1. *Définition des groupes; exemples*

On appelle **groupe** *un couple formé d'un ensemble* G *et d'une loi de composition* $(x, y) \to xy$ *sur l'ensemble* G, *ces données devant vérifier les trois conditions suivantes :*

a) *on a* $x(yz) = (xy)z$ *quels que soient* $x, y, z \in G$ (associativité);

b) *il existe un élément* e *de* G *tel que* $xe = ex = x$ *pour tout* $x \in G$ (existence d'un élément neutre);

c) *pour tout* $x \in G$, *il existe un élément* $x^{-1} \in G$ *tel que* $x^{-1}x = xx^{-1} = e$ (existence d'un inverse pour tout élément de G).

Pour définir un groupe, il ne suffit pas de se donner un ensemble G; il faut aussi se donner une loi de composition sur l'ensemble G, vérifiant les conditions *a*), *b*), *c*) ci-dessus; néanmoins, on désigne toujours un groupe par la même lettre, G par exemple, que l'ensemble qui en constitue l'une des données.

Le débutant aura soin de *ne pas* dire qu'un groupe « est un ensemble G sur lequel *il existe* une loi de composition vérifiant les conditions *a*), *b*), *c*) ci-dessus », car on peut facilement démontrer que, sur tout ensemble, il existe une telle loi de composition, et même qu'on peut en construire une infinité pour peu que l'ensemble donné soit lui-même infini; en disant qu'un groupe est « un ensemble sur lequel il existe » une loi de composition, on ne dit donc rien d'autre que ceci : « un groupe est un ensemble » — définition dont la stupidité est particulièrement claire...

En fait, en théorie des groupes, on ne s'intéresse pas du tout à l'existence (i.e. à la possibilité de construction) sur un ensemble donné G d'une loi de composition vérifiant les conditions *a*), *b*), *c*); au contraire, on suppose qu'une telle loi *est donnée d'avance* une fois pour toutes, et on se propose de l'utiliser pour démontrer des théorèmes.

Dans la définition donnée plus haut, nous avons utilisé l'écriture multiplicative, ce qu'on fait en effet le plus souvent (signalons en passant que l'élément neutre se note parfois 1 au lieu de e et s'appelle fréquemment l'**élément unité** de G); mais lorsqu'on a un **groupe commutatif** (ou **abélien**), i.e. un groupe dont la loi de composition est commutative, on utilise parfois l'écriture additive $(x, y) \to x + y$; dans ce cas, les conditions *a*), *b*), *c*) se traduisent comme suit :

a') *on a* $x + (y + z) = (x + y) + z$ *quels que soient* $x, y, z \in G$;

b') *il existe un élément* 0 *de* G *tel que* $x + 0 = x$ *pour tout* $x \in G$;

c') *pour tout* $x \in G$, *il existe dans* G *un élément, noté* $-x$, *tel que* $x + (-x) = 0$.

Il faut bien entendu, dans ce cas, ajouter la condition

d') *on a* $x + y = y + x$ *quels que soient* $x, y \in G$.

Exemple 1. L'ensemble **Z** des entiers rationnels et la loi de composition $(x, y) \mapsto x + y$ constituent évidemment un groupe commutatif; on l'appelle le **groupe additif des entiers rationnels.** En remplaçant **Z** par **Q** ou par **R**, on définirait de même le **groupe additif des nombres rationnels** et le **groupe additif des nombres réels.**

Exemple 2. Le couple formé par l'ensemble $\mathbf{Q}^*$ des nombres rationnels non nuls et par la loi de composition $(x, y) \mapsto xy$ sur cet ensemble est un groupe (dont l'élément neutre est le nombre 1); on l'appelle le **groupe multiplicatif des nombres rationnels non nuls.** On définirait de même le **groupe multiplicatif des nombres réels non nuls,** noté $\mathbf{R}^*$.

Exemple 3. On note $\mathbf{Q}_+^*$ le groupe obtenu en considérant l'ensemble de tous les nombres rationnels *strictement positifs*, la loi de composition sur cet ensemble étant la multiplication usuelle. On note de même $\mathbf{R}_+^*$ le groupe multiplicatif des nombres réels strictement positifs.

On notera par contre que le couple formé par l'ensemble I des nombres réels x tels que $0 < x \leqslant 1$, et par la loi de composition $(x, y) \mapsto xy$ sur cet ensemble, n'est pas un groupe : la condition *c*) de la définition des groupes *n'est pas* vérifiée.

Exemple 4. Soit X un ensemble quelconque; rappelons (§ 2, n° 8) qu'on appelle *permutation de* X toute application *bijective* de X dans X. Soit $\mathfrak{S}(X)$ l'ensemble de ces permutations; si f, g sont des permutations de X, il en est de même de l'application composée $f \circ g$ (§ 2, Théorème 6); la formule $(f, g) \mapsto f \circ g$ définit donc une loi de composition sur l'ensemble $\mathfrak{S}(X)$; cette loi de composition est associative (§ 2, Théorème 2); elle admet un élément neutre, à savoir l'application identique j_X (appelée souvent la **permutation unité** de l'ensemble X); enfin, si f est une permutation de X, il en est de même de l'application réciproque f^{-1} en vertu du § 2, Théorème 5, et celle-ci est évidemment inverse de f pour la loi de composition considérée.

Ainsi, le couple formé par l'ensemble $\mathfrak{S}(X)$ et par la loi de composition $(f, g) \to f \circ g$ sur cet ensemble est un groupe; on l'appelle le **groupe des permutations de l'ensemble** X. C'est l'étude de ces groupes par Galois (lorsque X est un ensemble fini) qui a conduit, historiquement, à la notion générale et « abstraite » de groupe.

Prenons par exemple pour X l'ensemble constitué par les entiers 1, 2, 3; alors $\mathfrak{S}(X)$ comporte six éléments, à savoir les permutations

$$\begin{aligned}
s_1 &: 1, 2, 3 \mapsto 1, 2, 3\\
s_2 &: 1, 2, 3 \mapsto 2, 3, 1\\
s_3 &: 1, 2, 3 \mapsto 3, 1, 2\\
s_4 &: 1, 2, 3 \mapsto 1, 3, 2\\
s_5 &: 1, 2, 3 \mapsto 2, 1, 3\\
s_6 &: 1, 2, 3 \mapsto 3, 2, 1
\end{aligned}$$

et la loi de composition est donnée par la « table de multiplication » suivante :

	s_1	s_2	s_3	s_4	s_5	s_6
s_1	s_1	s_2	s_3	s_4	s_5	s_6
s_2	s_2	s_3	s_1	s_5	s_6	s_4
s_3	s_3	s_1	s_2	s_6	s_4	s_5
s_4	s_4	s_6	s_5	s_1	s_3	s_2
s_5	s_5	s_4	s_6	s_2	s_1	s_3
s_6	s_6	s_5	s_4	s_3	s_2	s_1

(on a adopté la convention suivante : pour calculer un produit xy à l'aide de cette table, on porte x en *ligne* et y en *colonne*. Exemple : $s_2 s_4 = s_5$, $s_4 s_2 = s_6$).

Cet exemple prouve l'existence de **groupes finis,** i.e. de groupes à un nombre fini d'éléments; il est clair d'ailleurs que $\mathfrak{S}(X)$ est fini dès que (et seulement si) l'ensemble X est fini.

Lorsque X est l'ensemble formé des entiers $1, 2, \cdots, n$ (on a vu ci-dessus ce qui se passe pour $n = 3$), on utilise, au lieu de la notation $\mathfrak{S}(X)$, la notation

$$\mathfrak{S}_n$$

et on appelle $\mathfrak{S}_n$ le **groupe des permutations de *n* objets** ou encore le **groupe symétrique à *n* variables** On a vu au § 5 (Corollaire du Théorème 9) que le nombre d'éléments de $\mathfrak{S}_n$ est l'entier

$$n\,! = 1.2\ldots n,$$

produits des n premiers entiers strictement positifs. Étant donné qu'on a

$$6\,! = 720, \quad 7\,! = 5\,040, \quad 8\,! = 40\,320, \quad 9\,! = 362\,880, \quad 10\,! = 3\,628\,800,$$

il serait tout à fait utopique d'espérer déduire les propriétés des groupes $\mathfrak{S}_n$ d'un examen de leurs tables de multiplication...

Exemple 5. On obtient un groupe commutatif (noté additivement) en considérant l'ensemble G des vecteurs d'origine donnée O dans l'espace usuel, et, sur cet ensemble, la loi de composition $(x, y) \to x + y$ donnée par la classique règle du parallélogramme.

2. *Produit direct de groupes*

Soient $G_1, \ldots, G_n$ des groupes notés multiplicativement; sur l'ensemble produit

$$G = G_1 \times \cdots \times G_n$$

(§ 2, n° 2), considérons la loi de composition donnée par la formule

$$(x_1, \ldots, x_n)\ (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n);$$

le couple formé par l'ensemble G et cette loi de composition *est un groupe.*

Pour établir l'associativité, considérons trois éléments

$$x = (x_1, \ldots, x_n), \qquad y = (y_1, \ldots, y_n), \qquad z = (z_1, \ldots, z_n)$$

de G; on a par définition

$$xy = (x_1 y_1, \ldots, x_n y_n), \qquad yz = (y_1 z_1, \ldots, y_n z_n)$$

et par suite

$$(xy)z = ((x_1 y_1)z_1, \ldots, (x_n y_n)z_n), \qquad x(yz) = (x_1(y_1 z_1), \ldots, x_n(y_n z_n)),$$

de sorte que l'associativité dans G résulte de l'associativité des lois de composition données sur $G_1, \ldots, G_n$.

Pour montrer que G possède un élément neutre, il suffit de considérer l'élément

$$e = (e_1, \ldots, e_n)$$

où e_i désigne l'élément neutre de G_i pour $1 \leqslant i \leqslant n$; un calcul trivial montre aussitôt que e est élément neutre pour la loi de composition considérée sur G. Enfin, si

$$x = (x_1, \ldots, x_n)$$

est un élément de G, on voit immédiatement que x admet un inverse, donné par la formule

$$x^{-1} = (x_1^{-1}, \ldots, x_n^{-1}).$$

On obtient donc bien un groupe en munissant l'ensemble produit $G_1 \times \cdots \times G_n$ de la loi de composition définie plus haut; le groupe ainsi obtenu s'appelle le **produit direct des groupes** $G_1, \ldots, G_n$.

Lorsque les groupes $G_1, \ldots, G_n$ sont commutatifs et notés additivement, on utilise aussi l'écriture additive sur leur produit direct (ce qui est légitime, un produit direct de groupes commutatifs étant commutatif). La loi de composition sur le produit direct est donc alors donnée par la relation

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),$$

et l'élément neutre du produit direct n'est autre que

$$(0, \ldots, 0)$$

(où l'on désigne par le même symbole 0 les éléments neutres des divers groupes $G_1, \ldots, G_n$).

Enfin, étant donné un groupe G, on définit, pour tout entier $n \geqslant 1$, le *groupe*

$$G^n$$

comme étant le produit direct de n groupes identiques à G :

$$G^n = G \times \cdots \times G \quad (n \text{ facteurs}).$$

Exemple 6. Le **groupe additif $\mathbf{Z}^n$** est défini comme suit : ses éléments sont les suites $(x_1, \ldots, x_n)$ de n entiers rationnels, et la loi de composition est donnée par la formule

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n).$$

On définirait de même le **groupe additif $\mathbf{Q}^n$** (où $\mathbf{Q}$ est le groupe additif des nombres rationnels, défini dans l'*Exemple* 1), et le **groupe additif $\mathbf{R}^n$** (où $\mathbf{R}$ est le groupe additif des nombres réels).

