{G}$ est un groupe pour la loi de composition ou loi rond ; il est noté $\mathrm{Aut}(\mathbf{G})$.

Exercice 1.2.1

Quel est l'effet d'un morphisme (d'un isomorphisme) sur l'ordre d'un élément ?

Exercice 1.2.2

Les groupes $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ munis de l'addition sont-ils isomorphes ?

Exercice 1.2.3

Soit x un élément quelconque de $\mathbf{G}$. On note i_x l'application :

$$\begin{array}{rccc} i_x : & \mathbf{G} & \to & \mathbf{G} \\ & g & \mapsto & i_x(g) = xgx^{-1} \end{array}$$

Montrer que i_x est un automorphisme de $\mathbf{G}$. On l'appelle **automorphisme intérieur**. Montrer que l'ensemble des automorphismes intérieurs est un sous-groupe de l'ensemble des automorphismes de $\mathbf{G}$. On le note $\mathrm{Int}(\mathbf{G})$.

Exercice 1.2.4

Montrer que $x \mapsto x^2$ de $\mathbf{G}$ dans $\mathbf{G}$ est un morphisme ssi $\mathbf{G}$ est commutatif. Lorsque $\mathbf{G}$ est fini, à quelle condition est-ce un automorphisme ?

Un sous-groupe $\mathbf{H}$ de $\mathbf{G}$ est **normal** (ou **distingué**) dans $\mathbf{G}$ si toute classe à gauche est