Théorie des Groupes
L3–Mathématiques
2019–2020

Paul LESCOT
Université de Rouen
paul.lescot@univ-rouen.fr

Sommaire

1. Définitions et généralités

DÉFINITION 1.1. On appelle groupe un ensemble G muni d'une loi de composition interne $*$ satisfaisant les axiomes suivants :

(G1) *Associativité*

$$(\forall (a,b,c) \in G^3)\ (a*b)*c = a*(b*c),$$

(G2) *Elément neutre*

$$(\exists e \in G)(\forall a \in G)\ a*e = e*a = a,$$

et

(G3) *Symétriques*

$$(\forall a \in G)(\exists b \in G)\ a*b = *a = e.$$

Si on a de plus

(GA)

$$\forall (a,b) \in G^2\ a*b = b*a,$$

le groupe G est dit *commutatif* (ou *abélien*).

REMARQUES 1.2. (1) L'élément neutre e est unique.

Supposons en effet l'existence de deux éléments neutres e_1 et e_2 ; alors

$$(\forall a \in G)\ a*e_1 = e_1*a = a$$

et

$$(\forall a \in G)\ a*e_2 = e_2*a = a.$$

Prenant $a = e_2$ dans la première équation, l'on obtient

$$e_2*e_1 = e_1*e_2 = e_2\ ;$$

prenant alors $a = e_1$ dans la seconde, il vient

$$e_1*e_2 = e_2*e_1 = e_1\ .$$

Mais alors

$$e_2 = e_2*e_1 = e_1\ ,$$

et

$$e_2 = e_1.$$

(2) Pour chaque élément a de G, l'élément b figurant dans **(G3)** est unique.

En effet, supposons

$$a*b = b*a = e$$

et

$$a*c = c*a = e.$$

Il vient

$$\begin{aligned} c &= e * c \\ &\quad \text{(par } \mathbf{(G2)}\text{)} \\ &= (b * a) * c \\ &= b * (a * c) \\ &\quad \text{(par } \mathbf{(G1)}\text{)} \\ &= b * e \\ &= b \\ &\quad \text{(par } \mathbf{(G2)}\text{)}, \end{aligned}$$

d'où $c = b$.

On notera dorénavant cet élément $a^{'}$, et on l'appellera l'*inverse* (ou le *symétrique*) de a.

(3) On peut remplacer l'axiome **(G3)** par

$$\mathbf{(G4)} \quad (\forall a \in G)(\exists b \in G) \ \ a * b = e.$$

En effet, il est clair que **(G3)** entraîne **(G4)**, donc (**(G1)**, **(G2)** et **(G3)**) entraîne (**(G1)**, **(G2)** et **(G4)**).

Réciproquement, supposons **(G1)**, **(G2)** et **(G4)** satisfaits, et démontrons **(G3)**.

Soit $a \in G$; d'après **(G4)**, il existe $b \in G$ tel que $a * b = e$, et il existe $c \in G$ tel que $b * c = e$. Mais alors

$$\begin{aligned} c &= e * c \\ &\quad \text{(d'après } \mathbf{(G2)}\text{)} \\ &= (a * b) * c \\ &= a * (b * c) \\ &\quad \text{(d'après } \mathbf{(G1)}\text{)} \\ &= a * e \\ &= a \\ &\quad \text{(d'après } \mathbf{(G2)}\text{)}, \end{aligned}$$

soit $c = a$.

Il s'ensuit que

$$b * a = b * c = e,$$

d'où

$$a * b = b * a = e$$

et **(G3)**.

Au passage nous avons établi que $a^{''} = c = a$, d'où $a^{''} = a$ pour tout élément a de G.

(4) Prenant $a = e$ dans **(G3)**, on obtient $e * e^{'} = e$, d'où $e^{'} = e$ d'après **(G2)**: l'élément neutre e est donc son propre inverse.

On notera le plus souvent $a * b$ par ab ou $a.b$, e par e_G, 1_G ou 1 et $a^{'}$ par a^{-1}.

Si G est abélien on notera parfois $a * b$ par $a + b$ et e par 0 ou 0_G, ainsi que $a^{'}$ par $-a$.

Dorénavant G désignera un groupe ; $ab := a * b$.

LEMME 1.3. *Pour tout couple $(a, b) \in G^2$, il existe un unique $c \in G$ tel que $ac = b$, et il existe un unique $d \in G$ tel que $da = b$.*

DÉMONSTRATION. De $ac = b$ suit

$$\begin{aligned} c &= ec \\ &= (a^{-1}a)c \\ &= a^{-1}(ac) \\ &= a^{-1}b\,, \end{aligned}$$

d'où l'unicité.

Réciproquement, soit $c = a^{-1}b$; alors

$$\begin{aligned} ac &= a(a^{-1}b) \\ &= (aa^{-1})b \\ &= eb \\ &= b\ , \end{aligned}$$

et c convient.

Le raisonnement est semblable dans l'autre cas (sans surprise, on trouve

$$d = ba^{-1}).$$

□

PROPOSITION 1.4. (1) $(\forall x \in G)\ (x^{-1})^{-1} = x$.
(2) $\forall (x, y) \in G^2\ (xy)^{-1} = y^{-1}x^{-1}$.

DÉMONSTRATION.

(1) Cela a été établi incidemment lors de la justification de la Remarque 1.2.(3). En effet, on a vu que

$$(\forall a \in G)\ a^{''} = a\ ;$$

mais $a^{-1} = a^{'}$, d'où, pour tout $x \in G$:

$$(x^{-1})^{-1} = (x^{-1})^{'} = (x^{'})^{'} = x^{''} = x.$$

(2)

$$\begin{aligned} (xy)(xy)^{-1} &= e_G \\ &= xx^{-1} \\ &= (xe_G)x^{-1} \\ &= (x(yy^{-1}))x^{-1} \\ &= ((xy)y^{-1})x^{-1} \\ &= (xy)(y^{-1}x^{-1}). \end{aligned}$$

La conclusion suit alors du Lemme 1.3.

□

DÉFINITION 1.5. (*Puissances* d'un élément)
Soit $x \in G$; on définit $x^0 = e_G$,

$$(\forall n \in \mathbf{N})\ x^{n+1} := x^n.x,$$

et

$$(\forall n \leq -1)\ x^n := (x^{-1})^{-n}.$$

REMARQUE 1.6. Dans un groupe G, le produit vide est conventionnnellement considéré comm égal à l'élément neutre e_G, ce qui est cohérent avec $x^0 = e_G$.

PROPOSITION 1.7. $(\forall x \in G)\ (\forall (m,n) \in \mathbf{N}^2)\ x^{m+n} = x^m x^n$.

DÉMONSTRATION. Fixons $m \in \mathbf{N}$ et $x \in G$; on va établir que

$$(\forall n \in \mathbf{N})\ x^{m+n} = x^m x^n\ \ (\mathcal{P}_n)$$

par récurrence sur n.
Pour $n = 0$ c'est évident :

$$x^m x^n = x^m x^0 = x^m e_G = x^m = x^{m+0} = x^{m+n}.$$

Supposons $(\mathcal{P}_n)$; alors

$$\begin{array}{rcl} x^{m+(n+1)} & = & x^{(m+n)+1} \\ & = & x^{m+n}x \\ & = & (x^m x^n)x \\ & & \text{(d'après } (\mathcal{P}_n)\text{)} \\ & = & x^m(x^n x) \\ & & \text{(d'après } \textbf{(G1)}\text{)} \\ & = & x^m x^{n+1}\ , \end{array}$$

soit $(\mathcal{P}_{n+1})$. □

LEMME 1.8. *Pour chaque $x \in G$ et chaque $n \in \mathbf{Z}$,*

$$(x^n)^{-1} = (x^{-1})^n = x^{-n}.$$

DÉMONSTRATION.

$1^o)$ $n \in \mathbf{N}$.
Nous allons procéder par récurrence sur n.
Si $n = 0$ on a bien

$$(x^n)^{-1} = (x^0)^{-1} = e^{-1} = e = x^0 = x^{-n}$$

et

$$(x^{-1})^n = (x^{-1})^0 = e = x^0 = x^{-n}.$$

Supposons le résultat établi au rang n ; alors

$$\begin{aligned}(x^{n+1})^{-1} &= (x^n x)^{-1} \\ &\quad \text{(d'après la Définition 1.5)} \\ &= x^{-1}(x^n)^{-1} \\ &\quad \text{(d'après la Proposition 1.4(2))} \\ &= x^{-1}(x^{-1})^n \\ &\quad \text{(par l'hypothèse de récurrence)} \\ &= (x^{-1})^1(x^{-1})^n \\ &= (x^{-1})^{1+n} \\ &\quad \text{(d'après la Proposition 1.7)} \\ &= (x^{-1})^{n+1} \ ;\end{aligned}$$

de plus, il suit de la Définition 1.5 que

$$x^{-(n+1)} = (x^{-1})^{-(-(n+1))} = (x^{-1})^{n+1},$$

et le résultat au rang $n+1$ s'ensuit.

2^o) $n \leq -1$.

Alors

$$\begin{aligned}(x^n)^{-1} &= ((x^{-1})^{-n})^{-1} \\ &\quad \text{(Définition 1.5)} \\ &= ((x^{-1})^{-1})^{-n} \text{(d'après le résultat de } 1^o) \text{ appliqué à } -n \in \mathbf{N}) \\ &= x^{-n}\end{aligned}$$

et

$$\begin{aligned}(x^{-1})^n &= ((x^{-1})^{-1})^{-n} \\ &= x^{-n} \\ &= (x^n)^{-1}.\end{aligned}$$

□

Nous sommes maintenant en mesure de généraliser la Proposition 1.7.