Choisissons, dans un plan, un système d'axes de coordonnées Ox, Oy, et à tout élément (x, y) de $\mathbf{R}^2$ associons le vecteur $\overrightarrow{OP}$ d'origine O ayant pour composantes, relativement au système de coordonnées choisi, les nombres x et y. On obtient ainsi une bijection de l'ensemble $\mathbf{R}^2$ sur l'ensemble des vecteurs d'origine O dans le plan. Cette bijection transforme la somme (dans le groupe additif $\mathbf{R}^2$) de deux éléments (x', y') et (x'', y'') de $\mathbf{R}^2$ en la somme des vecteurs $\overrightarrow{OP'}$ et $\overrightarrow{OP''}$ qui leur correspondent : en effet, il est bien connu que pour additionner des vecteurs, on doit additionner leurs composantes.

On peut donc considérer l'addition dans $\mathbf{R}^2$ comme une traduction algébrique de la notion « géométrique » de somme de deux vecteurs dans le plan.

3. *Sous-groupes d'un groupe*

On dit qu'une partie H *d'un groupe* G *est un* **sous-groupe** *de* G *si* H *est non vide et si les relations*

$$x \in H \quad et \quad y \in H \quad impliquent \quad xy^{-1} \in H.$$

Un groupe G possède toujours au moins deux sous-groupes : G tout entier, et l'ensemble $\{e\}$ réduit à l'élément neutre de G. Il est clair d'autre part que les groupes additifs $\mathbf{Z}$ et $\mathbf{Q}$ sont des sous-groupes du groupe additif $\mathbf{R}$ (*Exemple* 1).

Soit H un sous-groupe d'un groupe G; comme H est non vide, il contient au moins un élément a; des relations $a \in H$ et $a \in H$ résulte alors que H contient

$$aa^{-1} = e;$$

ainsi, *un sous-groupe* H *de* G *contient toujours l'élément neutre de* G. D'autre part, si H contient un élément x, comme il contient e et x il contient aussi

$$ex^{-1} = x^{-1};$$

ainsi, *la relation* $x \in H$ *implique la relation* $x^{-1} \in H$. Soient alors x, y des éléments de H; comme H contient, d'après ce qui précède, x et y^{-1}, il devra contenir

$$x(y^{-1})^{-1} = xy;$$

donc, *les relations* $x \in H$ *et* $y \in H$ *impliquent la relation* $xy \in H$.

Réciproquement, considérons une partie H de G qui possède les trois propriétés suivantes :

a) *les relations* $x \in H$ *et* $y \in H$ *impliquent* $xy \in H$;

b) H *contient l'élément neutre e de* G;

c) *la relation* $x \in H$ *implique la relation* $x^{-1} \in H$.

Alors H est un sous-groupe de G. En effet, H est non vide d'après la condition *b*); soient d'autre part x et y deux éléments de H; d'après *c*), H contient x et y^{-1}; d'après *a*), il contient donc xy^{-1}, et notre assertion est établie.

Ainsi, les conditions *a*), *b*) et *c*) ci-dessus *caractérisent* les sous-groupes; dans la pratique, on les utilise très souvent à la place de la définition initiale.

On notera par contre qu'une partie H de G vérifiant seulement *a*), ou seulement *a*) et *b*), n'est pas nécessairement un sous-groupe de G; si par exemple G est le groupe additif $\mathbf{Z}$ des entiers rationnels, l'ensemble $\mathbf{N}$ des entiers $n \geqslant 0$ vérifie *a*) et *b*) mais n'est pas un sous-groupe de G.

Soit H un sous-groupe d'un groupe G; la condition *a*) ci-dessus montre que l'application $(x, y) \to xy$ de $G \times G$ dans G applique $H \times H$ dans H, donc « induit » une loi de composition sur H; cela dit, *l'ensemble* H, *muni de cette loi de composition, est un groupe*. En effet, la loi de composition donnée sur G étant associative l'est *a fortiori* sur H; puisque H contient l'élément neutre de G, il est clair d'autre part que la loi de composition considérée sur H admet bien un élément neutre (à savoir celui de G); enfin, tout $x \in H$ est inversible dans H en vertu de la condition *c*) ci-dessus.

Dorénavant, quand nous considérerons un sous-groupe H d'un groupe G, nous regarderons toujours H comme étant lui-même un groupe en le munissant, comme ci-dessus, de la loi de composition induite par celle du groupe donné G.

Exemple 7. Étant donné un ensemble X quelconque, on appelle **groupe de transformations de l'ensemble** X tout sous-groupe du groupe $\mathfrak{S}(X)$ des permutations de X. Un groupe de transformations de X est donc un ensemble G d'applications de X dans X, possédant les propriétés suivantes : *toute* $s \in G$ *est bijective;* G *contient l'application identique* j_X; *et si* G *contient deux applications s et t, il contient aussi* $s \circ t^{-1}$. On peut alors regarder l'ensemble G comme un groupe en le munissant de la loi de composition

$$(s, t) \mapsto s \circ t.$$

La Géométrie élémentaire fournit de nombreux exemples de groupes de transformations : le groupe des translations sur la droite, ou dans le plan, ou dans l'espace; le groupe des rotations autour d'un point dans le plan, ou dans l'espace; le groupe des déplacements dans le plan, ou dans l'espace; le groupe des homothéties de centre donné et de rapport *non nul* dans le plan ou dans l'espace; etc, etc...

Exemple 8. Prenons pour G le groupe additif $\mathbf{Z}$ des entiers; un sous-groupe de $\mathbf{Z}$ est donc un ensemble I d'entiers vérifiant les conditions suivantes : on a $0 \in I$, et si I contient deux entiers x et y il contient aussi $x - y$. Pour tout entier n, notons $n\mathbf{Z}$ l'ensemble des multiples de n (i.e. l'ensemble des entiers nx où x parcourt $\mathbf{Z}$); il est clair que c'est un sous-groupe de $\mathbf{Z}$. Inversement, *pour tout sous-groupe* I *de* $\mathbf{Z}$, *il existe un et un seul entier* $n \geqslant 0$ *tel que* $I = n\mathbf{Z}$. Notons d'abord que cette assertion est triviale si $I = \{0\}$: il suffit alors de prendre $n = 0$. Supposons donc $I \neq \{0\}$; il existe dans I des entiers non nuls, et même *strictement positifs* (car si $n \in I$ on a aussi $-n \in I$); soit alors n *le plus petit entier strictement positif appartenant à* I (rappelons que, dans tout ensemble d'entiers positifs, il existe un élément plus petit que tous les autres d'après le § 5, *Remarque* 2); nous allons montrer que $I = n\mathbf{Z}$. En effet, comme I contient n et n il contient $n + n = 2n$, donc $n + 2n = 3n$, etc..., donc nx pour tout $x \geqslant 1$; d'autre part I contient $n0 = 0$; enfin, si x est un entier négatif, I contient $n(-x) = -nx$ d'après ce qu'on a déjà vu, donc aussi $-(-nx) = nx$; ainsi, on a déjà l'inclusion $n\mathbf{Z} \subset I$. Il reste à établir l'inclusion opposée. Pour cela considérons un élément $x \in I$, et écrivons (division euclidienne)

$$x = nq + r \quad (0 \leqslant r < n);$$

le sous-groupe I contient n, donc nq, et comme il contient x il contient aussi $x - nq = r$; or r est positif ou nul, et strictement inférieur à n; si l'on avait $r \neq 0$, n ne serait pas le *plus petit* entier strictement positif contenu dans I; c'est donc que $r = 0$, et ceci démontre que tout élément de I est un multiple de n, autrement dit que $I \subset n\mathbf{Z}$; on a donc bien en définitive $I = n\mathbf{Z}$.

Pour établir l'unicité de n, il est suffisant de montrer que si l'on a $p\mathbf{Z} = q\mathbf{Z}$ avec p, $q \geqslant 0$, alors $p = q$; mais comme $q\mathbf{Z}$ contient q, l'hypothèse faite montre que q est multiple de p — et aussi que p est multiple de q — d'où évidemment $p = q$.

Le fait que tout sous-groupe de $\mathbf{Z}$ soit de la forme $n\mathbf{Z}$ joue un rôle très important en Arithmétique et ailleurs et, dans bien des cas, remplace avantageusement les démonstrations fondées sur la théorie de la « division euclidienne » (ou « division avec reste ») des entiers.

Montrons par exemple comment ce résultat conduit aux principales propriétés des pgcd. Soient $x_1, \ldots, x_n$ des entiers non nuls; désignons par I l'ensemble des $x \in \mathbf{Z}$ tels qu'il existe $u_1, \ldots, u_n \in \mathbf{Z}$ vérifiant

$$x = u_1x_1 + \cdots + u_nx_n;$$

il est évident que I est un sous-groupe de $\mathbf{Z}$, et par suite $I = d\mathbf{Z}$ où d est un entier positif bien déterminé. Tout élément de I est un multiple de d; en particulier, $x_1, \ldots, x_n$ sont des multiples de d, qui est donc un diviseur commun aux nombres donnés; mais d'autre part, tout diviseur commun d' à $x_1, \ldots, x_n$ divise évidemment $u_1x_1 + \cdots + u_nx_n$ quels que soient les entiers $u_1, \ldots, u_n$, donc divise tout élément de I, et en particulier divise d. Autrement dit, d est le plus grand commun diviseur de $x_1, \ldots, x_n$, et on voit en même temps que celui-ci possède la propriété de pouvoir s'écrire sous la forme

$$d = u_1x_1 + \cdots + u_nx_n$$

pour des entiers u_i $(1 \leqslant i \leqslant n)$ convenablement choisis.

Notons, comme conséquence, le *théorème de Bezout : pour que* $x_1, \ldots, x_n$ *soient premiers entre eux, il faut et il suffit qu'il existe des entiers* $u_1, \ldots, u_n$ *tels que*

$$u_1x_1 + \cdots + u_nx_n = 1.$$

En effet, avec les notations ci-dessus, cette condition exprime que le sous-groupe I contient le nombre 1; or pour exprimer que les x_i sont premiers entre eux, i.e. que $d = 1$, il suffit évidemment d'exprimer que 1 est un multiple de d, i.e. que $1 \in I$, d'où le résultat annoncé.

On obtiendrait de même la théorie du ppcm en considérant le sous-groupe

$$x_1\mathbf{Z} \cap \cdots \cap x_n\mathbf{Z}$$

de $\mathbf{Z}$; si l'on note m son générateur positif, il est immédiat de vérifier que m est le ppcm des entiers x_i donnés.

Ces questions seront étudiés d'une façon plus détaillée et plus générale au § 3[1].