THÉORÈME 1.9. $(\forall x \in G)(\forall (m,n) \in \mathbf{Z}^2)\ x^{m+n} = x^m x^n$.

DÉMONSTRATION. Supposons d'abord $m \in \mathbf{N}$; alors on a vu que l'égalité était vérifiée pour chaque $n \in \mathbf{N}$. Deux autres cas peuvent se présenter

1^o) $-m \leq n \leq -1$

Alors

$$\begin{aligned}x^{m+n}(x^n)^{-1} &= x^{m+n}(x^{-1})^n \\ &\quad \text{(Lemme 1.8)} \\ &= x^{m+n}((x^{-1})^{-1})^{-n} \\ &\quad \text{(en vertu de la Définition 1.5)} \\ &= x^{m+n}x^{-n} \\ &= x^{(m+n)+(-n)} \\ &\quad \text{(car } m+n \geq 0 \text{ et } -n \geq 0) \\ &= x^m \ ,\end{aligned}$$

d'où

$$\begin{aligned} x^m x^n &= (x^{m+n}(x^n)^{-1})x^n \\ &= x^{m+n}((x^n)^{-1}x^n) \\ &= x^{m+n}e \\ &= x^{m+n}. \end{aligned}$$

$2^o)\, n \leq -m-1$
Alors $k := -n-m \geq 1$ et

$$\begin{aligned} x^{m+n} &= x^{-k} \\ &= (x^{-1})^k \\ &= e(x^{-1})^k \\ &= (x^m(x^m)^{-1})(x^{-1})^k \\ &= x^m((x^m)^{-1}(x^{-1})^k) \\ &= x^m((x^{-1})^m(x^{-1})^k) \\ &= x^m(x^{-1})^{m+k} \\ &= x^m(x^{-1})^{-n} \\ &= x^m x^n. \end{aligned}$$

On a donc établi le résultat lorsque $m \in \mathbf{N}$.

Soit maintenant $m \leq -1$; il suit

$$\begin{aligned} x^n &= x^{-m+(m+n)} \\ &= x^{-m}x^{m+n}\ , \end{aligned}$$

d'où

$$\begin{aligned} x^m x^n &= x^m(x^{-m}x^{m+n}) \\ &= (x^m x^{-m})x^{m+n} \\ &= (x^m(x^m)^{-1})x^{m+n} \\ &= ex^{m+n} \\ &= x^{m+n}. \end{aligned}$$

□

COROLLAIRE 1.10. $(\forall x \in G)(\forall (m,n) \in \mathbf{Z}^2)\ \ x^{mn} = (x^m)^n$.

DÉMONSTRATION. $x \in G$ et $m \in \mathbf{Z}$ étant fixés, nous établirons d'abord le résultat pour $n \in \mathbf{N}$, par récurrence sur n.

Pour $n = 0$, on a bien

$$(x^m)^0 = e = x^0 = x^{m.0} = x^{mn}.$$

Supposons le résultat établi au rang n ; alors

$$\begin{aligned}(x^m)^{n+1} &= (x^m)^n x^m \\ &= x^{mn}x^m \\ &\quad \text{(par l'hypothèse de récurrence)} \\ &= x^{mn+m} \\ &\quad \text{(Théorème 1.9)} \\ &= x^{m(n+1)}\ ,\end{aligned}$$

soit le résultat au rang $n+1$.

Soit maintenant $n \leq -1$; on peut écrire

$$\begin{aligned}(x^m)^n &= ((x^m)^{-1})^{-n} \\ &\quad \text{(d'après la Définition 1.5)} \\ &= ((x^{-1})^m)^{-n} \\ &\quad \text{(d'après le Lemme 1.8)} \\ &= (x^{-1})^{m(-n)} \\ &\quad \text{(car } -n \in \mathbf{N}\text{)} \\ &= (x^{-1})^{-mn} \\ &= x^{-(-mn)} \\ &\quad \text{(d'après le Lemme 1.8)} \\ &= x^{mn}.\end{aligned}$$

□

PROPOSITION 1.11. *Si $(a,b) \in G^2$ et $ab = ba$ (on dit que a et b commutent) alors*

$$(\forall n \in \mathbf{Z})\ (ab)^n = a^n b^n.$$

DÉMONSTRATION. Etablissons d'abord par récurrence sur n que

$$(\forall n \in \mathbf{N})\ ab^n = b^n a.\ (\mathbf{I}_n)$$

Pour $n = 0$ on a bien

$$ab^0 = ae = a = ea = b^0 a.$$

Supposons la propriété vraie au rang n ; alors

$$\begin{aligned} ab^{n+1} &= ab^{1+n} \\ &= a(b^1b^n) \\ &= a(bb^n) \\ &= (ab)b^n \\ &= (ba)b^n \\ &= b(ab^n) \\ &= b(b^na) \\ &\quad \text{(d'après } (\mathbf{I}_n)) \\ &= (bb^n)a \\ &= (b^1b^n)a \\ &= b^{1+n}a \\ &= b^{n+1}a, \end{aligned}$$

soit $(\mathbf{I}_{n+1})$.

D'où le résultat.

Nous allons utiliser cette égalité afin d'établir que

$$(\forall n \in \mathbf{N})\ (ab)^n = a^nb^n.$$

C'est clair pour $n = 0$:

$$\begin{aligned} a^0b^0 &= e.e \\ &= e \\ &= (ab)^0. \end{aligned}$$

Supposons l'égalité vraie au rang n ; alors

$$\begin{aligned} (ab)^{n+1} &= (ab)^nab \\ &= (a^nb^n)ab \\ &= a^n(b^n(ab)) \\ &= a^n((b^na)b) \\ &= a^n((ab^n)b) \\ &\quad \text{(d'après } (\mathbf{I}_n)) \\ &= a^n(a(b^nb))) \\ &= (a^na)(b^nb) \\ &= a^{n+1}b^{n+1}\ , \end{aligned}$$

d'où le résultat par récurrence sur n.

De $ab = ba$ il suit que

$$a^{-1}b^{-1} = (ba)^{-1} = (ab)^{-1} = b^{-1}a^{-1}\ :$$

a^{-1} et b^{-1} commutent.

Soit alors $n \leq -1$; il apparaît que

$$\begin{aligned}(ab)^n &= ((ab)^{-1})^{-n} \\ &= (b^{-1}a^{-1})^{-n} \\ &= (a^{-1}b^{-1})^{-n} \\ &= (a^{-1})^{-n}(b^{-1})^{-n} \\ &\quad (\text{car } -n \in \mathbf{N}) \\ &= a^{-(-n)}b^{-(-n)} \\ &= a^n b^n.\end{aligned}$$

On a bien établi que

$$(\forall n \in \mathbf{Z})\ (ab)^n = a^n b^n.$$

□

COROLLAIRE 1.12. *Si le groupe G est abélien, on a*

$$(\forall n \in \mathbf{Z})\ (\forall (a,b) \in G^2)\ (ab)^n = a^n b^n.$$

DÉMONSTRATION. Puisque G est abélien, l'hypothèse de la Proposition 1.11 est satisfaite par tout couple $(a,b) \in G^2$. □

Au vu du Théorème 1.9, du Corollaire 1.10 et du Corollaire 1.12, l'on peut dire que, dans un groupe abélien, l'opération "puissance" $((n,x) \mapsto x^n)$ possède toutes les propriétés habituelles.

2. Une caractérisation des groupes abéliens à partir des propriétés de la soustraction.

Soit G un groupe abélien ; pour $(a,b) \in G^2$, posons

$$a - b := a + (-b).$$

Alors, pour tous a, b, et c éléments de G :

$$\begin{aligned} a-(b-c) &= a+(-(b+(-c))) \\ &= a+(-(-c)+(-b)) \\ &= a+(c+(-b)) \\ &= (a+c)+(-b) \\ &= (c+a)+(-b) \\ &= c+(a+(-b)) \\ &= c+((-(-a))+(-b)) \\ &= c+(-(b+(-a))) \\ &= c-(b+(-a)) \\ &= c-(b-a) \end{aligned}$$

et

$$\begin{aligned} a-(b-b) &= a-0 \\ &= a+(-0) \\ &= a+0 \\ &= a. \end{aligned}$$

Réciproquement

THÉORÈME 2.1. *(Vaughan, [**1**], p. 349) Soit G un ensemble non vide muni d'une loi de composition $*$ satisfaisant les identités suivantes :*

$$\forall (a,b,c) \in G^3 \quad a*(b*c) = c*(b*a) \quad (\mathcal{C}_1)$$

et

$$\forall (a,b) \in G^2 \quad a*(b*b) = a. \quad (\mathcal{C}_2).$$

Alors il existe une unique loi de composition $+$ sur G telle que $(G,+)$ soit un groupe abélien et que la soustraction associée $(-)$ coïncide avec $*$.

DÉMONSTRATION. Soit $u \in G$; on doit avoir

$$0 = u - u = u * u$$

et, pour tout $(a,b) \in G^2$

$$\begin{aligned} a+b &= a-(-b) \\ &= a-(0-b) \\ &= a*((u*u)*b), \end{aligned}$$

d'où l'unicité.

Réciproquement, posons $e := u * u$ et définissons

$$a + b := a * (e * b)$$

Il apparaıt que, pour tout $a \in G$,

$$\begin{aligned} a * e &= a * (u * u) \\ &= a \\ &\quad \text{(d'après } (\mathcal{C}_2)\text{).} \end{aligned}$$

(1) $+$ **est commutative**
Pour $(a, b) \in G^2$

$$\begin{aligned} a + b &= a * (e * b) \\ &= b * (e * a) \\ &\quad \text{(d'après } (\mathcal{C}_1)\text{)} \\ &= b + a. \end{aligned}$$

(2) e **est élément neutre pour** $+$
Soit $a \in G$;

$$\begin{aligned} e + a &= a + e \\ &\quad \text{(d'après (1))} \\ &= a * (e * e) \\ &= a \\ &\quad \text{(d'après } (\mathcal{C}_2)\text{).} \end{aligned}$$

(3) $+$ **est associative**
Soient a, b et c trois éléments de G ; alors

$$\begin{aligned} (a + b) + c &= (a * (e * b)) * (e * c) \\ &= c * (e * (a * (e * b))) \\ &= c * ((e * b) * (a * e)) \\ &\quad \text{(d'après } (\mathcal{C}_1)\text{)} \\ &= c * ((e * b) * a) \\ &= a * ((e * b) * c) \\ &\quad \text{(d'après } (\mathcal{C}_1)\text{)} \\ &= a * ((e * b) * (c * e)) \\ &= a * (e * (c * (e * b))) \\ &\quad \text{(encore d'après } (\mathcal{C}_1)\text{)} \\ &= a * (e * (c + b)) \\ &= a + (c + b) \\ &= a + (b + c) \\ &\quad \text{(d'après (1)).} \end{aligned}$$

(4) **Chaque élément de** G **possède un symétrique pour** $+$

Pour $a \in G$, posons $a^{'} := e * a$. Alors

$$\begin{aligned} a^{'} + a &= a + a^{'} \\ &= a * (e * a^{'}) \\ &= a * (e * (e * a)) \\ &= a * (a * (e * e)) \\ &\quad \text{(d'après } (\mathcal{C}_1)) \\ &= a * (a * e) \\ &= e * (a * a) \\ &\quad \text{(d'après } (\mathcal{C}_1)) \\ &= e \\ &\quad \text{(d'après } (\mathcal{C}_2)) : \end{aligned}$$

$a^{'}$ est symétrique de a pour $+$.

Nous avons bien vérifié les axiomes des groupes abéliens : (1) équivaut à **(GA)**, (2) à **(G2)**, (3) à **(G1)** et (4) à **(G3)**; $(G, +)$ est donc bien un groupe abélien, et

$$\forall (a, b) \in G^2$$

$$\begin{aligned} a - b &= a + (-b) \\ &= a + b^{'} \\ &= a * (e * b^{'}) \\ &= a * (e * (e * b)) \\ &= a * (b * (e * e)) \\ &\quad \text{(d'après } (\mathcal{C}_1)) \\ &= a * b. \end{aligned}$$

□

La classe des groupes abéliens peut donc être caractérisée au moyen d'une opération et d'axiomes non existentiels.

3. Sous–groupes, classes modulo un sous–groupe, morphismes de groupes

Dans tout ce chapitre, G désignera un groupe noté multiplicativement, sauf dans les Exemples 3.2 et 3.5.(1), ainsi que l'exercice 3.7. On appelle *sous–groupe* de G une partie H de G formant un groupe pour le restriction de la loi de composition de G.

PROPOSITION 3.1. *Soit $H \subset G$; les propriétés suivantes sont équivalentes :*

(1) $e_G \in H$, $\forall (x,y) \in H^2$ $xy \in H$ *et* $(\forall x \in H)$ $x^{-1} \in H$;
(2) H *est un sous–groupe de* G ;
(3) $H \neq \emptyset$ *et* $\forall (x,y) \in H^2$ $xy^{-1} \in H$.

DÉMONSTRATION. 1) $\Longrightarrow$ 2)

Vu que pour tout couple $(x,y) \in H^2$ on a $xy \in H$, la restriction à H de la loi de composition interne sur G définit une loi de composition interne sur H, dont l'associativité est évidente.

Du fait que $e_G \in H$, e_G est un élément neutre pour cette loi : e_H existe, et $e_H = e_G$.

Soit $a \in H$; $a^{-1} \in H$ et

$$aa^{-1} = a^{-1}a = e_G = e_H \,,$$

donc a^{-1} est un symétrique de a **dans** H.

H est donc un sous–groupe de G.

2) $\Longrightarrow$ 3)

$e_H \in H$ donc $H \neq \emptyset$.

Soit alors $(x,y) \in H^2$; H étant un sous–groupe de G, il existe, en vertu du Lemme 1.3 appliqué dans H, un élément $z \in H$ tel que $zy = x$.

Mais le même Lemme appliqué dans G entraîne que $z = xy^{-1}$, d'où $xy^{-1} = z \in H$.

3) $\Longrightarrow$ 1)

$H \neq \emptyset$, donc il existe $h \in H$; alors $e_G = hh^{-1} \in H$.

Soit $x \in H$; $x^{-1} = e_G x^{-1} \in H$.

Soit $(x,y) \in H^2$; $y^{-1} \in H$ donc $xy = x(y^{-1})^{-1} \in H$. □

EXEMPLE 3.2. $G = \mathbf{Z}$, ensemble des entiers relatifs, muni de l'addition habituelle. Il est facile de voir que, pour chaque $n \in \mathbf{N}$,

$$n\mathbf{Z} := \{na | a \in \mathbf{Z}\}$$

est un sous–groupe de $\mathbf{Z}$.

Réciproquement, tout sous–groupe de $\mathbf{Z}$ est de cette forme. Soit en effet H un sous–groupe de $\mathbf{Z}$; si $H = \{0\}$, $H = 0.\mathbf{Z}$ et $n = 0$ convient. Dans le cas contraire, il existe un élément $a \in H$, $a \neq 0$; vu que $-a \in H$, $|a| \in H$, et $|a| \geq 1$. On a donc

$$|a| \in H \cap \mathbf{N}^* \,;$$

$H \cap \mathbf{N}^*$ est donc un ensemble non vide d'entiers positifs. Soit n son plus petit élément. Pour $y \in \mathbf{Z}$, trois possibilités apparaissent :

(1) $y \geq 1$.
Alors
$$ny = \underbrace{n + ... + n}_{y \text{ termes}} \in H.$$
(2) $y = 0$.
Alors $ny = 0 \in H$.
(3) $y \leq -1$.
Alors, du fait que $n \in H$, $-n \in H$ et
$$\begin{aligned} ny &= (-n)(-y) \\ &= \underbrace{(-n) + ... + (-n)}_{-y \text{ termes}} \\ &\in H. \end{aligned}$$

On a donc $ny \in H$ pour tout $y \in \mathbf{Z}$, soit $n\mathbf{Z} \subset H$.

Réciproquement, soit $h \in H$. Effectuons la division euclidienne de h par n ; on obtient une expression de la forme

$$h = nq + r \ ,$$

avec $(q, r) \in \mathbf{Z}^2$ et $0 \leq r \leq n - 1$.

Mais alors $nq \in n\mathbf{Z} \subset H$, donc $nq \in H$ et

$$r = h - nq \in H \ ;$$

vu que $r < n$, on ne saurait avoir $r \in \mathbf{N}^*$, car on aurait alors $r \in H \cap \mathbf{N}^*$, contrairement à la définition de n. Il s'ensuit que $r = 0$, d'où $h = nq \in n\mathbf{Z}$. Le sous–groupe H est ainsi contenu dans $n\mathbf{Z}$; il lui est donc égal : $H = n\mathbf{Z}$.

Les sous–groupes de $\mathbf{Z}$ sont donc les $(n\mathbf{Z})_{n \in \mathbf{N}}$; il est aisé de voir qu'ils sont distincts pour des valeurs distinctes de n.

PROPOSITION 3.3. *Soit $(H_i)_{i \in I}$ une famille de sous–groupes de G ; alors l'intersection*
$$\bigcap_{i \in I} H_i$$
est un sous–groupe de G.

DÉMONSTRATION. Pour chaque $i \in I$ on a $e_G \in H_i$, d'où
$$e_G \in \bigcap_{i \in I} H_i$$
et
$$\bigcap_{i \in I} H_i \neq \emptyset.$$
Soit $(x, y) \in (\bigcap_{i \in I} H_i)^2$; pour chaque $i \in I$ on a $x \in H_i$ et $y \in H_i$, d'où $xy^{-1} \in H_i$. Mais alors
$$xy^{-1} \in \bigcap_{i \in I} H_i \, ;$$
on voit que $\bigcap_{i \in I} H_i$ satisfait aux deux conditions de la Proposition 3.1(3), donc $\bigcap_{i \in I} H_i$ est un sous–groupe de G. □

PROPOSITION 3.4. *Soit X une partie de G ; il existe un plus petit sous–groupe de G contanant X. On le note $< X >$, et on l'appelle le* ***sous–groupe de*** *G engendré par X.*

On a

$$< X >= \{x_1^{\epsilon_1}...x_n^{\epsilon_n} | n \geq 0, x_i \in X, \epsilon_i \in \{-1, 1\}\}.$$

DÉMONSTRATION. Soit

$$H = \{x_1^{\epsilon_1}...x_n^{\epsilon_n} | n \geq 1, x_i \in X, \epsilon_i \in \{-1, 1\}\}.$$

On a $e_G \in H$, vu que e_G est égal au produit vide d'éléments de X.

Soit $(u, v) \in H^2$; alors

$$u = x_1^{\epsilon_1}...x_n^{\epsilon_n}$$

et

$$v = y_1^{\epsilon_1'}...y_m^{\epsilon_m'},$$

les x_i et y_i appartenant à H est les ϵ_i et ϵ_i' à $\{-1, 1\}$. Mais alors

$$uv^{-1} = x_1^{\epsilon_1}...x_n^{\epsilon_n} y_m^{-\epsilon_m'}...y_1^{-\epsilon_1'} \in H;$$

H est donc bien un sous–groupe de G.