Exemple 9. La construction des sous-groupes $n\mathbf{Z}$ de $\mathbf{Z}$ se généralise comme suit. Soient G un groupe (que nous notons maintenant multiplicativement, car il serait inutile de supposer G commutatif pour ce qui va suivre) et x un élément de G; pour tout entier rationnel p, définissons x^p comme suit :

$$x^p = \begin{cases} x \ldots x \ (p \text{ facteurs}) & \text{si } p \geqslant 1 \\ e \ (\text{élément neutre}) & \text{si } p = 0 \\ (x^{-1})^{-p} & \text{si } p < 0. \end{cases}$$

A l'aide de l'associativité de la multiplication dans G, on vérifie facilement les règles de calcul suivantes :

$$x^p x^q = x^{p+q}; \qquad (x^p)^{-1} = x^{-p}; \qquad (x^p)^q = x^{pq}.$$

Il s'ensuit que l'ensemble des x^p (pour x donné, et p variable dans $\mathbf{Z}$), est un sous-groupe de G : en effet, il n'est évidemment pas vide, et s'il contient des éléments $u = x^p$, $v = x^q$, la formule $uv^{-1} = x^{p-q}$ montre qu'il contient aussi uv^{-1}.

Ce sous-groupe s'appelle le **sous-groupe de G engendré par x** (de sorte que, dans le groupe additif $\mathbf{Z}$, $n\mathbf{Z}$ n'est autre que le sous-groupe engendré par n), et ses éléments s'appellent **les puissances de x**.

Lorsque G est écrit additivement, on utilise, au lieu de la notation x^p, la notation px, et on dit que les px sont **les multiples entiers de x**. On a donc par définition

$$px = \begin{cases} x + \cdots + x \ (p \text{ facteurs}) & \text{si } p \geqslant 1 \\ 0 \ (\text{élément neutre} & \text{si } p = 0 \\ (-p) \ (-x) & \text{si } p < 0, \end{cases}$$

avec les formules

$$px + qx = (p + q)x, \qquad -(px) = (-p)x, \qquad p(qx) = (pq)x.$$

Remarque 1. Dans un groupe additif on a aussi la relation

$$px + py = p(x + y)$$

quels que soient les éléments x et y du groupe considéré. Dans un groupe quelconque G (donc noté multiplicativement), la formule analogue

$$x^p y^p = (xy)^p$$

est fausse sauf si x et y **commutent** (ou **permutent**, comme on dit encore), i.e. si l'on a

$$xy = yx.$$

Tout d'abord, si $xy = yx$, on a

$$(xy)^2 = xyxy = xxyy = x^2y^2$$

et ainsi de suite. Inversement, si la relation $(xy)^p = x^py^p$ est vraie pour $p = 2$, il vient $xyxy = xxyy$; en multipliant les deux membres à gauche par x^{-1} et à droite par y^{-1}, il vient $x^{-1}xyxyy^{-1} = x^{-1}xxyyy^{-1}$, ce qui s'écrit $xy = yx$ comme prévu.

Remarque 2. On appelle **groupe cyclique** tout groupe G pour lequel il existe un $x \in G$ tel que tout élément de G soit une puissance de x; on dit alors que x est un **générateur** de G. Le groupe additif $\mathbf{Z}$ est cyclique, et admet pour générateur soit 1, soit -1. Il existe des groupes cycliques qui sont finis (considérer un groupe fini G et le sous-groupe de G engendré par un élément quelconque de G); on verra plus loin qu'on peut décrire entièrement leur structure.

4. *Intersection de sous-groupes; générateurs*

On a le résultat suivant :

THÉORÈME 1. *Soit $(H_i)_{i \in I}$ une famille de sous-groupes d'un groupe G. Alors l'intersection des H_i est encore un sous-groupe de G. Pour que la réunion des H_i soit aussi un sous-groupe de G, il suffit que, quels que soient les indices $i, j \in I$, il existe un indice $k \in I$ tel que l'on ait*

$$H_i, \ H_j \subset H_k.$$

Soit M l'intersection des H_i; elle n'est pas vide (puisque l'élément neutre de G appartient à tous les H_i, donc aussi à M); si M contient deux éléments x et y, ceux-ci appartiennent à H_i pour tout i, de sorte qu'il en est de même de xy^{-1}, qui appartient donc aussi à M; donc M est un sous-groupe de G.

Soit maintenant U la réunion des H_i; elle est évidemment non vide; soient x, y deux éléments de U; il existe des indices i, $j \in I$ tels que l'on ait $x \in H_i$, $y \in H_j$; d'après l'hypothèse faite dans l'énoncé, il existe donc un indice k tel que H_k contienne *à la fois* x et y, donc aussi xy^{-1}; il s'ensuit que xy^{-1} appartient à la réunion U, ce qui achève la démonstration.

Soit B une partie d'un groupe G; il existe des sous-groupes de G qui contiennent B (par exemple, G lui-même); l'intersection de tous ces sous-groupes est encore un sous-groupe d'après le Théorème 1, et contient encore B, tout en étant contenue, par construction même, dans tout sous-groupe de G contenant B. Ce sous-groupe intersection est donc le « plus petit » de tous les sous-groupes de G contenant B; on dit que c'est **le sous-groupe de G engendré par B**.

Supposons par exemple B réduit à un seul élément x; un sous-groupe contenant x contient évidemment toutes les puissances de x (définies dans l'Exemple 9 ci-dessus);

or celles-ci forment un sous-groupe de G contenant x et donc aussi B. On voit donc qu'ici le plus petit sous-groupe de G contenant B est le sous-groupe formé par les puissances de x, i.e. le sous-groupe de G engendré par x au sens de l'*Exemple* 9 ci-dessus.

Dans le cas d'une partie quelconque B de G, on peut construire le sous-groupe engendré par B par une méthode analogue à celle de l'*Exemple* 9 :

THÉORÈME 2. *Soit* B *une partie d'un groupe* G. *Pour qu'un* $x \in G$ *appartienne au sous-groupe de* G *engendré par* B, *il faut et il suffit qu'il existe un entier* $p \geqslant 0$ *et des éléments* $x_1, \cdots, x_p \in G$ *possédant les propriétés suivantes :*

a) on a la relation

$$x = x_1 \cdots x_p;$$

b) pour chaque i $(1 \leqslant i \leqslant p)$ *on a soit* $x_i \in B$, *soit* $x_i^{-1} \in B$.

Remarque 3. Pour $p = 0$ on doit par convention interpréter la relation figurant dans l'assertion *a*) de l'énoncé comme signifiant $x = e$ (d'une manière générale dans un groupe on convient d'attribuer un sens à la notion de **produit vide** ou **produit de zéro facteur** en déclarant qu'un tel produit n'est autre que l'élément neutre du groupe. Cette convention est nécessaire pour assurer la validité de certains énoncés).

Pour démontrer le Théorème 2, considérons l'ensemble H des $x \in G$ qui satisfont aux conditions de l'énoncé : tout revient à prouver que H est un sous-groupe, contient B, et est contenu dans tout sous-groupe contenant B.

La dernière de ces trois assertions est évidente : si un sous-groupe contient B, il contient évidemment les x_i de l'assertion *b*), donc l'élément x figurant dans l'assertion *a*) de l'énoncé.

Le fait que H contienne B est non moins clair : un élément x de B vérifie en effet les conditions *a*) et *b*), comme on le voit en prenant $p = 1$ et $x_1 = x$.

Il reste à prouver que H est un sous-groupe. Tout d'abord, H contient l'élément neutre d'après la *Remarque* 3 ci-dessus. Soient maintenant x et y deux éléments de H; on peut donc écrire

$$x = x_1 \cdots x_p, \qquad y = y_1 \cdots y_q,$$

avec

$$x_i \in B \text{ ou } x_i^{-1} \in B \quad \text{pour tout } i$$
$$y_j \in B \text{ ou } y_j^{-1} \in B \quad \text{pour tout } j;$$

on a alors

$$x y^{-1} = (x_1 \cdots x_p).(y_1 \cdots y_q)^{-1} = x_1 \cdots x_p y_q^{-1} \cdots y_1^{-1}$$

d'après le § 6, Théorème 3, et on a ainsi décomposé l'élément $x y^{-1}$ de G en un produit

$$x y^{-1} = z_1 \cdots z_{p+q}$$

avec

$$z_k \in B \text{ ou } z_k^{-1} \in B \quad \text{pour tout } k,$$

ce qui prouve que $x y^{-1} \in H$. Par suite, H est un sous-groupe de G, et le Théorème est démontré.

Lorsque le sous-groupe de G engendré par une partie B de G est G tout entier, on dit que B est un **ensemble de générateurs de** G. Si G admet un ensemble fini de générateurs (i.e. s'il existe une partie *finie* B de G qui engendre G), on dit que G est un **groupe à engendrement fini**, ou un **groupe de type fini** — il est clair par exemple que tout groupe cyclique est de type fini.

Soient G un groupe *commutatif de type fini*, et $B = \{a_1, \cdots, a_n\}$ un ensemble fini de générateurs de G. Appliquons le Théorème 2 : tout $x \in G$ admet alors une décomposition

$$x = x_1 \cdots x_p, \quad \text{avec} \quad x_i \in B \quad \text{ou} \quad x_i^{-1} \in B \quad \text{pour tout } i;$$

chacun des facteurs de cette décomposition est donc soit l'un des a_j, soit l'un des éléments a_j^{-1}. Mais comme G est commutatif, on peut grouper ensemble tous ceux des x_i qui, pour un indice j donné, sont égaux soit à a_j soit à a_j^{-1}; le produit de ces x_i est évidemment une puissance de a_j, et finalement on a une décomposition de x de la forme

$$x = a_1^{r_1} \ldots a_n^{r_n}$$

avec des entiers rationnels $r_1, \ldots, r_n$.

Il est clair inversement que si tout $x \in G$ peut s'écrire sous la forme précédente, alors G est de type fini et engendré par les éléments $a_1, \ldots, a_n$.

Exemple 10. *Le groupe additif* $\mathbf{Z}^n$ *est de type fini*, et admet pour ensemble de générateurs les éléments

$$e_1 = (1, 0, \ldots, 0), \qquad e_2 = (0, 1, 0, \ldots, 0), \qquad e_n = (0, \ldots, 0, 1)$$

de ce groupe. En effet, si $r_1, r_2, \ldots, r_n$ sont des entiers quelconques, on a immédiatement les formules

$$r_1 e_1 = (r_1, 0, \ldots, 0)$$
$$r_2 e_2 = (0, r_2, \ldots, 0)$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$r_n e_n = (0, 0, \ldots, r_n)$$

et par suite

$$r_1 e_1 + r_2 e_2 + \cdots + r_n e_n = (r_1, r_2, \ldots, r_n),$$

ce qui montre bien que tout élément de $\mathbf{Z}^n$ est un produit (i.e. une somme) de puissances (i.e. de multiples) des éléments $e_1, \ldots, e_n$.

Par contre, *le groupe additif* $\mathbf{Q}$ *des nombres rationnels n'est pas de type fini*. Supposons-le en effet engendré par des nombres rationnels

$$a_1 = p_1/q_1, \ \ldots, \ a_n = p_n/q_n$$

en nombre fini; cela voudrait dire que, pour *tout* nombre rationnel x, il existe des *entiers* $r_1, \ldots, r_n$ tels que

$$x = r_1 a_1 + \cdots + r_n a_n;$$

mais il est clair qu'alors on pourrait écrire x sous forme d'une fraction ayant pour dénominateur $q_1 \dots q_n$ (ou plus généralement n'importe quel dénominateur commun à $a_1, \dots, a_n$); autrement dit, il serait possible de « réduire au même dénominateur » *tous* les nombres rationnels *à la fois*, ce qui est visiblement (*) absurde !