Soit $x \in X$; alors $x = x^1 \in H$; on a donc bien $X \subset H$.

Soit maintenat I un sous–groupe de G tel que $X \subset I$, et soit $h \in H$; h s'écrit

$$h = x_1^{\epsilon_1}...x_m^{\epsilon_m}.$$

Si $\epsilon_i = 1$, $x_i^{\epsilon_i} = x_i \in X \subset I$ donc $x_i^{\epsilon_i} \in I$.

Si $\epsilon_i = -1$, vu que $x_i \in I$, $x_i^{\epsilon_i} = x_i^{-1} \in I$.

Dans tous les cas on a donc $x_i^{\epsilon_i} \in I$, d'où $h = x_1^{\epsilon_1}...x_m^{\epsilon_m} \in I$.

On a donc $H \subset I$ pour tout sous–groupe I de G contenant X : H possède donc bien les propriétés requises. □

Si $A = \{a_1, ..., a_n\}$, on notera aussi

$$< a_1, ..., a_n >:=< A >,$$

que l'on appellera sous–groupe de G engendré par a_1,..., a_n, si $A = B \cup C$

$$< B, C >:=< A >,$$

et si $A \subset X$ et $x \in X$,

$$< A, x >:=< A, \{x\} >=< A \cup \{x\} > .$$

EXEMPLES 3.5. Ces exemples seront repris en détail par la suite.

(1) Dans $(\mathbf{Z}, +)$

$$\mathbf{Z} =< 1 >=< 2, 5 > .$$

(2) Dans le groupe symétrique $(\Sigma_n, \circ)$, on a

$$\Sigma_n =< (12), (12...n) > .$$

(3) Dans le groupe $G := O_2(\mathbf{R})$, soient A l'ensemble des rotations et soit s une symétrie orthogonale ; alors

$$G =< A, \{s\} > .$$

DÉFINITION 3.6. Le groupe G est dit **de type fini** s'il existe un sous–ensemble fini X de G tel que $< X >= G$.

Tout groupe fini est, bien sûr, de type fini ; $\mathbf{Z}$ est de type fini.

EXERCICE 3.7. Le groupe $(\mathbf{Q}, +)$ des nombres rationnels muni de l'addition habituelle n'est pas de type fini.

THÉORÈME 3.8. *Soient G un groupe et H un sous–groupe de G ; définissons une relation $\mathcal{L}_H$ sur G ("équivalence à gauche modulo H ") par*

$$x\mathcal{L}_H y \text{ si et seulement si } x^{-1}y \in H.$$

Alors $\mathcal{L}_H$ est une relation d'équivalence sur G.

De même, la relation $\mathcal{R}_H$ sur G ("équivalence à droite modulo H ") éfinie par

$$x\mathcal{R}_H y \text{ si et seulement si } yx^{-1} \in H$$

est une relation d'équivalence sur G.

DÉMONSTRATION. Pour chaque $x \in G$, on a $x^{-1}x = e \in H$, d'où $x\mathcal{L}_H x$: $\mathcal{L}_H$ est *réflexive*.

Supposons $x\mathcal{L}_H y$; alors $x^{-1}y \in H$, d'où $(x^{-1}y)^{-1} \in H$. Mais $(x^{-1}y)^{-1} = y^{-1}(x^{-1})^{-1} = y^{-1}x$, d'où $y^{-1}x \in H$ et $y\mathcal{L}_H x$: $\mathcal{L}_H$ est *symétrique*.

Supposons maintenant $x\mathcal{L}_H y$ et $y\mathcal{L}_H z$; alors $x^{-1}y \in H$ et $y^{-1}z \in H$, d'où

$$x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$$

et $x\mathcal{L}_H z$: $\mathcal{L}_H$ est *transitive*.

$\mathcal{L}_H$ est donc bien une relation d'équivalence sur G ; la preuve concernant $\mathcal{R}_H$ procède de manière similaire. □

Les classes d'équivalence selon $\mathcal{R}_H$ sont appelées **classes à droite modulo** H, et celles selon $\mathcal{L}_H$ sont appelées **classes à gauche modulo** H.

REMARQUE 3.9. Attention au fait que cette convention n'est pas uniformément respectée dans la liitérature : certains auteurs qualifient de **classes à droite modulo** H ce que nous appelons **classes à gauche modulo** H, et réciproquement.

DÉFINITION 3.10. Soit G un groupe ; un sous–groupe N du groupe G est dit **normal** (ou **distingué**) dans G si

$$(\forall x \in G)(\forall y \in N)\ xyx^{-1} \in N.$$

On note alors $N \triangleleft G$.

PROPOSITION 3.11. *Si G est abélien, tout sous–groupe de G est distingué.*

DÉMONSTRATION. Soient $x \in G$ et $n \in N$; alors

$$\begin{aligned} xnx^{-1} &= (xn)x^{-1} \\ &= (nx)x^{-1} \\ &= n(xx^{-1}) \\ &= ne \\ &= n \in N\ , \end{aligned}$$

donc $N \triangleleft G$. □

REMARQUE 3.12. La réciproque de la Proposition 3.11 est inexacte : il existe des groupes non abéliens dans lesquels tout sous–groupe est distingué (**groupes hamiltoniens** ; Dedekind les a déterminés). Le plus petit d'entre eux est le **groupe quaternionique**

$$\mathbf{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

dans lequel la multiplication est définie par $ij = -ji = k$ et $i^2 = j^2 = k^2 = -1$.

LEMME 3.13. *Un sous–groupe N de G est distingué si et seulement si*

$$\mathcal{R}_N = \mathcal{L}_N.$$

DÉMONSTRATION. Pour $x \in G$, notons $\bar{x}$ sa classe d'équivalence selon $\mathcal{L}_N$ et $\tilde{x}$ sa classe d'équivalence selon $\mathcal{R}_N$.

Supposons $N \lhd G$, et soient $x \in G$ et $y \in \bar{x}$; alors $x^{-1}y \in N$, d'où

$$yx^{-1} = x(x^{-1}y)x^{-1} \in N$$

et $x\mathcal{R}_N y$: $y \in \tilde{x}$. Il s'ensuit que $\bar{x} \subset \tilde{x}$.

Supposons maintenant $y \in \tilde{x}$; alors $yx^{-1} \in N$, d'où

$$x^{-1}y = x^{-1}(yx^{-1})x = x^{-1}(yx^{-1})(x^{-1})^{-1} \in N$$

et $x\mathcal{L}_N y$, soit $y \in \bar{x}$. On a donc $\tilde{x} \subset \bar{x}$, d'où $\tilde{x} = \bar{x}$: les classes d'équivalence selon $\mathcal{R}_N$ et selon $\mathcal{L}_N$ sont donc les mêmes, d'où $\mathcal{R}_N = \mathcal{L}_N$.

Réciproquement, supposons que $\mathcal{R}_N = \mathcal{L}_N$, et soient $x \in G$ et $n \in N$; vu que

$$x^{-1}(xn) = n \in N\ ,$$

on a $x\mathcal{L}_N xn$; mais alors $x\mathcal{R}_N xn$, soit $xnx^{-1} \in N$, et

$$N \lhd G.$$

□

DÉFINITION 3.14. Soient deux groupes G et H ; on appelle **morphisme** de G dans H une application $\varphi : G \to H$ telle que

$$\forall (g, g') \in G^2\ \varphi(gg') = \varphi(g)\varphi(g').$$

PROPOSITION 3.15.

(1) *Si $\varphi : G \to H$ et $\psi : H \to K$ sont des morphismes de groupes, alors $\psi \circ \varphi : G \to K$ en est un.*
(2) *Pour tout groupe G, l'application identité $Id_G : G \to G$ est un morphisme de groupes.*

DÉMONSTRATION. (1) Soit $(g, g') \in G^2$; on a

$$\begin{aligned}(\psi \circ \varphi)(gg') &= \psi(\varphi(gg')) \\ &= \psi(\varphi(g)\varphi(g')) \\ &= \psi(\varphi(g))\psi(\varphi(g')) \\ &= (\psi \circ \varphi)(g)(\psi \circ \varphi)(g')\ :\end{aligned}$$

$\psi \circ \varphi$ est un morphisme de groupes.

(2) Laissé en exercice.

□

LEMME 3.16. *Soient G et H deux groupes, et $\varphi : G \to H$ un morphisme de groupes ; alors*

(1) $\varphi(e_G) = e_H$
et
(2)
$$(\forall x \in G)\ \varphi(x^{-1}) = (\varphi(x))^{-1}.$$

DÉMONSTRATION. (1) On a

$$\begin{aligned} \varphi(e_G)e_H &= \varphi(e_G) \\ &= \varphi(e_G e_G) \\ &= \varphi(e_G)\varphi(e_G)\,, \end{aligned}$$

d'où $e_H = \varphi(e_G)$ d'après le Lemme 1.3.

(2)

$$\begin{aligned} \varphi(x)\varphi(x)^{-1} &= e_H \\ &= \varphi(e_G)(\text{d'après (1)}) \\ &= \varphi(xx^{-1}) \\ &= \varphi(x)\varphi(x^{-1})\ , \end{aligned}$$

d'où en effet $\varphi(x)^{-1} = \varphi(x^{-1})$. □

DÉFINITION 3.17. Soit $\varphi : G \to H$ un morphisme de groupes ; on appelle **noyau** de φ, et on note $\ker(\varphi)$, l'ensemble

$$\ker(\varphi) := \{x \in G | \varphi(x) = e_H\}.$$

On appelle **image** de φ, et on note $\mathrm{Im}(\varphi)$, l'ensemble

$$\mathrm{Im}(\varphi) := \{\varphi(x) | x \in G\}$$

PROPOSITION 3.18.

(1) $\mathrm{Im}(\varphi)$ *est un sous–groupe de H.*
(2) $\ker(\varphi)$ *est un sous–groupe distingué de G.*
(3) φ *est injectif si et seulement si* $\ker(\varphi) = \{e_G\}$.

DÉMONSTRATION. (1) $e_H = \varphi(e_G) \in \mathrm{Im}(\varphi)$, donc $\mathrm{Im}(\varphi) \neq \emptyset$.
Soient a et b deux éléments de $\mathrm{Im}(\varphi)$; on peut alors écrire $a = \varphi(x)$ et $b = \varphi(y)$, pour un couple $(x, y) \in G^2$. Il s'ensuit que

$$\begin{aligned} ab^{-1} &= \varphi(x)\varphi(y)^{-1} \\ &= \varphi(x)\varphi(y^{-1}) \\ &= \varphi(xy^{-1}) \in \mathrm{Im}(\varphi). \end{aligned}$$

En vertu de la clause (3) de la Proposition 3.1, il apparaît que $\mathrm{Im}(\varphi)$ est un sous–groupe de G.

(2) $\varphi(e_G) = e_H$, donc $e_G \in \ker(\varphi)$: $\ker(\varphi)$ n'est pas vide.

Soient x et y deux éléments de $\ker(\varphi)$; on voit que

$$\begin{aligned}\varphi(xy^{-1}) &= \varphi(x)\varphi(y^{-1}) \\ &= \varphi(x)(\varphi(y))^{-1} \\ &= e_H e_H^{-1} \\ &= e_H\ ,\end{aligned}$$

soit $xy^{-1} \in \ker(\varphi)$. Le noyau $\ker(\varphi)$ est donc bien un sous–groupe de G.

Considérons maintenant $x \in G$ et $n \in \ker(\varphi)$; alors

$$\begin{aligned}\varphi(xnx^{-1}) &= \varphi(x)\varphi(n)\varphi(x^{-1}) \\ &= \varphi(x)e_H\varphi(x^{-1}) \\ &= \varphi(x)\varphi(x^{-1}) \\ &= \varphi(xx^{-1}) \\ &= \varphi(e_G) \\ &= e_H\ ,\end{aligned}$$

d'où $xnx^{-1} \in \ker(\varphi)$: $\ker(\varphi)$ est distingué dans G.

(3) Supposons φ injectif, et soit $x \in \ker(\varphi)$; alors $\varphi(x) = e_H = \varphi(e_G)$, d'où $x = e_G$ en vertu de l'injectivité de φ. On a donc $\ker(\varphi) \subset \{e_G\}$ et donc $\ker(\varphi) = \{e_G\}$.

Réciproquement, supposons $\ker(\varphi) = \{e_G\}$, et soit $(x, y) \in G^2$ avec $\varphi(x) = \varphi(y)$. Alors

$$\begin{aligned}e_H &= \varphi(x)\varphi(x)^{-1} \\ &= \varphi(x)\varphi(y)^{-1} \\ &= \varphi(x)\varphi(y^{-1}) \\ &= \varphi(xy^{-1})\end{aligned}$$

d'où $xy^{-1} \in \ker(\varphi) = \{e_G\}$, $xy^{-1} = e_G$ et $x = y$: φ est injectif.

□

PROPOSITION 3.19. *Soient G un groupe et H un sous–groupe de G ; il existe un groupe K et un morphisme $\varphi : K \to G$ tels que* $\mathrm{Im}(\varphi) = H$.

DÉMONSTRATION. Il suffit de prendre $K = H$ et de définir φ comme l'*injection canonique*

$$\begin{aligned}\varphi\ &: H \to G \\ &\ \ h \mapsto h.\end{aligned}$$

Du fait que

$$\forall (h, h^{'}) \in H^2\ \ \varphi(hh^{'}) = hh^{'} = \varphi(h)\varphi(h^{'})\,,$$

il suit que φ est un morphisme de groupes. De plus

$$\begin{aligned}\mathrm{Im}(\varphi) &= \{\varphi(h) | h \in H\} \\ &= \{h | h \in H\} \\ &= H.\end{aligned}$$

□

L'analogue de la Proposition 3.19 pour les noyaux et les sous–groupes distingués sera établi plus tard.

LEMME 3.20. *Soit $\varphi : G \to H$ un morphisme bijectif ; alors $\varphi^{-1} : H \to G$ est un morphisme de groupes.*

DÉMONSTRATION. Soit $(x, y) \in H^2$; alors

$$\begin{aligned} \varphi(\varphi^{-1}(x)\varphi^{-1}(y)) &= \varphi(\varphi^{-1}(x))\varphi(\varphi^{-1}(y)) \\ &= xy \\ &= \varphi(\varphi^{-1}(xy)), \end{aligned}$$

d'où

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

et le résultat. □

Un morphisme bijectif est appelé **isomorphisme**.

DÉFINITION 3.21. On dit que les groupes G et H sont **isomorphes**, et on note $G \simeq H$, s'il existe un isomorphisme $\varphi : G \to H$.

THÉORÈME 3.22. *$\simeq$ est une relation d'équivalence.*

DÉMONSTRATION.

$$Id_G : G \to G$$

est un isomorphisme, donc $G \simeq G$.

Si $G \simeq H$, soit $\varphi : G \to H$ un isomorphisme ; d'après le Lemme 3.13, $\varphi^{-1} : H \to G$ est un morphisme, et il est évidemment bijectif, d'où $H \simeq G$.

Enfin, supposons $G \simeq H$ et $H \simeq K$; alors il existe des isomorphismes $\varphi : G \to H$ et $\psi : H \to K$. Il est alors très facile de voir que $\psi \circ \varphi$ est un isomorphime, d'où $G \simeq K$. □

4. Groupes quotients, théorèmes d'isomorphisme.

Dans tout ce chapitre, G désignera un groupe.

LEMME 4.1. *Un sous–groupe N de G est distingué si et seulement si $\mathcal{R}_N = \mathcal{L}_N$.*

DÉMONSTRATION. Pour $x \in G$, notons $\bar{x}$ sa classe d'équivalence selon $\mathcal{R}_N$ et $\tilde{x}$ sa classe d'équivalence selon $\mathcal{L}_N$.

Supposons $N \lhd G$, et soient $x \in G$ et $y \in \bar{x}$; alors $x^{-1}y \in N$, d'où

$$yx^{-1} = x(x^{-1}y)x^{-1} \in N$$

et $x\mathcal{L}_N y$: $y \in \tilde{x}$. Il s'ensuit que $\bar{x} \subset \tilde{x}$.

Symétriquement, supposons $y \in \tilde{x}$; alors $yx^{-1} \in N$, d'où

$$x^{-1}y = x^{-1}(yx^{-1})x = x^{-1}(yx^{-1})(x^{-1})^{-1} \in N$$

et $x\mathcal{R}_N y$, soit $y \in \bar{x}$. On a donc $\tilde{x} \subset \bar{x}$, d'où $\tilde{x} = \bar{x}$: les classes d'équivalence selon $\mathcal{R}_N$ et selon $\mathcal{L}_N$ sont donc les mêmes, d'où $\mathcal{R}_N = \mathcal{L}_N$.

Réciproquement, supposons que $\mathcal{R}_N = \mathcal{L}_N$, et soient $x \in G$ et $n \in N$; vu que

$$x^{-1}(xn) = n \in N\ ,$$

on a $x\mathcal{R}_N xn$; mais alors $x\mathcal{L}_N xn$, soit $xnx^{-1} \in N$:

$$N \lhd G.$$

□

Nous supposerons fixé, pour la suite de ce chapitre, un sous–groupe distingué N de G.

Pour $x \in G$, l'on notera $\bar{x}$ la classe d'équivalence de x pour $\mathcal{R}_N$, et $\dfrac{G}{N}$ l'ensemble de ces classes :

$$\frac{G}{N} = \{\bar{x} | x \in G\}.$$

LEMME 4.2. *Pour $\alpha \in \dfrac{G}{N}$ et $\beta \in \dfrac{G}{N}$, choisissons $x \in G$ et $y \in G$ tels que $\alpha = \bar{x}$ et $\beta = \bar{y}$; posons alors*

$$\alpha.\beta := \overline{xy}.$$

Alors la loi . est bien définie et fait de $\dfrac{G}{N}$ un groupe.

DÉMONSTRATION. Supposons $\alpha = \bar{x} = \bar{x'}$ et $\beta = \bar{y} = \bar{y'}$: alors $x\mathcal{R}_N x'$ et $y\mathcal{R}_N y'$, soit $x^{-1}x' \in N$ et $y^{-1}y' \in N$. Mais, du fait que $N \lhd G$, on a alors

$$y^{-1}(x^{-1}x')y \in N,$$

d'où

$$\begin{aligned}(xy)^{-1}(x'y') &= y^{-1}x^{-1}x'y' \\ &= (y^{-1}(x^{-1}x')y)(y^{-1}y') \\ &\in N,\end{aligned}$$

et $xy\mathcal{R}_N x'y'$. Il s'ensuit que $\overline{xy} = \overline{x'y'}$: la loi . est bien définie.

Soit $(\alpha,\beta,\gamma)\in(\frac{G}{N})^3$; écrivons $\alpha=\bar{x}$, $\beta=\bar{y}$ et $\gamma=\bar{z}$ $((x,y,z)\in G^3)$. Alors

$$\begin{aligned}(\alpha.\beta).\gamma &= (\bar{x}.\bar{y}).\bar{z}\\ &= \overline{xy}.\bar{z}\\ &= \overline{(xy)z}\\ &= \overline{x(yz)}\\ &= \bar{x}.\overline{yz}\\ &= \bar{x}.(\bar{y}.\bar{z})\\ &= \alpha.(\beta.\gamma)\ :\end{aligned}$$

la loi . est associative.