5. *Permutations et transpositions*

Considérons le groupe $\mathfrak{S}_n$ des permutations de l'ensemble

$$I_n = \{1, 2, \dots, n\};$$

on dit qu'une permutation $t \in \mathfrak{S}_n$ est une **transposition** s'il existe un entier i, vérifiant $1 \leqslant i \leqslant n-1$, tel qu'on ait les relations suivantes :

$$t(i) = i+1, \qquad t(i+1) = i, \qquad t(k) = k \quad \text{pour} \quad k \neq i,\ i+1.$$

THÉORÈME 3. *Le groupe $\mathfrak{S}_n$ est engendré par les transpositions qu'il contient.*

On va en fait montrer que toute permutation $s \in \mathfrak{S}_n$ est un produit de transpositions, en raisonnant par récurrence sur n (le cas $n = 1$ est trivial puisque le groupe $\mathfrak{S}_n$ se réduit alors à son élément neutre).

Considérons donc une permutation $s \in \mathfrak{S}_n$, et posons $s(n) = i$. Désignant par t_j la transposition qui échange j et $j+1$, il est clair que la permutation

$$u = t_{n-1} \circ \cdots \circ t_i \circ s$$

vérifie $u(n) = n$, et que l'on a

$$s = t_i^{-1} \circ \cdots \circ t_{n-1}^{-1} \circ u = t_i \circ \cdots \circ t_{n-1} \circ u$$

en vertu du fait que

$$t^{-1} = t$$

pour toute transposition. Pour montrer que s est un produit de transpositions, il suffit donc de l'établir pour u, i.e. pour une permutation vérifiant $u(n) = n$.

Mais cette relation montre que u permute les éléments $1, 2, \dots, n-1$ de I_n, autrement dit que u « induit » dans I_{n-1} une permutation $u' \in \mathfrak{S}_{n-1}$; celle-ci, d'après l'hypothèse de récurrence, peut s'écrire

$$u' = v_1 \circ \cdots \circ v_q$$

où $v_1, \dots, v_q$ sont des transpositions dans le groupe $\mathfrak{S}_{n-1}$. Définissons alors des permutations $w_1, \dots, w_q$ de I_n en posant

$$w_j(x) = \begin{cases} v_j(x) & \text{si} \quad x \in I_{n-1} \\ n & \text{si} \quad x = n; \end{cases}$$

(*) On conseille néanmoins au lecteur de *démontrer* cette assertion.

comme u et u' coïncident sur I_{n-1}, et comme $u(n) = n$, il est clair que

$$u = w_1 \circ \cdots \circ w_q;$$

mais comme les v_j sont des transpositions de I_{n-1}, les w_j sont évidemment des transpositions de I_n. Donc, dans le groupe $\mathfrak{S}_n$, la permutation u est un produit de transpositions, ce qui achève la démonstration.

6. *Classes modulo un sous-groupe*

Soient G un groupe et H un sous-groupe de G; alors *la relation*

$$R\{x, y\} : x^{-1}y \in H$$

est une relation d'équivalence sur l'ensemble G au sens du § 4, n° 1. Il est clair, tout d'abord, que la relation $R\{x, x\}$ est toujours vraie, puisqu'elle signifie que H contient l'élément neutre de G; d'autre part, pour montrer que $R\{x, y\}$ implique $R\{y, x\}$, on observe que, par définition d'un sous-groupe, la relation

$$x^{-1}y \in H \qquad \text{implique} \qquad (x^{-1}y)^{-1} \in H, \quad \text{i.e. } y^{-1}x \in H;$$

enfin, des relations $R\{x, y\}$ et $R\{y, z\}$, i.e. des relations

$$x^{-1}y \in H \qquad \text{et} \qquad y^{-1}z \in H,$$

résulte par définition d'un sous-groupe la relation

$$(x^{-1}y)\,(y^{-1}z) \in H \quad \text{i.e. } x^{-1}z \in H,$$

i.e. la relation $R\{x, z\}$.

La relation considérée est donc bien une relation d'équivalence sur l'ensemble G. Nous allons construire les classes d'équivalence F_x correspondantes (§ 4, n° 2). Pour $x \in G$, l'ensemble F_x est par définition formé des $y \in G$ tels que la relation $R\{x, y\}$ soit vraie, autrement dit des y tels que l'on ait $x^{-1}y \in H$; posant $x^{-1}y = z$ il vient $y = xz$, et dire que $R\{x, y\}$ est vraie signifie que $z \in H$. Ainsi, F_x *est l'ensemble des éléments de* G *de la forme* xz *avec* $z \in H$; pour cette raison, on utilise au lieu de F_x la notation

$$xH$$

et on dit que l'ensemble xH est une **classe à droite modulo** H (on définit de même les **classes à gauche modulo** H : ce sont les parties de G de la forme Hx, où Hx désigne l'ensemble des éléments de la forme zx, avec $z \in H$). L'ensemble des classes xH (resp. Hx) modulo H, i.e. le quotient de l'ensemble G par la relation d'équivalence $x^{-1}y \in H$ (resp. $yx^{-1} \in H$), se note G/H (resp. H\G).

Exemple 11. Prenons pour G le groupe additif $\mathbf{Z}$ des entiers rationnels et pour H le sous-groupe $p\mathbf{Z}$ formé des multiples d'un entier p donné; alors la relation

R $\{x, y\}$ s'écrit (on est maintenant en notation additive)

$$y - x \in p\mathbf{Z} \quad \text{i.e.} \quad x \equiv y \pmod{p},$$

et on retrouve l'*Exemple* 4 du § 4, les classes modulo le sous-groupe $p\mathbf{Z}$ étant ici par conséquent les classes de congruence modulo p définies au § 4, *Exemple* 9.

On notera à ce sujet qu'au § 4 on a défini une « addition » sur l'ensemble $\mathbf{Z}/p\mathbf{Z}$, laquelle vérifie la relation

$$\theta(x + y) = \theta(x) + \theta(y)$$

quels que soient $x, y \in \mathbf{Z}$ (on note θ l'application canonique de $\mathbf{Z}$ sur $\mathbf{Z}/p\mathbf{Z}$). On peut facilement montrer (cf. § 8, n° 3) que l'ensemble $\mathbf{Z}/p\mathbf{Z}$, muni de cette loi de composition, est un *groupe* (groupe additif des entiers modulo p). Voir une construction plus générale dans l'*Exercice* 16 de ce §.

On remarquera que, pour toute classe xH modulo H, il existe une *bijection* de H sur xH, à savoir l'application $z \mapsto xz$ (cette application est surjective par définition des classes, et injective parce que tout $x \in$ G est inversible, de sorte que le Théorème 4 du § 6 s'applique). Si en particulier G est un groupe fini, auquel cas il en est de même de H, on voit donc que chaque classe xH comporte autant d'éléments que H. Or les classes xH forment une partition de l'ensemble G; donc (§ 5, Théorème 7) le nombre d'éléments de G est égal au nombre d'éléments de H multiplié par le nombre de classes xH distinctes. Par suite :

THÉORÈME 4. *Soient* G *un groupe fini et* H *un sous-groupe de* G. *On a alors la relation*

$$\text{Card (G)} = \text{Card (G/H)} . \text{Card (H)}.$$

Remarque 4. Le nombre Card (G) d'éléments d'un groupe fini G s'appelle traditionnellement **l'ordre de** G (donc un « groupe fini d'ordre 5 » n'est autre qu'un groupe possédant 5 éléments). D'autre part, le nombre Card (G/H), noté aussi parfois (G : H), et qui figure dans l'énoncé du Théorème 4 s'appelle **l'indice de** H **dans** G; on peut montrer facilement qu'il est aussi égal au nombre de classes Hx distinctes dans G.

Le Théorème 4 montre, en particulier, que *l'ordre de* H *est un diviseur de l'ordre de* G. On va donner une importante application de ce résultat.

THÉORÈME 5. *Soit* G *un groupe fini d'ordre* n. *On a alors*

$$x^n = e$$

pour tout $x \in$ G.

Soit en effet H le sous-groupe de G engendré par x, et soit r = Card (H); comme n est un multiple de r, il suffit pour établir le Théorème de prouver que $x^r = e$. Autrement dit, il suffit de prouver le Théorème 5 dans le cas où G est engendré par x, ce que nous supposerons donc dans ce qui suit.

Considérons alors l'application $f : \mathbf{Z} \to$ G donnée par

$$f(q) = x^q;$$

elle est *surjective* par hypothèse. Les règles de calcul sur les puissances (*Exemple* 9) montrent qu'on a les relations

$$f(0) = e, \qquad f(q' - q'') = f(q') f(q'')^{-1};$$

de ces relations résulte aussitôt que les $q \in \mathbf{Z}$ tels que $f(q) = e$ forment un *sous-groupe* de $\mathbf{Z}$, donc de la forme $s\mathbf{Z}$ où s est un entier positif bien déterminé.

De plus, la relation $f(q') = f(q'')$, qui équivaut évidemment à

$$f(q') f(q'')^{-1} = e,$$

s'écrit aussi d'après ce qui précède sous la forme $f(q' - q'') = e$, et équivaut donc à

$$q' - q'' \in s\mathbf{Z}, \quad \text{i.e. à} \quad q' \equiv q'' \pmod{s}.$$

Comme f est *surjective*, G possède donc autant d'éléments qu'il y a de classes modulo s dans $\mathbf{Z}$; autrement dit, s n'est autre que le nombre d'éléments de G, et comme on a $x^s = e$ le Théorème est démontré.

7. *Nombre de permutations de n objets*

On a établi, au § 5 (Corollaire du Théorème 9), le résultat suivant :

THÉORÈME. *Soit* X *un ensemble fini à* n *éléments. Alors le groupe* $\mathfrak{S}(X)$ *des permutations de* X *est d'ordre*

$$n! = 1.2 \ldots n.$$

Nous allons donner ici de ce résultat une démonstration qui, sans différer essentiellement de celle du § 5, fait plus systématiquement usage de la structure de groupe existant sur l'ensemble $\mathfrak{S}(X)$.

Le Théorème est clair si $n = 1$, et on va le démontrer par récurrence sur n, autrement dit prouver que s'il est vrai pour l'entier $n - 1$ il l'est aussi pour l'entier n.

Choisissons pour cela une fois pour toutes un élément a de X, et soit

$$Y = X - \{a\}$$

l'ensemble obtenu en ôtant de X l'élément a; Y est un ensemble à $n - 1$ éléments, auquel le Théorème 6 est donc applicable (hypothèse de récurrence).

D'autre part, on peut considérer le groupe $\mathfrak{S}(Y)$ comme un sous-groupe de $\mathfrak{S}(X)$; il suffit pour cela d'associer à toute permutation s de l'ensemble Y la permutation $\bar{s}$ de X donnée par

$$\bar{s}(x) = \begin{cases} s(x) & \text{si} \quad x \in Y \\ a & \text{si} \quad x = a; \end{cases}$$

de cette façon, $\mathfrak{S}(Y)$ *s'identifie au sous-groupe de* $\mathfrak{S}(X)$ *formé des permutations de* X *qui admettent a pour point fixe.*

D'après l'hypothèse de récurrence, le groupe $\mathfrak{S}(Y)$ possède $(n-1)!$ éléments; pour en déduire que $\mathfrak{S}(X)$ en possède $n!$, i.e. n fois plus, il suffit donc (Théorème 4) de prouver que, dans $\mathfrak{S}(X)$, les classes modulo $\mathfrak{S}(Y)$ sont au nombre de n exactement.