Soit $\alpha\in\frac{G}{N}$; alors $\alpha=\bar{x}$ pour un $x\in G$. Mais alors

$$\begin{aligned}\alpha.\overline{e_G} &= \bar{x}.\overline{e_G}\\ &= \overline{x.e_G}\\ &= \bar{x}\\ &= \alpha,\end{aligned}$$

et de même

$$\overline{e_G}\alpha=\alpha;$$

$e_{\frac{G}{N}}:=\overline{e_G}$ est donc un élément neutre pour la loi. .

Pour $\beta\in\frac{G}{N}$, posons $\gamma=\overline{y^{-1}}$; alors

$$\begin{aligned}\beta.\gamma &= \bar{y}.\overline{y^{-1}}\\ &= \overline{y.y^{-1}}\\ &= \overline{e_G}\\ &= e_{\frac{G}{N}}\end{aligned}$$

et de même $\gamma.\beta=e_{\frac{G}{N}}$.

Chaque élément de $\frac{G}{N}$ possède donc un symétrique pour la loi . : $(\frac{G}{N},.)$ est un groupe. □

Exemple 4.3. (Exercice) Soit $n\geq 1$ un entier ; le groupe $\frac{\mathbf{Z}}{n\mathbf{Z}}$ est d'ordre n, et

$$\frac{\mathbf{Z}}{n\mathbf{Z}}=\{\bar{0},\bar{1},..,\overline{n-1}\}=<\bar{1}>.$$

En particulier, il existe au moins un groupe à n éléments.

Remarque 4.4. Une fois de plus il s'avère qu'en Algèbre le plus difficile est souvent d'établir que les objets naturellement considérés sont bien définis ; lorsque tel est le cas, ils possèdent généralement les propriétés voulues.

Corollaire 4.5. *Soient G un groupe et N un sous–groupe distingué de G ; alors il existe un groupe K et un morphisme $\psi:G\to K$ tels que $N=\ker(\psi)$.*

DÉMONSTRATION. Prenons $K = \dfrac{G}{N}$, et définissons

$$\begin{aligned} \psi \quad : \quad & G \to K \\ & g \mapsto \bar{g}. \end{aligned}$$

Alors, pour tout $(g, g^{'}) \in G^2$

$$\begin{aligned} \psi(gg^{'}) &= \overline{gg^{'}} \\ &= \bar{g}.\bar{g^{'}} \\ &\quad \text{(par définition de la loi .)} \\ &= \psi(g)\psi(g^{'}). \end{aligned}$$

ψ est donc un morphisme de groupes (on le notera désormais $p_{G,N}$: la **projection canonique** de G sur $\dfrac{G}{N}$).

Pour $g \in G$, on a les équivalences

$$\begin{aligned} g \in \ker(\psi) &\iff \psi(g) = e_K \\ &\iff \psi(g) = e_{\frac{G}{N}} \\ &\iff \bar{g} = \overline{e_G} \\ &\iff e_G \mathcal{R} g \\ &\iff e_G^{-1} g \in N \\ &\iff e_G g \in N \\ &\iff g \in N \ , \end{aligned}$$

d'où bel et bien $N = \ker(\psi)$. □

REMARQUE 4.6. Pour tout groupe G et tout sous–groupe N distingué de G, la projection canonique $p_{G,N} : G \to \dfrac{G}{N}$ est surjective :

$$\begin{aligned} \mathrm{Im}(p_{G,N}) &= \{p_{G,N}(g) | g \in G\} \\ &= \{\bar{g} | g \in G\} \\ &= \frac{G}{N}. \end{aligned}$$

THÉORÈME 4.7. ***(Théorème d'Isomorphisme)*** *Soit $\varphi : G \to H$ un morphisme de groupes ; alors*

$$\frac{G}{\ker(\varphi)} \simeq \mathrm{Im}(\varphi).$$

DÉMONSTRATION. Définissons

$$\begin{aligned} \psi \quad : \quad & \frac{G}{\ker(\varphi)} \to \mathrm{Im}(\varphi) \\ & \bar{x} \mapsto \varphi(x). \end{aligned}$$

(1) ψ **est bien définie.**

Supposons $\bar{x} = \bar{y}$; alors $x \mathcal{R}_{\ker(\varphi)} y$, soit $x^{-1}y \in \ker(\varphi)$ et

$$\begin{aligned} \varphi(x)^{-1}\varphi(y) &= \varphi(x^{-1}y) \\ &= e_H, \end{aligned}$$

d'où $\varphi(x) = \varphi(y)$.

(2) ψ **est un morphisme de groupes.**

Soit $(a, b) \in (\frac{G}{\ker(\varphi)})^2$; écrivons $a = \bar{u}$ et $b = \bar{v}$ $((u, v) \in G^2)$; alors

$$\begin{aligned} \psi(ab) &= \psi(\bar{u}\bar{v}) \\ &= \psi(\overline{uv}) \\ &= \varphi(uv) \\ &= \varphi(u)\varphi(v) \\ &= \psi(a)\psi(b). \end{aligned}$$

(3) ψ **est injectif.**

Il suffit pour le voir de lire à rebours le raisonnement de (1) : supposons $\psi(a) = \psi(b)$ $(a = \bar{x},\ b = \bar{y})$; alors

$$\varphi(x) = \psi(\bar{x}) = \psi(a) = \psi(b) = \psi(\bar{y}) = \varphi(y),$$

d'où

$$\varphi(x^{-1}y) = \varphi(x)^{-1}\varphi(y) = e_H,$$

soit $x^{-1}y \in \ker(\varphi)$, $x\mathcal{R}_{\ker(\varphi)}y$ et $\bar{x} = \bar{y}$, d'où $a = \bar{x} = \bar{y} = b$.

(4) φ **est surjectif.**

Soit $a \in \mathrm{Im}(\varphi)$; alors $a = \varphi(x)$ pour un $x \in G$, d'où $\psi(\bar{x}) = \varphi(x) = a$ et $a \in \mathrm{Im}(\psi)$: $\mathrm{Im}(\psi) = \mathrm{Im}(\varphi)$ et ψ est surjectif.

ψ est donc un isomorphisme, d'où le résultat.

□

Corollaire 4.8. *(Deuxième Théorème d'Isomorphisme) Soient H un sous–groupe de G et K un sous–groupe distingué de G ; posons*

$$HK := \{hk | h \in H, k \in K\}.$$

Alors

(1) *HK est un sous–groupe de G*
(2) $K \triangleleft HK$
(3) $H \cap K \triangleleft H$
(4) $\frac{HK}{K} \simeq \frac{H}{H \cap K}$.

Démonstration. (1)

$e_G \in H$ and $e_G \in K$, donc $e_G e_G = e_G \in HK$: $HK \neq \emptyset$.

(2) Soit $(x, y) \in (HK)^2$; on peut écrire $x = hk$ et $y = h'k'$, avec $(h, h') \in H^2$ et $(k, k') \in K^2$. Mais alors $kk'^{-1} \in K$, d'où

$$h'(kk'^{-1})h'^{-1} \in K$$

(car K est distingué dans G), et

$$\begin{aligned} xy^{-1} &= hkk'^{-1}h'^{-1} \\ &= (hh'^{-1})(h'(kk'^{-1})h'^{-1}) \\ &\in HK\ ; \end{aligned}$$

HK est donc bien un sous–groupe de G.

(3) Soit $k \in K$; $k = e_G.K \in HK$, d'où $K \subset HK$. K est donc un sous–groupe de HK ; vu qu'il est distingué dans G, il est distingué dans HK.

(4) $H \cap K$ est un sous–groupe de G contenu dans H ; c'est donc un sous–groupe de H. Soient $x \in H \cap K$ et $h \in H$; alors $x \in H$ et $x \in K$. On a donc $hxh^{-1} \in H$ (car H est un sous–groupe de G) et $hxh^{-1} \in K$ (car $K \lhd G$), d'où $hxh^{-1} \in H \cap K$: $H \cap K$ est distingué dans H.

(5) Soit $p : G \to \dfrac{G}{K}$ la projection canonique, et soit $\varphi = p|_H$ la restriction de p à H ; φ est un morphisme de groupes.

Pour chaque $h \in H$ on a

$$\begin{aligned} \varphi(h) = e_{\frac{G}{K}} &\iff \bar{h} = \bar{e_G} \\ &\iff e_G^{-1} h \in K \\ &\iff h \in K \\ &\iff h \in H \cap K, \end{aligned}$$

d'où $\ker(\varphi) = H \cap K$.

Soit $\alpha \in \mathrm{Im}(\varphi)$; alors $\alpha = \varphi(h) = p(h) = \bar{h}$, pour un $h \in H$. Mais $h = h.e_G \in HK$, d'où $\alpha = \bar{h} \in \dfrac{HK}{K}$. On a donc $\mathrm{Im}(\varphi) \subset \dfrac{HK}{K}$.

Réciproquement, soit $\alpha \in \dfrac{HK}{K}$; alors $\alpha = \bar{x}$ pour un $x \in HK$. Ecrivons $x = hk (h \in H, k \in K)$; alors $h^{-1}x = k \in K$, d'où $\bar{h} = \bar{x}$ et

$$\alpha = \bar{x} = \bar{h} = \varphi(h) \in \mathrm{Im}(\varphi).$$

On a donc $\dfrac{HK}{K} \subset \mathrm{Im}(\varphi)$, d'où $\dfrac{HK}{K} = \mathrm{Im}(\varphi)$.

Mais alors il suit du Théorème 4.7 que

$$\frac{H}{H \cap K} = \frac{H}{\ker(\varphi)} \simeq \mathrm{Im}(\varphi) = \frac{HK}{K}.$$

□

5. Groupes monogènes, ordre d'un élément

Si G est un groupe, on appelle **ordre de** G le cardinal $|G|$ de G. Soient G un groupe et x un élément de G ; définissons

$$\begin{aligned} \varphi_x \quad : \quad & \mathbf{Z} \to G \\ & n \mapsto x^n. \end{aligned}$$

LEMME 5.1. *φ_x est un morphisme de groupes.*

DÉMONSTRATION. Pour tout $(m,n) \in \mathbf{Z}^2$,

$$\begin{aligned} \varphi_x(m+n) &= x^{m+n} \\ &= x^m x^n \\ &\quad \text{(d'après le Théorème 1.9)} \\ &= \varphi_x(m)\varphi_x(n). \end{aligned}$$

□

Il est clair que l'image $\mathrm{Im}(\varphi_x)$ de φ_x contient $x = \varphi_x(1)$.

Réciproquement, soit H un sous–groupe de G contenant x ; pour chaque $n \in \mathbf{Z}$, x^n est le même dans G et H, donc $\varphi_x(n) = x^n \in H$, et on en déduit que

$$\mathrm{Im}(\varphi_x) \subset H.$$

$\mathrm{Im}(\varphi_x)$ est donc le plus petit sous–groupe de G contenant x : $\mathrm{Im}(\varphi_x) =< x >$, le sous–groupe de G engendré par x.

Du fait que $\mathbf{Z}$ est abélien, $< x >= \mathrm{Im}(\varphi_x)$ l'est.

PROPOSITION 5.2. *On a un, et un seul, des cas suivants.*

(1) *Les $(x^n)_{n\in\mathbf{Z}}$ sont deux à deux distincts.*
Alors $< x >= \mathrm{Im}(\varphi_x) \simeq \mathbf{Z}$ est infini. Dans ce cas, on pose $\omega(x) = \infty$.

(2) *Il existe un entier $k \geq 1$ tel que $x^k = e_G$.*
Soit $\omega(x)$ le plus petit tel entier k. Alors

$$< x >= \{e_G, x, ..., x^{\omega(x)-1}\}$$

et

$$| < x > | = \omega(x).$$

De plus $x^l = e_G$ si et seulement si $\omega(x)$ divise l.

DÉMONSTRATION. φ_x étant un morphisme de groupes, $\ker(\varphi_x)$ est un sous–groupe de $\mathbf{Z}$, donc (Exemple 3.2) il existe un unique $n_x \in \mathbf{N}$ tel que $\ker(\varphi_x) = n_x\mathbf{Z}$.

Si $n_x = 0$, $\ker(\varphi_x) = \{0\}$ donc

$$\varphi_x : \mathbf{Z} \to \mathrm{Im}(\varphi_x) =< x >$$

est injectif donc bijectif d'où

$$< x >\simeq \mathbf{Z}$$

et l'on est dans le cas (1).

Lorsque $n_x \geq 1$, il apparaît que $x^k = e$ si et seulement si $\varphi_x(k) = e$, soit $k \in \ker(\varphi_x) = n_x\mathbf{Z}$, ou $n_x|k$. Il s'ensuit l'existence de $\omega(x) := n_x$, et la dernière clause.

De plus

$$\begin{aligned} x^k = x^l &\Leftrightarrow \varphi_x(k) = \varphi_x(l) \\ &\Leftrightarrow \varphi_x(k)\varphi_x(l)^{-1} = e_G \\ &\Leftrightarrow \varphi_x(k-l) = e_G \\ &\Longleftrightarrow k-l \in \ker(\varphi_x) \\ &\Longleftrightarrow k-l \in \omega(x)\mathbf{Z} \\ &\Longleftrightarrow k \equiv l\,[\omega(x)] \end{aligned}$$

En particulier les $(x^k)_{0\leq k\leq \omega(x)-1}$ sont distincts.

Soit alors $n \in \mathbf{Z}$; on peut écrire

$$n = \omega(x)q + r$$

avec $q \in \mathbf{Z}$ et $0 \leq r \leq \omega(x) - 1$. Vu que $n \equiv r[\omega(x)]$, $x^n = x^r$. Il apparaît que

$$\mathrm{Im}(\varphi_x) = \{x^0, ..., x^{\omega(x)-1}\},$$

soit

$$< x >= \{e_G, x, ..., x^{\omega(x)-1}\};$$

en particulier,

$$| < x > | = \omega(x).$$

□

Bien sûr, lorsque G est fini, l'on se trouve nécessairement dans le cas (2).

$\omega(x)$ est appelé **l'ordre** de x.

Définition 5.3. Le groupe G est dit **monogène** s'il existe un élément y de G tel que $G =< y >$.

Corollaire 5.4. *Si G est monogène, G est abélien, et il est soit isomorphe à $\mathbf{Z}$, soit d'ordre fini. Dans le second cas, si $n = |G|$, G est isomorphe à*

$$\frac{\mathbf{Z}}{n\mathbf{Z}}.$$

Démonstration. On peut supposer que $G =< x >$ avec $\omega(x) = n$. D'après la démonstration de la Proposition 5.2, $\ker(\varphi_x) = \omega(x)\mathbf{Z} = n\mathbf{Z}$.

Mais alors

$$\frac{\mathbf{Z}}{n\mathbf{Z}} = \frac{\mathbf{Z}}{\ker(\varphi_x)} \simeq \mathrm{Im}(\varphi_x) =< x >= G.$$

On peut également procéder directement : soit

$$\begin{aligned} \psi \quad : \quad & \frac{\mathbf{Z}}{n\mathbf{Z}} \to G \\ & \bar{m} \mapsto x^m. \end{aligned}$$

Il est facile de vérifier que ψ est bien défini, et qu'il s'agit d'un isomorphisme. □

Proposition 5.5. *Soient G un groupe, et x et y deux éléments de G d'ordres finis tels que $xy = yx$ (tel est par exemple le cas si G est abélien). Alors xy est d'ordre fini, et l'ordre $\omega(xy)$ divise le produit $\omega(x)\omega(y)$.*

Démonstration.

$$\begin{aligned}(xy)^{\omega(x)\omega(y)} &= x^{\omega(x)\omega(y)}y^{\omega(x)\omega(y)} \\ &\quad \text{(d'après la Proposition 1.11)} \\ &= x^{\omega(x)\omega(y)}y^{\omega(y)\omega(x)} \\ &= (x^{\omega(x)})^{\omega(y)}(y^{\omega(y)})^{\omega(x)} \\ &= (e_G)^{\omega(y)}(e_G)^{\omega(x)} \\ &= e_G.e_G \\ &= e_G.\end{aligned}$$

Donc xy est d'ordre fini et son ordre $\omega(xy)$ divise $\omega(x)\omega(y)$. □

Remarque 5.6. Ce résultat ne subsiste pas en général. Par exemple, dans le groupe symétrique Σ_3 de degré 3 (cf. plus loin), soient $x = (12)$ et $y = (23)$; alors $\omega(x) = \omega(y) = 2$ et $xy = (123)$, d'où $\omega(xy) = 3$, lequel ne divise pas $\omega(x)\omega(y) = 2.2 = 4$.

L'ordre de xy peut même être infini. Par exemple, pour α un réel tel que $\dfrac{\alpha}{\pi}$ soit irrationnel, considérons, dans le groupe $G = GL_2(\mathbf{R})$ des matrices réelles 2×2 inversibles,

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

et

$$B = \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{bmatrix}$$

Alors $\omega(A) = \omega(B) = 2$ et $\omega(AB) = \infty$ (exercice!).

6. Théorème de Lagrange

Dans tout ce chapitre, G désignera un groupe fini.

THÉORÈME 6.1. *(**Théorème de Lagrange**) Soit H un sous–groupe de G ; alors l'ordre $|H|$ de H divise l'ordre $|G|$ de G.*

DÉMONSTRATION. Pour $x \in G$, soit $\overline{x}$ sa classe modulo $\mathcal{L}_H$; alors

$$\begin{aligned} y \in \overline{x} &\Leftrightarrow x\mathcal{L}_H y \\ &\Leftrightarrow x^{-1}y \in H \\ &\Leftrightarrow (\exists h \in H) x^{-1}y = h \\ &\Leftrightarrow (\exists h \in H) y = xh. \end{aligned}$$

L'application

$$\begin{aligned} \alpha \quad : \quad & H \to \overline{x} \\ & h \mapsto xh \end{aligned}$$

est donc surjective ; en vertu du Lemme 1.3, elle est injective, donc bijective. Il en résulte que

$$|\overline{x}| = |H|;$$

chaque $\mathcal{L}_H$–classe est donc de cardinal $|H|$.

Soient C_1,...,C_r les classes d'équivalence modulo $\mathcal{L}_H$; G est réunion disjointe des $(C_i)_{1\leq i\leq r}$, d'où

$$\begin{aligned} |G| &= |C_1| + ... + |C_r| \\ &= \underbrace{|H| + ... + |H|}_{r \text{ termes}} \\ &= r|H|. \end{aligned}$$

En particulier, $|H|$ divise $|G|$. □

REMARQUE 6.2. Au passage, on a montré que le nombre de classes d'équivalence selon $\mathcal{L}_H$ est $\dfrac{|G|}{|H|}$; on appelle ce nombre **l'indice de H dans G**, et on le note $[G : H]$.