Pour cela, introduisons l'application $f: \mathfrak{S}(X) \to X$ donnée par

$$f(s) = s(a) \quad \text{pour tout} \quad s \in \mathfrak{S}(X).$$

Étant données des permutations s et t de X, la relation $f(s) = f(t)$ s'écrit

$$s(a) = t(a), \quad \text{i.e. } a = s^{-1}t(a),$$

et par suite signifie que

$$s^{-1}t \in \mathfrak{S}(Y),$$

i.e. que s et t appartiennent à la même classe à droite modulo le sous-groupe $\mathfrak{S}(Y)$. Utilisant le Théorème 2 du § 4 on voit donc que le nombre de classes modulo $\mathfrak{S}(Y)$ est égal au nombre d'éléments de l'image de $\mathfrak{S}(X)$ par f, i.e. au nombre d'éléments $x \in X$ pour lesquels il existe une permutation s de X telle que $x = s(a)$; mais il est clair que *tout* $x \in X$ peut s'écrire $x = s(a)$ pour une permutation convenable s; par suite, les classes modulo $\mathfrak{S}(Y)$ dans $\mathfrak{S}(X)$ sont au nombre de n, et ceci termine la démonstration du Théorème.

8. Homomorphismes de groupes

Étant donnés des groupes G et H, on appelle **homomorphisme de G dans H** toute application f de G dans H telle que l'on ait

$$f(xy) = f(x)f(y) \quad \text{quels que soient} \quad x, y \in G.$$

Faisant $y = e$ dans la relation précédente, on trouve $f(x) = f(x)f(e)$ et par suite

$$f(e) = e.$$

Enfin, en prenant $y = x^{-1}$, et en tenant compte du résultat qu'on vient d'obtenir, on trouve évidemment que

$$f(x^{-1}) = f(x)^{-1} \quad \text{pour tout} \quad x \in G.$$

Remarque 5. La définition donnée plus haut suppose les groupes G et H écrits multiplicativement, et doit être modifiée en conséquence si G ou H ou G et H sont notés additivement. Par exemple, si G est noté additivement et H multiplicativement, un homomorphisme est une application f de G dans H vérifiant

$$f(x+y) = f(x)f(y) \quad \text{quels que soient} \quad x, y \in G.$$

Exemple 12. Prenons pour G le groupe additif **Z** des entiers rationnels et pour H un groupe (multiplicatif) arbitraire. Pour tout $a \in H$, l'application f donnée par

$$f(n) = a^n \quad \text{pour tout} \quad n \in \mathbf{Z}$$

est un homomorphisme : cela résulte des formules de l'*Exemple* 9. En outre, *tout* homomorphisme f de **Z** dans H s'obtient par la méthode en question. En effet, pour un tel homomorphisme, posons

$$f(1) = a;$$

on a alors

$$f(2) = f(1+1) = f(1)f(1) = aa = a^2,$$
$$f(3) = f(2+1) = f(2)f(1) = a^2a = a^3,$$

etc, d'où $f(n) = a^n$ pour n positif, puis, pour n négatif,

$$f(n) = f(-n)^{-1} = (a^{-n})^{-1} = a^n,$$

de sorte que la relation $f(n) = a^n$ est valable pour tout $n \in \mathbf{Z}$.

Exemple 13. Pour tout entier p, l'application canonique de **Z** sur $\mathbf{Z}/p\mathbf{Z}$ est un homomorphisme du groupe additif **Z** sur le groupe additif $\mathbf{Z}/p\mathbf{Z}$.

Exemple 14. La formule

$$\log(xy) = \log(x) + \log(y)$$

montre que la fonction logarithmique, définie en Analyse, est un homomorphisme du groupe multiplicatif $\mathbf{R}_+^*$ dans le groupe additif **R**.

THÉORÈME 6. *Soient* $f: M \to N$ *et* $g: N \to P$ *des homomorphismes de groupes; alors l'application composée* $g \circ f: M \to P$ *est encore un homomorphisme. Si un homomorphisme de groupes* $f: M \to N$ *est bijectif, l'application réciproque* $f^{-1}: N \to M$ *est encore un homomorphisme.*

Pour établir la première assertion, il suffit d'observer que, pour $x, y \in M$, on a

$$g \circ f(xy) = g[f(xy)] = g[f(x)f(y)] = g[f(x)] \cdot g[f(y)].$$

Pour établir la seconde, autrement dit que

$$f^{-1}(uv) = f^{-1}(u)f^{-1}(v)$$

pour $u, v \in N$, on remarque qu'il suffit (puisque f est bijectif, et en particulier injectif) d'établir que les images par f des deux membres de cette relation sont égales. Autrement dit, tout revient à prouver que

$$f[f^{-1}(uv)] = f[f^{-1}(u)f^{-1}(v)];$$

or le premier membre est égal à uv par définition de f^{-1}; le second membre, puisque f est un homomorphisme, est égal à

$$f[f^{-1}(u)] \cdot f[f^{-1}(v)] = uv,$$

ce qui termine la démonstration.

Soient G et H deux groupes; on appelle **isomorphisme de G sur H** tout homomorphisme *bijectif* de G sur H, et on dit que G et H sont **isomorphes** lorsqu'il existe un isomorphisme de G sur H.

Exemple 15. En utilisant comme dans l'*Exemple* 14 la fonction logarithmique, on voit que les groupes $\mathbf{R}_+^*$ et $\mathbf{R}$ sont isomorphes.

La relation

G et H sont isomorphes

est une *relation d'équivalence*; en effet, G et G sont isomorphes quel que soit G, car l'application identique est évidemment un isomorphisme de G sur G; d'autre part, s'il existe un isomorphisme f d'un groupe G sur un groupe H, alors il existe aussi un isomorphisme de H sur G, à savoir f^{-1}; enfin ,s'il existe un isomorphisme f d'un groupe M sur un groupe N, et un isomorphisme g de N sur un troisième groupe P, il existe aussi un isomorphisme de M sur P — à savoir $g \circ f$, qui est un homomorphisme d'après le Théorème 6, et est bijectif puisque f et g le sont.

On appelle **automorphisme d'un groupe** G tout isomorphisme de G sur G.

Exemple 16. Soit G un groupe noté multiplicativement; alors, pour tout $a \in G$, l'application f de G dans G donnée par

$$f(x) = axa^{-1}$$

est un automorphisme de G. On a en effet

$$\begin{aligned} f(x)f(y) &= (axa^{-1})(aya^{-1}) = (ax)(aa^{-1})(ya^{-1}) \\ &= (ax)e(ya^{-1}) = (ax)(ya^{-1}) = a(xy)a^{-1} = f(xy), \end{aligned}$$

de sorte que f est un homomorphisme; de plus, pour tout $y \in G$, l'équation $axa^{-1} = y$ admet une et une seule solution $x = a^{-1}ya$, ce qui montre que f est bijectif.

Les automorphismes de G obtenus par la méthode qu'on vient de décrire s'appellent les **automorphismes intérieurs** du groupe G. Cette notion n'a évidemment d'intérêt que pour les groupes non commutatifs.

Exemple 17. Considérons le groupe multiplicatif $\mathbf{R}_+^*$ des nombres réels strictement positifs; alors, pour tout nombre réel α non nul la fonction

$$f(x) = x^\alpha,$$

définie en Analyse, est un automorphisme du groupe $\mathbf{R}_+^*$; l'automorphisme réciproque est

$$f^{-1}(x) = x^{1/\alpha}.$$

Remarque 6. Dans la pratique, on considère souvent deux groupes isomorphes G et H comme identiques; plus exactement, et dans la mesure où l'on se place au point de vue de la pure théorie des groupes, G et H possèdent exactement les mêmes propriétés; par exemple, si G est commutatif, il en est de même de H; si G est engendré par n éléments, il en est de même de H; et d'une manière générale, une fois qu'on a choisi un isomorphisme f de G sur H, on peut « traduire » toute relation entre éléments de G en une relation analogue entre les éléments de H obtenus en appliquant f aux éléments considérés de G.

On notera que la fonction logarithmique, isomorphisme du groupe multiplicatif $\mathbf{R}_+^*$ sur le groupe additif $\mathbf{R}$, a justement été inventée pour transformer toute relation multiplicative entre nombres positifs en une relation additive entre nombres de signe quelconque...

9. *Noyau et image d'un homomorphisme*

Établissons d'abord le résultat suivant :

THÉORÈME 7. *Soit f un homomorphisme d'un groupe* G *dans un groupe* H. *L'image par f de tout sous-groupe de* G *est un sous-groupe de* H. *L'image réciproque par f de tout sous-groupe de* H *est un sous-groupe de* G.

Soient G' un sous-groupe de G et $H' = f(G')$ son image; si $u, v \in H'$, il existe $x, y \in G'$ tels que $u = f(x)$, $v = f(y)$; on a alors

$$uv^{-1} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}),$$

et comme $xy^{-1} \in G'$ il s'ensuit que $uv^{-1} \in H'$; ceci établit la première assertion de l'énoncé. La seconde se démontre par des raisonnements analogues, qu'on laisse au lecteur le soin de détailler.

Il résulte du Théorème 7 que, si f est un homomorphisme de G dans H, alors $f(G)$ est un sous-groupe de H; on l'appelle l'**image de** f, et on le note

$$\mathrm{Im}(f);$$

de même, l'ensemble $f^{-1}(\{e\})$, formé des $x \in G$ tels que

$$f(x) = e,$$

est un sous-groupe de G; on l'appelle le **noyau de** f, et on le désigne par la notation

$$\mathrm{Ker}(f)$$

(le mot « noyau » se traduit par « kernel » en anglais, et par « Kern » en allemand).

Exemple 18. Soient G un groupe multiplicatif, a un élément de G, et considérons l'homomorphisme $f: \mathbf{Z} \to G$ donné par $f(n) = a^n$. Alors l'image de f est le sous-groupe de G engendré par a; et le noyau de f est le sous-groupe de $\mathbf{Z}$ formé des entiers n tels que $a^n = e$ (le fait que ces entiers forment un sous-groupe a déjà été établi et utilisé dans la démonstration du Théorème 5).

Remarque 7. Soit N le noyau d'un homomorphisme $f: G \to H$; pour $x \in N$ et $a \in G$ on a

$$f(axa^{-1}) = f(a)f(x)f(a)^{-1} = f(a)ef(a)^{-1} = f(a)f(a)^{-1} = e;$$

par suite, on a

$$axa^{-1} \in N \text{ quels que soient } a \in G \text{ et } x \in N;$$

un sous-groupe d'un groupe G est dit **invariant** (ou **normal**, ou **distingué**) lorsqu'il possède la propriété précédente; cela signifie évidemment qu'on a

$$s(N) \subset N$$

pour tout automorphisme intérieur s de G.

On voit donc que *le noyau d'un homomorphisme est un sous-groupe invariant* Réciproquement, on peut démontrer que, si N est un sous-groupe invariant d'un groupe G, il existe un groupe H et un homomorphisme f de G dans H tel que N soit le noyau de f; cf. *Exercice* 16.