Nous aurions pu raisonner tout le long avec la relation $\mathcal{R}_H$; il serait apparu de même que le nombre de classes d'équivalence selon $\mathcal{R}_H$ est égal à l'indice

$$[G : H] = \frac{|G|}{|H|}.$$

On peut se demander si, réciproquement, pour tout diviseur d de l'ordre $|G|$ est l'ordre d'un sous–groupe de G. C'est faux en général (par exemple le groupe alterné $\mathcal{A}_4$, d'ordre 12, ne contient aucun sous–groupe d'ordre 6.

Le Théorème de Sylow (voir plus loin) constitue une réciproque partielle du Théorème de Lagrange.

THÉORÈME 6.3. *Soit x un élément de G ; alors l'ordre $\omega(x)$ de x divise l'ordre $|G|$ de G. En particulier $x^{|G|} = e_G$.*

DÉMONSTRATION. $< x >$ est un sous–groupe de G ; en lui appliquant le Théorème 6.1, on obtient que $| < x > |$ divise $|G|$, c'est–à–dire que $\omega(x)$ divise $|G|$. La dernière clause s'ensuit au moyen de la Proposition 5.2(2). □

COROLLAIRE 6.4. *Si l'ordre de G est un nombre premier p, alors G est isomorphe à $\dfrac{\mathbf{Z}}{p\mathbf{Z}}$; en particulier, il est abélien et monogène.*

DÉMONSTRATION. Du fait que $|G| = p > 1$, il existe un élément $x \neq e_G$ de G. Mais alors $\omega(x) > 1$ et $\omega(x)$ divise $|G| = p$. On a donc $\omega(x) = p$, d'où $| < x > | = p = |G|$. Il en résulte que $G =< x >$; G est donc isomorphe à $\dfrac{\mathbf{Z}}{p\mathbf{Z}}$ en vertu du Corollaire 5.4. □

PROPOSITION 6.5. *Si H est un sous–groupe d'indice 2 de G, alors H est distingué dans G.*

DÉMONSTRATION. D'après le raisonnement utilisé dans la preuve du Théorème de Lagrange, $x \in \overline{e_G}$ si et seulement si $e_G^{-1}x \in H$, soit $x \in H$; la classe $\overline{e_G}$ de e_G selon $\mathcal{L}_H$ est donc H. Vu qu'il y a en tout $[G : H] = 2$ classes pour $\mathcal{L}_H$, l'autre classe est nécessairement $G\backslash H$; les $\mathcal{L}_H$–classes d'équivalence sont donc H et $G\backslash H$.

Le même raisonnement utilisant $\mathcal{R}_H$ permet d'établir que les $\mathcal{R}_H$–classes d'équivalence sont H et $G \setminus H$.

Les deux relations d'équivalence $\mathcal{L}_H$ et $\mathcal{R}_H$ sur G ont donc les mêmes classes d'équivalence, d'où $\mathcal{R}_H = \mathcal{L}_H$. D'après le Lemme 3.13, on a bien

$$H \lhd G.$$

□

Frobenius a établi un résultat plus général : si l'indice $[G : H]$ est égal au plus petit diviseur premier de l'ordre de G, alors $H \lhd G$. Nous le démontrerons par la suite.

7. Groupes de petit (≤ 7) ordre

Soit G un groupe fini d'ordre n. Enumérons les éléments de G : $g_1 = e = e_G$, g_2,...,g_n. Il est maintenant possible de construire la **table de multiplication** de G : à l'intersection de la i–ème ligne et de la j–ème colonne, on fait figurer le produit $g_i g_j$. Il est facile de voir que deux groupes finis sont isomorphes si et seulement si leurs tables de multiplication sont de la même forme.

Le Lemme 1.3 entraîne que chaque ligne et chaque colonne de la table fait apparaître une fois et une seule chaque élément de G.

Nous allons déterminer, à isomorphisme près, les groupes d'ordre au plus 7.

n = 1.

Alors $G = \{e$ et $ee = e$, d'où la table

.	e
e	e

Tous les groupes d'ordre 1 sont donc isomorphes entre eux.

n = 2

Alors $G = \{e, a\}$ pour un $a \neq e$. D'après le Lemme 1.3 on a, vu que $a \neq e$, $aa \neq a.e = a$, d'où $aa = e$. Il en résulte la table

.	e	a
e	e	a
a	a	e

Tous les groupes d'ordre 2 sont donc isomorphes entre eux, ce qui résulte aussi du Corollaire 6.4.

n = 3

Alors $G = \{e, a, b\}$. D'après le Lemme 1.3, vu que $a \neq e$, $ab \neq eb = b$, et, du fait que $b \neq e$, $ab \neq eb = b$. On a donc $ab = e$. Le même raisonnement avec a et b inversés donne que $ba = e$. Mais alors, de $a \neq e$ et $a \neq b$ suivent $a^2 \neq ea = a$ et $a^2 \neq ab = e$, donc $a^2 = b$; on a de même $b^2 = a$. on a, vu que $a \neq e$, $a.a \neq a.e = a$, d'où $a^2 = e$. Il en résulte la table

.	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

On reconnaît la table de $\dfrac{\mathbf{Z}}{3\mathbf{Z}}$, d'où $G \simeq \dfrac{\mathbf{Z}}{3\mathbf{Z}}$, en accord avec la Proposition 5.4.

n = 4

Deux cas peuvent se présenter.

Cas 1

Il existe $a \in G$ tel que $a^2 \neq e$.

Alors $a \neq e$, donc $a^2 \neq ae = a$; on peut donc écrire

$$G = \{e, a, b, c\}$$

avec $b = a^2$. Alors, vu que $a \neq e$, $b \neq a$, on trouve que $ac \neq ec = c$, $ac \neq ae = a$ et $ac \neq aa = b$; on a donc $ac = e$, et de même $ca = e$. En considérant la deuxième

ligne, il apparaît que $ab = c$, et en considérant la deuxième colonne que $ba = c$. Il est dorénavant aisé de compléter la table

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

On reconnaît la table de $\frac{\mathbf{Z}}{4\mathbf{Z}}$, d'où $G \simeq \frac{\mathbf{Z}}{4\mathbf{Z}}$.

Cas 2

Pour chaque $a \in G$, $a^2 = e$.

Soit $G = \{e, a, b, c\}$. Vu que $b \neq e$, $ab \neq ae = a$; de même, $ab \neq b$. Comme $b \neq a$, $ab \neq aa = e$; on a donc $ab = c$. Pour la même raison $ba = c$, $ac = b$ etc., d'où la table

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

Il est facile (exercice!) de voir que ce groupe est isomorphe à $\frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}}$. On l'appelle **Groupe de Klein**.

Il y a donc, à isomorphisme près, deux groupes d'ordre 4, l'un et l'autre abéliens.

On remarquera que l'associativité n'a été nulle part utilisée. Nous avons en fait démontré qu'un **quasigroupe** (ensemble muni d'une loi de composition possédant un élément neutre et telle que la multiplication à droite et à gauche par tout élément fixé soient bijectives) d'ordre au plus 4 était un groupe. Ce n'est plus exact dès l'ordre 5 (exercice).

n = 5

5 étant premier, on a $G \simeq \frac{\mathbf{Z}}{5\mathbf{Z}}$ en vertu de la Proposition 5.4.

n = 6

Nous admettrons pour le moment le

THÉORÈME 7.1. *(Cauchy)Si le nombre premier p divise l'ordre du groupe G, alors G contient un élément d'ordre p.*

En appliquant ce résultat pour $p = 2$ puis $p = 3$, on obtient que G contient un élément x d'ordre 2 et un élément y d'ordre 3. Le sous–groupe $< y >$ de G engendré par y est donc d'ordre 3 ; en vertu de la Proposition 6.5, il est alors distingué dans G. On a donc

$$xyx^{-1} \in < y >= \{e, y, y^2\}.$$

Vu que $\omega(xyx^{-1}) = \omega(y) = 3$ (exercice !), on a, soit $xyx^{-1} = y$, soit $xyx^{-1} = y^{-1}$.

Dans le premier cas, $xy = yx$; vu que les ordres de x et de y, respectivement 2 et 3, sont premiers entre eux, on a, d'après la Proposition 5.5, $\omega(xy) = 6$; le

sous–groupe $< xy >$ engendré par xy est par conséquent d'ordre 6, c'est donc G tout entier et $G =< xy > \simeq \dfrac{\mathbf{Z}}{6\mathbf{Z}}$.

Dans le second cas, il est facile de voir que $G = \{e, y, y^2, x, xy, xy^2\}$; la relation $xy = y^{-1}x$ permet de reconstituer toute la table de multiplication de G ; il y a donc au plus une possibilité, à isomorphisme près, pour G. Or le groupe symétrique Σ_3 est d'ordre 6 et n'est pas isomorphe à $\dfrac{\mathbf{Z}}{6\mathbf{Z}}$; on trouve donc $G \simeq \Sigma_3$.

n = 7

7 étant premier, on a $G \simeq \dfrac{\mathbf{Z}}{7\mathbf{Z}}$ en vertu de la Proposition 5.4.

En conclusion, un groupe d'ordre $n \leq 7$ est soit isomorphe à $\dfrac{\mathbf{Z}}{n\mathbf{Z}}$, soit (pour $n = 4$) à $\dfrac{\mathbf{Z}}{2\mathbf{Z}} \times \dfrac{\mathbf{Z}}{2\mathbf{Z}}$, soit (pour $n = 6$) à Σ_3.

La détermination à isomorphisme près des groupes d'ordre 8 est plus délicate, et sera effectuée par la suite.

Bibliography

[1] H. E. Vaughan *Cliques and groups*, Math. Gaz. 52(1968), 347–350.