Lorsque G est commutatif, il va de soi que tout sous-groupe de G est invariant.

THÉORÈME 8. *Soient* G *et* H *deux groupes et f un homomorphisme de* G *dans* H. *Pour que f soit injectif, il faut et il suffit que son noyau soit réduit à l'élément neutre.*

Comme $f(e) = e$, la relation $f(x) = e$ signifie que $f(x) = f(e)$; si f est injectif elle implique donc $x = e$, autrement dit $\mathrm{Ker}(f) = \{e\}$. Supposons inversement le noyau de f réduit à e; la relation $f(x) = f(y)$ s'écrit encore

$$f(x)f(y)^{-1} = e,$$

ou, puisque f est un homomorphisme, $f(xy^{-1}) = e$, et par suite signifie que

$$xy^{-1} \in \mathrm{Ker}(f);$$

comme $\mathrm{Ker}(f) = \{e\}$, il vient donc $xy^{-1} = e$, autrement dit $x = y$, et f est injectif, ce qui achève la démonstration.

THÉORÈME 9. *Soient* G, H *et* M *trois groupes, $p : G \to H$ et $f : G \to M$ des homomorphismes; on suppose p surjectif. Les conditions suivantes sont alors équivalentes :*

a) il existe un homomorphisme $f' : H \to M$ tel que $f = f' \circ p$;

b) on a la relation $\mathrm{Ker}(p) \subset \mathrm{Ker}(f)$.

Si ces conditions sont réalisées, l'homomorphisme f' est unique; il est injectif si et seulement si $\mathrm{Ker}(p) = \mathrm{Ker}(f)$, *et surjectif si et seulement si f est surjectif.*

Cherchons d'abord à quelle condition il existe une application f' de H dans M telle que $f = f' \circ p$; la réponse est donnée par le Théorème 1 du § 2 : tout revient à vérifier que la relation $p(x) = p(y)$ implique la relation $f(x) = f(y)$. Or, comme p est un homomorphisme, la première s'écrit

$$e = p(x)p(y)^{-1} = p(xy^{-1}),$$

autrement dit $xy^{-1} \in \mathrm{Ker}(p)$; et pour la même raison la seconde relation s'écrit $xy^{-1} \in \mathrm{Ker}(f)$; prenant $y = e$ on voit que la relation $x \in \mathrm{Ker}(p)$ doit impliquer la relation $x \in \mathrm{Ker}(f)$, ce qui exige $\mathrm{Ker}(p) \subset \mathrm{Ker}(f)$, et cette condition est évidemment suffisante.

Ainsi, la condition *b*) équivaut à l'existence d'une application f' telle que $f = f' \circ p$. Cette application est nécessairement un homomorphisme; soient en effet $u, v \in H$; puisque p est surjectif, on peut écrire $u = p(x)$, $v = p(y)$ avec $x, y \in G$; alors

$$\begin{aligned} f'(uv) &= f'(p(x)p(y)) = f'(p(xy)) = f(xy) = f(x)f(y) \\ &= f'(p(x))f'(p(y)) = f'(u)f'(v), \end{aligned}$$

ce qui établit notre assertion.

L'équivalence des conditions *a*) et *b*) est donc établie.

L'unicité de f' est évidente; car, p étant surjectif, la relation

$$f'_1 \circ p = f'_2 \circ p \quad \text{implique} \quad f'_1 = f'_2.$$

Il est non moins clair que

$$f'(H) = f'(p(G)) = f(G),$$

et par suite que f' est surjective si et seulement si f l'est. Enfin, cherchons le noyau de f'; il est formé des $u \in H$ tels que $f'(u) = e$; posant $u = p(x)$, cela s'écrit encore $f(x) = e$, autrement dit $x \in \mathrm{Ker}(f)$; par suite, on a

$$\mathrm{Ker}(f') = p[\mathrm{Ker}(f)].$$

Pour que f' soit injective, il est donc nécessaire et suffisant (Théorème 8) que $p[\mathrm{Ker}(f)] = \{e\}$, autrement dit que $\mathrm{Ker}(f) \subset \mathrm{Ker}(p)$, autrement dit que

$$\mathrm{Ker}(f) = \mathrm{Ker}(p)$$

puisque la relation $\mathrm{Ker}(p) \subset \mathrm{Ker}(f)$ est déjà vérifiée. Ceci termine la démonstration.

10. *Application aux groupes cycliques*

Soient G un groupe cyclique et x un générateur de G: tout élément de G est donc une puissance de x. Autrement dit l'homomorphisme

$$f : \mathbf{Z} \to G$$

donné par

$$f(n) = x^n$$

est *surjectif*.

Désignons son noyau par I; c'est un sous-groupe de **Z**, par suite il existe un et un seul entier $p \geqslant 0$ tel que

$$I = p\mathbf{Z}$$

(cf. *Exemple* 8). Distinguons deux cas.

Tout d'abord, il peut arriver que $p = 0$; alors (Théorème 8) f est *injectif*, donc bijectif, et par suite est un *isomorphisme du groupe additif* **Z** *sur* G.

Supposons maintenant $p \neq 0$; considérons le groupe additif $\mathbf{Z}/p\mathbf{Z}$ (*Exemple* 11) et l'application canonique g de $\mathbf{Z}$ sur $\mathbf{Z}/p\mathbf{Z}$; c'est un homomorphisme surjectif, ayant pour noyau $p\mathbf{Z}$, de sorte que $\mathrm{Ker}(g) = \mathrm{Ker}(f)$. D'après le Théorème 9, il existe donc un et un seul homomorphisme

$$f' : \mathbf{Z}/p\mathbf{Z} \to \mathrm{G}$$

tel que $f = f' \circ g$ [ce qui signifie que, pour tout entier n, x^n est l'image par f' de la classe de n modulo p; l'existence de f' provient du fait que la relation

$$m \equiv n \pmod{p} \quad \text{implique} \quad x^m = x^n,$$

en sorte que x^n dépend, non pas de l'entier n, mais seulement de sa classe modulo p; bien entendu, ce raisonnement n'est autre qu'une traduction, dans le cas particulier qui nous intéresse, du raisonnement général utilisé dans la démonstration du Théorème 9]; comme f est surjectif, f' est surjectif; comme $\mathrm{Ker}(f) = \mathrm{Ker}(g)$, f' est injectif; par suite, f' est bijectif, et G *est isomorphe au groupe additif* $\mathbf{Z}/p\mathbf{Z}$ *des entiers modulo* p. En particulier, G a le même nombre d'éléments que celui-ci, i.e. a p éléments, ce qui caractérise l'entier p : c'est le nombre d'éléments de G. Donc :

THÉORÈME 10. *Tout groupe cyclique infini est isomorphe au groupe additif* $\mathbf{Z}$. *Tout groupe cyclique fini* G *est isomorphe au groupe additif* $\mathbf{Z}/p\mathbf{Z}$, *où* p *est le nombre d'éléments de* G.

On déduit évidemment de là que deux groupes cycliques sont isomorphes si et seulement s'ils ont le même nombre (fini ou non) d'éléments.

Soit x un élément d'un groupe G quelconque; on appelle *ordre de* x l'ordre (ou cardinal) du sous-groupe H de G engendré par x. Comme celui-ci est l'image de $\mathbf{Z}$ par l'homomorphisme $n \to x^n$, on voit qu'une condition nécessaire et suffisante pour que x soit d'ordre fini est qu'il existe un entier p *non nul* tel que

$$x^p = e;$$

l'ordre de x est alors le *plus petit* entier $p \geqslant 1$ vérifiant la relation précédente.

11. Groupes opérant sur un ensemble

Soient G un groupe et X un ensemble; on dit que G **opère sur** X si l'on s'est donné une application de $\mathrm{G} \times \mathrm{X}$ dans X, notée

$$(s, x) \mapsto s.x,$$

et vérifiant les deux conditions que voici : on a la relation d'associativité

$$s.(t.x) = (st).x \quad \text{quels que soient} \quad s, t \in \mathrm{G} \quad \text{et} \quad x \in \mathrm{X},$$

et d'autre part

$$e.x = x \quad \text{quel que soit} \quad x \in \mathrm{X},$$

où e désigne bien entendu l'élément neutre de G.

Exemple 19. On peut faire opérer le groupe G sur lui-même de plusieurs façons, soit à l'aide de l'application

$$(s, x) \mapsto sx,$$

(« translations à gauche »), soit à l'aide de l'application

$$(s, x) \mapsto xs^{-1}$$

(« translations à droite »), soit à l'aide de l'application

$$(s, x) \mapsto sxs^{-1}$$

(« automorphismes intérieurs »).

Exemple 20. Soient G un groupe et H un sous-groupe de G et prenons

$$\mathrm{X} = \mathrm{G}/\mathrm{H},$$

ensemble des classes $x\mathrm{H}$ dans G (n° 6); pour $s \in \mathrm{G}$ et $\mathrm{A} \in \mathrm{X}$, l'ensemble $s\mathrm{A} \subset \mathrm{G}$ des sa où $a \in \mathrm{A}$ est encore une classe modulo H (en effet, si l'on choisit un $x \in \mathrm{A}$, alors A est l'ensemble des xh, où $h \in \mathrm{H}$, et par suite $s\mathrm{A}$ est l'ensemble des sxh; autrement dit, si $\mathrm{A} = x\mathrm{H}$, on a $s\mathrm{A} = (sx)\mathrm{H}$, ce qui montre bien que $s\mathrm{A} \in \mathrm{X}$); ceci permet donc de définir une application de $\mathrm{G} \times \mathrm{X}$ dans X, à savoir $(s, \mathrm{A}) \mapsto s\mathrm{A}$; on vérifie alors immédiatement que, grâce à cette construction, G opère sur $\mathrm{X} = \mathrm{G}/\mathrm{H}$.

Exemple 21. Soient E un ensemble et p un entier; prenons

$$\mathrm{X} = \mathrm{E}^p,$$

ensemble des systèmes $(x_1, \ldots, x_p)$ de p éléments de E, et

$$\mathrm{G} = \mathfrak{S}_p,$$

groupe des permutations de l'ensemble $\{1, 2, \ldots, p\}$; pour

$$s \in \mathrm{G}, \qquad x = (x_1, \ldots, x_p) \in \mathrm{X},$$

définissons

$$s.x = (x_{s^{-1}(1)}, \ldots, x_{s^{-1}(p)});$$

l'application de $\mathrm{G} \times \mathrm{X}$ dans X ainsi définie permet de faire opérer G sur X. En effet, soient $s, t \in \mathrm{G}$ et $x \in \mathrm{X}$, et posons

$$t.x = y = (y_1, \ldots, y_p);$$

on a

$$s.(t.x) = s.y = (y_{s^{-1}(1)}, \ldots, y_{s^{-1}(p)});$$

mais on a d'autre part

$$y = (x_{t^{-1}(1)}, \ldots, x_{t^{-1}(p)})$$

et donc

$$y_i = x_{t^{-1}(i)} \quad \text{pour} \quad 1 \leqslant i \leqslant p;$$

par suite on a

$$s.(t.x) = (z_1, \ldots, z_p)$$

avec

$$z_i = y_{s^{-1}(i)} = x_{t^{-1}(s^{-1}(i))} = x_{(st)^{-1}(i)}$$

ce qui établit la relation $s.(t.x) = (st).x$; la relation $e.x = x$ est évidente.

Exemple 22. Soient X un ensemble et G un groupe de transformations de X (*Exemple* 7), alors l'application $(s, x) \mapsto s(x)$ de $G \times X$ dans X permet de faire opérer G sur X

On notera que, si un groupe G opère sur un ensemble X, alors pour tout $s \in G$ l'application

$$\bar{s} : X \to X$$

donnée par

$$\bar{s}(x) = s.x$$

est *bijective* en vertu du fait que $s^{-1}.(s.x) = (s^{-1}s).x = e.x = x$. Ceci dit, on peut encore interpréter les conditions énoncées au début de ce n° en disant que l'application $s \mapsto \bar{s}$ *est un homomorphisme du groupe* G *sur un groupe de transformations de l'ensemble* X.

Soit G un groupe opérant sur un ensemble X. Pour chaque $x \in X$, les $s \in G$ tels que $s.x = x$ forment évidemment un *sous-groupe* de G; on l'appelle le **stabilisateur de x dans** G; d'autre part, on appelle **orbite de x par** G l'ensemble (qu'on note fréquemment $G.x$) des éléments de X de la forme $s.x$, $s \in G$.

On trouvera des compléments sur ces notions dans les *Exercices* du présent §.

EXERCICES

Il est parfaitement utopique d'espérer apprendre des Mathématiques, si élémentaires ou si supérieures soient-elles, sans résoudre des Exercices.

Les Exercices qu'on trouvera dans ce livre sont de trois sortes. Certains sont des illustrations pratiques ou même numériques des théories exposées dans le texte; le lecteur débutant ne pourra pas acquérir la technique du calcul sans résoudre une partie appréciable des Exercices de ce genre. D'autres apportent au texte des compléments théoriques élémentaires; en les étudiant, le lecteur s'habituera à manipuler le langage et les modes de raisonnements utilisés dans le texte; ceux de ces Exercices qui ne sont pas *très* faciles sont précédés d'un signe ¶. Enfin, la dernière catégorie est constituée par des Exercices qui apportent au texte des compléments importants et difficiles; ils sont destinés uniquement aux étudiants déjà avancés qui s'intéressent vraiment aux Mathématiques; ces Exercices sont précédés de deux ou même trois signes ¶.

Nous ne saurions trop insister enfin sur le fait que résoudre un Exercice ne consiste pas seulement à se convaincre, à l'aide d'un « brouillon » fait à la hâte, du fait qu'on en a à peu près compris la solution; si cette méthode est admissible pour les Exercices de calcul numérique, il faut par contre s'efforcer de *rédiger intégralement* les Exercices plus théoriques, où l'on doit construire de véritables démonstrations. De cette façon, et uniquement de cette façon, l'étudiant parviendra à acquérir un langage clair et correct, et à utiliser les termes techniques dans leur sens propre, ce qui, en Mathématiques, est le signe le plus certain de la compréhension d'un sujet.

§ 7

1. Trouver tous les groupes à 1, 2 ou 3 éléments.

2. On munit un ensemble à quatre éléments (notés e, a, b, c dans ce qui suit) de la loi de composition commutative donnée par la table de multiplication suivante :

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Montrer que l'on obtient ainsi un groupe commutatif. Trouver tous ses automorphismes. (Ce groupe est connu sous le nom de **Vierergruppe** de Klein). Interpréter géométriquement ce groupe (considérer, dans l'espace, les symétries par rapport aux arêtes d'un trièdre trirectangle).

3. Montrer que le groupe $\mathfrak{S}_4$ des permutations de l'ensemble $\{1, 2, 3, 4\}$ possède un sous groupe invariant isomorphe au Vierergruppe de Klein.

4. On munit l'ensemble $\mathbf{R}$ des nombres réels de la loi de composition

$$(x, y) \to \sqrt[3]{x^3 + y^3};$$

montrer qu'on obtient ainsi un groupe, isomorphe au groupe additif $\mathbf{R}$.

5. Soient $G_1, \ldots, G_n$ des groupes, et $H_1, \ldots, H_n$ des sous-groupes de $G_1, \ldots, G_n$; montrer que $H_1 \times \cdots \times H_n$ est un sous-groupe du groupe produit $G_1 \times \cdots \times G_n$.

6. Soit G un groupe noté multiplicativement. Pour tout $a \in G$, on définit une application s_a de G dans G en posant

$$s_a(x) = ax \quad \text{pour tout } x \in G$$

(**translation à gauche** d'amplitude a dans G; le lecteur comprendra l'origine de cette terminologie en examinant le cas où G est le groupe additif des vecteurs d'origine donnée O de l'espace usuel). Montrer que l'application $a \to s_a$ est un isomorphisme du groupe G sur un groupe de permutations de l'ensemble G.

7. Soient G un groupe cyclique à m éléments et x un générateur de G. Pour que x^k soit un générateur de G, il faut et il suffit que les entiers m et k soient premiers entre eux (utiliser le théorème de Bezout). Dans le cas général, quel est l'ordre du sous-groupe de G engendré par x^k?

8. Soient m et n des entiers rationnels. Pour qu'il existe un entier r tel que l'on ait

$$r \equiv 0 \pmod{m} \qquad \text{et} \qquad r \equiv 1 \pmod{n},$$

il faut et il suffit que m et n soient premiers entre eux.

¶ Déduire de là le résultat suivant. Soient G un groupe commutatif, x et y des éléments de G d'ordres m et n premiers entre eux; alors $z = xy$ est d'ordre mn, et le sous-groupe engendré par z contient x et y. (On appelle **ordre** d'un élément x d'un groupe l'ordre, i.e. le nombre d'éléments, du sous-groupe engendré par x; cet ordre est fini si et seulement s'il existe un entier $n \neq 0$ tel que

$$x^n = e;$$

dans ce cas, l'ordre de x est le *plus petit* $n \geqslant 1$ vérifiant cette relation, comme le lecteur le démontrera).

¶ 9. Soient G et H des groupes cycliques à m et n éléments. Pour que $G \times H$ soit cyclique il faut et il suffit que m et n soient premiers entre eux. Si x et y sont des générateurs de G et H, le couple (x, y) est alors un générateur de $G \times H$.

¶ 10. Tout groupe fini d'ordre premier est cyclique, et admet pour générateur chacun de ses éléments autre que l'élément neutre (utiliser le Théorème 4 du § 7, ou l'*Exercice* 7).

11. Soit A une partie d'un groupe G. On appelle **centralisateur** de A dans G l'ensemble Z(A) des $x \in G$ tels que $xa = ax$ pour tout $a \in A$. Montrer que Z(A) est un sous-groupe de G. Montrer que Z(G) (qu'on appelle le **centre** de G) est un sous-groupe commutatif et invariant de G.

12. Deux éléments x et y d'un groupe G sont dits **conjugués** s'il existe un $s \in G$ tel que

$$y = sxs^{-1}.$$

Montrer que

$$x \text{ et } y \text{ sont conjugués}$$

est une relation d'équivalence sur l'ensemble G. On prend pour G le groupe des rotations autour d'un point donné O dans l'espace, et on choisit une droite D passant par O; montrer que tout élément de G est conjugué d'une rotation autour de D.

13. Étant donnée une partie A d'un groupe G, on note sAs^{-1} (pour $s \in G$ donné) l'ensemble des éléments de G de la forme sxs^{-1}, avec $x \in A$. Montrer que si A est un sous-groupe il en est de même de sAs^{-1} (on dit alors que c'est un sous-groupe **conjugué** de A dans G). On appelle **normalisateur** d'un sous-groupe A de G l'ensemble N(A) des $s \in G$ tels que $sAs^{-1} = A$. Montrer que le centralisateur de A (*Exercice* **11**) est un sous-groupe invariant du normalisateur de A.

14. Soit G un groupe opérant sur un ensemble X.

a) Montrer que la relation

$$\text{il existe un } s \in G \text{ tel que } y = sx$$

est une relation d'équivalence sur l'ensemble X (la classe pour cette relation d'un $x \in X$ s'appelle l'**orbite** de x par G). Montrer que, pour tout $x \in X$, l'ensemble des $s \in G$ tels que $sx = x$ est un sous-groupe H_x de G (appelé **stabilisateur** de x dans G), et que les stabilisateurs des divers points d'une même orbite sont deux à deux conjugués dans G au sens de l'*Exercice* **13**.

b) On considère, pour un $x \in X$ donné, l'application f de G dans X donnée par

$$f(s) = sx;$$

montrer qu'elle est composée de l'application canonique de G sur G/H_x et d'une application de G/H_x dans X; montrer que celle-ci induit une bijection de G/H_x sur l'orbite M de x par G, et que Card (G) = Card (M) . Card (H_x) si G est fini.

c) Décrire les orbites et les stabilisateurs lorsqu'on prend pour X l'espace usuel et pour G le groupe des rotations autour d'un point donné O dans X.

¶ *d*) On suppose que G est fini, d'ordre une puissance d'un nombre premier p, et que X est fini, le nombre d'éléments de X n'étant pas multiple de p. Montrer qu'alors G admet au moins un **point fixe** dans X (i.e. qu'il existe un $x \in X$ tel que $sx = x$ pour tout $s \in G$).

¶ *e*) Soit G un **p-groupe** i.e. un groupe fini dont l'ordre est une puissance d'un nombre premier p. En faisant opérer G sur lui-même par les automorphismes intérieurs (cf. *Exemple* **19**), montrer que le centre de G (*Exercice* **11**) n'est pas réduit à l'élément neutre.

¶ **15.** Soient G un groupe et H un sous-groupe de G; on fait opérer G sur G/H (*Exemple* **20**). Montrer que les éléments de G/H dont le stabilisateur contient H sont les images, par l'application canonique de G dans G/H, des éléments du sous-groupe N(H), normalisateur de H dans G, défini dans l'*Exercice* **13** ci-dessus.

¶ **16.** Soit H un sous-groupe *invariant* d'un groupe G. Montrer qu'il existe sur l'ensemble G/H une et une seule loi de composition faisant de G/H un groupe et telle que l'application canonique de G dans G/H soit un homomorphisme de groupes (utiliser le Théorème 3 du § 4); le groupe ainsi obtenu s'appelle le **groupe quotient** de G par H. Que se passe-t-il lorsqu'on prend pour G le groupe additif **Z** des entiers rationnels et pour H un sous-groupe de G?

Soit p l'application canonique de G sur G/H; montrer que, pour tout sous-groupe A de G/H, il existe un et un seul sous-groupe K de G contenant H tel que $A = p(K)$, et que l'on a du reste $K = p^{-1}(A)$.

On appelle **sous-groupe dérivé** de G le sous-groupe, noté G' ou D(G), engendré par les éléments de la forme $xyx^{-1}y^{-1}$. Montrer que D(G) est un sous-groupe invariant de G, et que, si H est un sous-groupe invariant de G, pour que le groupe quotient G/H soit commutatif il faut et il suffit que $H \supset D(G)$.

¶¶ **17.** Étant donnés des sous-groupes A et B d'un groupe G, on note (A, B) le sous-groupe de G engendré par les éléments $xyx^{-1}y^{-1}$ où $x \in A$ et $y \in B$. On pose

$$D(G) = (G, G), \qquad D^2(G) = D(D(G)), \qquad D^3(G) = D(D^2(G)), \text{ etc...}$$

Montrer que les conditions suivantes sont équivalentes :

a) Il existe un entier r tel que $D^{r+1}(G) = \{e\}$;

b) On peut construire des sous-groupes

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_s = G$$

de G tels que, pour chaque indice i vérifiant $0 \leqslant i \leqslant s-1$, le sous-groupe H_i soit invariant dans H_{i+1} et le groupe quotient H_{i+1}/H_i soit commutatif (la notion de groupe quotient est définie dans l'*Exercice* précédent);

c) On peut construire des sous-groupes invariants

$$\{e\} = K_0 \subset K \subset \cdots \subset K_s = G$$

de G tels que tous les groupes quotients K_{j+1}/K_j soient commutatifs.

Un groupe G vérifiant ces conditions est dit **résoluble.** Montrer que tout sous-groupe d'un groupe résoluble est résoluble. Soient G un groupe et H un sous-groupe invariant de G; les groupes H et G/H sont résolubles, il en est de même de G.

¶ **18.** Soit G un p-groupe (*Exercice* 14). Montrer que tout sous-groupe et tout groupe quotient de G est un p-groupe. En utilisant l'*Exercice* 14, *e*), montrer que G contient des sous-groupes invariants

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_s = G$$

tels que les quotients H_i/H_{i-1} soient isomorphes au groupe additif $\mathbf{Z}/p\mathbf{Z}$ (i.e. soient cycliques d'ordre p) pour $1 \leqslant i \leqslant r$. En particulier, un p-groupe est résoluble.

19. Soit G un groupe cyclique d'ordre fini n.

a) Montrer que pour tout diviseur d de n, les $x \in G$ tels $x^d = e$ sont en nombre d.

b) Soit d un diviseur de n. Pour qu'un $x \in G$ puisse s'écrire sous la forme y^d pour un $y \in G$ convenablement choisi, il faut et il suffit que

$$x^{n/d} = e.$$

¶¶ **20.** Soit G un groupe commutatif fini d'ordre n. On suppose que, pour tout diviseur d de n, les $x \in G$ tels que

$$x^d = e$$

soient en nombre d *au plus*; on se propose d'en déduire que G est *cyclique* (résultat indispensable pour l'étude des corps finis : voir § 33, *Exercice* 2). Dans ce qui suit, on désigne par

$$n = p_1^{r_1} \cdots p_h^{r_h}$$

la décomposition de n en facteurs premiers.

a) Prouver que, pour tout i tel que $1 \leqslant i \leqslant h$, il existe un $a_i \in G$ vérifiant

$$a_i^{p_i^{r_i}} = e, \qquad a_i^{p_i^{r_i-1}} \neq e$$

et que a_i est d'ordre

$$q_i = p_i^{r_i}$$

exactement.

b) Montrer, en utilisant le fait que les q_i sont deux à deux premiers entre eux, que l'élément $a_1 \dots a_h$ est d'ordre $q_1 \dots q_h = n$, et en conclure que G est cyclique comme annoncé.

c) Montrer qu'on parviendrait à la même conclusion en faisant l'hypothèse moins forte que voici : pour $1 \leqslant i \leqslant h$, les $x \in G$ tels que

$$x^{p_i} = e$$

sont en nombre p_i au plus.

21. Soit f un homomorphisme d'un groupe fini G dans un groupe H. Montrer que

$$\mathrm{Card}(G) = \mathrm{Card}(\mathrm{Ker}(f)) \,.\, \mathrm{Card}(\mathrm{Im}(f)).$$

¶ **22.** Soient G un groupe commutatif fini et n un entier tel que (*)

$$x^n = e \qquad \text{pour tout } x \in G.$$

a) On suppose $n = rs$ avec r et s premiers entre eux; soit M (resp. N) l'ensemble des $x \in G$ tels que

$$x^r = e \text{ (resp. } x^s = e).$$

Montrer que M et N sont des sous-groupes de G. En écrivant l'identité de Bezout pour r et s, montrer que l'application

$$f : M \times N \to G$$

donnée par $f(x, y) = xy$ est un isomorphisme de groupes.

b) Soit

$$n = p_1^{r_1} \dots p_h^{r_h} = q_1 \dots q_h \qquad \text{où} \qquad q_i = p_i^{r_i}$$

la décomposition de n en facteurs premiers; pour tout i tel que $1 \leqslant i \leqslant h$, soit M_i le sous-groupe des $x \in G$ tels que

$$x^{q_i} = e.$$

Montrer que G est isomorphe au produit direct des groupes $M_1, \dots, M_h$.

c) Soient M un groupe commutatif fini, p un nombre premier et r un entier naturel; on suppose que

$$x^{p^r} = e$$

pour tout $x \in M$; montrer que Card (M) est une puissance de p (observer que, si $M \neq \{e\}$, on peut trouver dans M un sous-groupe M' d'ordre p; l'introduction du groupe quotient M/M', cf. *Exercice* 16, permet alors de raisonner par récurrence sur le nombre d'éléments de M).

d) Démontrer le théorème suivant : *soit* G *un groupe commutatif fini d'ordre*

$$n = p_1^{r_1} \dots p_h^{r_h};$$

alors G *est isomorphe au produit direct de* h *groupes d'ordres* $p_1^{r_1}, \dots, p_h^{r_h}$ (ce résultat, que Gauss avait déjà plus ou moins démontré en 1801, sera complété dans les *Exercices* du § 31 : un groupe commutatif dont l'ordre est une puissance de p est isomorphe à un produit direct de groupes *cycliques* dont les ordres sont des puissances de p. Il en résultera que tout groupe commutatif fini est isomorphe à un produit direct de groupes cycliques. L'étude complète des groupes commutatifs à un nombre fini de générateurs a été faite par Kronecker en 1870; un tel groupe est produit direct d'un groupe commutatif fini et d'un groupe $\mathbf{Z}^n$).

(*) L'énoncé de cet *Exercice* est rédigé en notation multiplicative, mais le lecteur aura intérêt, pour des généralisations ultérieures, à le traduire en notation additive.

¶ **23.** On reprend la question *a*) de l'*Exercice* précédent. Soit A (resp. B) le sous-groupe de G formé des x tels que l'on ait

$$x = y^s \text{ (resp. } x = y^r)$$

pour au moins un $y \in G$. Montrer que $A = M$ et $B = N$ (on prouvera qu'on a les relations

$$\mathrm{Card}(G) = \mathrm{Card}(M) \,.\, \mathrm{Card}(N) = \mathrm{Card}(A) \,.\, \mathrm{Card}(N) = \mathrm{Card}(B) \,.\, \mathrm{Card}(M)$$

et on observera que $A \subset M$, $B \subset N$).

On suppose que $n = \mathrm{Card}(G)$. Montrer que $\mathrm{Card}(M) = r$, $\mathrm{Card}(N) = s$.

24. Soit $s \in \mathfrak{S}_n$ une permutation de l'ensemble $X = \{1, 2, \dots, n\}$ et soit G le sous-groupe de $\mathfrak{S}_n$ formé par les puissances de s.

a) Montrer qu'on peut trouver des parties non vides $I_1, \dots, I_r$ de X vérifiant les conditions suivantes : on a $g(I_k) = I_k$ pour $1 \leqslant k \leqslant r$ et tout $g \in G$; les ensembles I_k sont deux à deux disjoints et leur réunion est X tout entier; pour que $p, q \in X$ appartiennent à un même I_k, il faut et il suffit qu'il existe un $g \in G$ tel que $q = g(p)$. Relation avec l'*Exercice* 14, *a*)?

b) Montrer que les conditions précédentes caractérisent les ensembles I_k (à ceci près qu'on peut naturellement modifier l'ordre dans lequel on les écrit).

c) Montrer que, pour chaque k, on peut écrire les éléments de I_k sous forme d'une suite $i_0, \dots, i_p$ de telle sorte que l'on ait

$$s(i_0) = i_1, \quad s(i_1) = i_2, \quad \dots, \quad s(i_{p-1}) = i_p, \quad s(i_p) = i_0$$

(*décomposition d'une permutation en cycles*; on appelle **cycle** pour s toute suite d'entiers $i_0, \dots, i_p$ écrits dans l'ordre naturel, deux à deux distincts, et vérifiant les relations précédentes).

d) Trouver les cycles des permutations suivantes :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 3 & 6 & 5 & 7 & 4 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 9 & 2 & 1 & 4 & 3 & 6 & 7 \end{pmatrix}.$$

(NB. — On utilise ici la notation standard pour représenter une permutation s; celle-ci consiste à écrire sur la seconde ligne les images par s des éléments de la première).

e) Étant donnée une permutation $s \in \mathfrak{S}_n$, soient $n_1, \dots, n_r$ les nombres de termes des divers cycles de s. Montrer que l'ordre de s (i.e. le plus petit entier $q \geqslant 1$ tel que $s^q = e$, ou l'ordre du groupe cyclique engendré par s) est le ppcm des entiers $n_1, \dots, n_r$.

f) On considère la permutation

$$s : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 1 & 7 & 10 & 2 & 6 & 9 & 8 \end{pmatrix};$$

calculer l'ordre du sous-groupe de $\mathfrak{S}_{10}$ engendré par s. Calculer la permutation

$$s^{100}.$$

qq **25.** Dans cet Exercice, on utilise la terminologie suivante. Étant donnée une suite

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \longrightarrow \cdots G_n \xrightarrow{f_n} G_{n+1}$$

formée de groupes additifs G_i et d'homomorphismes $f_i : G_i \to G_{i+1}$, on dit que cette suite est **exacte** si, pour chaque entier i tel que $1 \leqslant i < n$, l'image de l'homomorphisme f_i est égale au noyau de l'homomorphisme suivant f_{i+1}. D'autre part, on dit qu'un diagramme, par exemple

$$\begin{array}{ccccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{k} & E \\ \downarrow p & & \downarrow q & & \downarrow r & & \downarrow s & & \downarrow t \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' & \xrightarrow{k'} & E' \end{array} \qquad (1)$$

formé d'ensembles et d'applications de ces ensembles les uns dans les autres, est **commutatif** si, quels que soient les «sommets» X et Y du diagramme, toutes les applications de X dans Y qu'on obtient en composant, de toutes les façons possibles, les applications figurant dans le diagramme donné, sont égales. Dans le cas du diagramme (1), la commutativité se traduirait par la relation $f' \circ p = q \circ f$ et de nombreuses autres relations analogues que le lecteur écrira.

On considère un diagramme *commutatif* (1) dans lequel A, B, ... sont des groupes additifs, et les applications des homomorphismes de groupes. On suppose que les deux lignes horizontales du diagramme sont des suites *exactes* — de sorte qu'on a

$$\mathrm{Im}(f) = \mathrm{Ker}(g), \qquad \mathrm{Im}(f') = \mathrm{Ker}(g'),$$

etc... Établir les résultats suivants (connus sous le nom de **lemme des cinq**) :

a) Si p est surjectif, et si q et s sont injectifs, alors r est injectif.

b) Si q et s sont surjectifs, et si t est injectif, alors r est surjectif.

c) Si p est surjectif, si q et s sont bijectifs, et si t est injectif, alors r est bijectif.