

**Introduction à la Théorie des  
Groupes  
L3 Mathématiques 2021–2022  
30 Décembre 2021**

Paul LESCOT  
Université de Rouen  
[paul.lescot@univ-rouen.fr](mailto:paul.lescot@univ-rouen.fr)



## Sommaire

- (1) Lois de composition.
- (2) Généralités sur les groupes ; puissances d'un élément.
- (3) Groupes de petit ordre.
- (4) Une caractérisation des groupes abéliens à partir des propriétés de la soustraction.
- (5) Sous-groupes, classes modulo un sous-groupe.
- (6) Groupes quotients, théorèmes d'isomorphisme.
- (7) Groupes monogènes, ordre d'un élément.
- (8) Théorème de Lagrange.
- (9) Produits directs.
- (10) Groupes diédraux.
- (11) Groupe symétrique, actions de groupes, groupe alterné.
- (12) Centre, automorphismes, automorphismes intérieurs
- (13) Classes de conjugaison, équation des classes.
- (14) Théorème de Sylow (1).
- (15) Groupes d'ordres spéciaux.
- (16) Groupes d'ordre au plus 15 (sauf 12).
- (17) Théorème de Sylow (2).
- (18) Exemple d'application : les groupes d'ordre 12.
- (19) Groupes abéliens finis.

### 1. Lois de composition

DÉFINITION 1.1. Soit  $E$  un ensemble ; on appelle *loi de composition* sur  $E$  une application

$$\varphi : E \times E \rightarrow E.$$

On notera souvent

$$a * b := \varphi(a, b).$$

Dans tout ce chapitre,  $E$  désignera un ensemble et  $*$  une loi de composition fixée sur  $E$ . Par abus de langage, nous écrirons parfois “ $E$ ” au lieu de “le couple  $(E, *)$ ”.

On appellera **ordre** de  $E$ , et on notera  $|E|$ , le cardinal de  $E$ .

Une loi de composition peut posséder diverses propriétés, que nous énumérons ci-dessous.

**(G1)** La loi  $*$  est dite *associative* si

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

DÉFINITION 1.2. L'élément  $e$  de  $E$  est dit *neutre à droite* si  
**(G'2)**

$$(\forall a \in E) a * e = a.$$

DÉFINITION 1.3. L'élément  $e$  de  $E$  est dit *neutre à gauche* si  
**(G''2)**

$$(\forall a \in E) e * a = a.$$

DÉFINITION 1.4. L'élément  $e$  de  $E$  est dit *neutre* s'il est à la fois neutre à droite et neutre à gauche, soit

**(G2)**

$$(\forall a \in E) a * e = e * a = a.$$

LEMME 1.5. Soient  $e_1$  un élément neutre à droite et  $e_2$  un élément neutre à gauche ; alors  $e_1 = e_2$ .

DÉMONSTRATION. On a par hypothèse

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

et

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

Prenons  $a = e_2$  dans la première égalité ; il vient

$$e_2 * e_1 = e_1.$$

2

En prenant  $a = e_1$  dans la seconde égalité, il vient

$$e_2 * e_1 = e_1.$$

Mais alors

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

d'où

$$e_1 = e_2.$$

□

En particulier, il existe au plus un élément neutre ; l'expression "l'élément neutre" est donc sans ambiguïté.

EXEMPLE 1.6. Soit  $E$  un ensemble ayant au moins deux éléments ; définissons une loi  $*$  sur  $E$  par

$$(\forall (a, b) \in E \times E) a * b = a.$$

Alors il n'existe pas d'élément neutre à gauche pour  $*$  mais il existe un élément neutre à droite (en fait chaque élément de  $E$  l'est).

Remarquons que cette loi  $*$  est associative :

$$(a * b) * c = a * c = a = a * (b * c).$$

DÉFINITION 1.7. On dit que  $E$  vérifie l'*Axiome des Symétries* relatif à  $e \in E$  si

(G3)

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

DÉFINITION 1.8. On dit que  $E$  vérifie l'*Axiome des Symétries à Droite* relatif à  $e \in E$  si

(G'3)

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

DÉFINITION 1.9. On dit que  $E$  vérifie l'*Axiome des Symétries à Gauche* relatif à  $e \in E$  si

(G''3)

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

DÉFINITION 1.10. La loi  $*$  est dite **commutative** si

(G4)

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

DÉFINITION 1.11. On dit que  $E$ , muni de la loi  $*$ , est un **semi-groupe** si  $E \neq \emptyset$  et la loi  $*$  est associative (c'est-à-dire que l'on a **(G1)**).

DÉFINITION 1.12. On dit que  $E$ , muni de la loi  $*$ , est un **monoïde** si la loi  $*$  est associative (c'est-à-dire que l'on a **(G1)**) et possède un élément neutre (c'est-à-dire que l'on a **(G2)**).

DÉFINITION 1.13.

Pour chaque  $a \in E$ , définissons deux applications

$$\begin{aligned} L_a & : E \rightarrow E \\ x & \mapsto a * x. \end{aligned}$$

(multiplication à gauche)

et

$$\begin{aligned} R_a & : E \rightarrow E \\ x & \mapsto x * a. \end{aligned}$$

(multiplication à droite).

DÉFINITION 1.14. On dit que  $E$  est un **quasigroupe** si  $E \neq \emptyset$  et, pour chaque  $a \in E$ ,  $L_a$  et  $R_a$  sont bijectives.

DÉFINITION 1.15. On dit que  $E$  est un **groupe** si l'on a **(G1)**, **(G2)** et **(G3)**.

THÉORÈME 1.16. *On a équivalence entre*

(i)  *$E$  est un groupe*

et

(ii)  *$E$  est un quasigroupe associatif (en d'autres termes, à la fois un semigroupe et un quasigroupe).*

DÉMONSTRATION. (i)  $\implies$  (ii) :

Puisque  $E$  est un groupe, on a **(G1)** d'où l'associativité. Soit maintenant  $a \in E$ . Pour  $b \in E$ , cherchons à résoudre l'équation  $L_a(c) = b$ , soit  $a * c = b$ .

D'après **(G3)**, il existe  $d \in E$  tel que  $a * d = d * a = e$ . De  $a * c = b$  suit

$$\begin{aligned}
c &= e * c \\
&= (d * a) * c \\
&= d * (a * c) \\
&= d * b,
\end{aligned}$$

d'où l'unicité de  $c$ .

Réciproquement, soit  $c = d * b$ ; alors

$$\begin{aligned}
a * c &= a * (d * b) \\
&= (a * d) * b \\
&= e * b \\
&= b,
\end{aligned}$$

et  $c$  convient.

$L_a(c) = b$  équivaut donc à  $c = d * b$  :  $L_a$  est bijective.

Le raisonnement est analogue concernant  $R_a$  ; sans surprise, on trouve que  $R_a(c) = b$  équivaut à  $c = b * d$ .  $R_a$  est donc bijective :  $E$  est un quasigroupe.

(ii)  $\implies$  (i) :

$E \neq \emptyset$ , donc il existe  $a \in E$ . Vu que  $L_a$  est bijective, il existe  $e \in E$  tel que  $L_a(e) = a$ , soit  $a * e = a$ . Soit maintenant  $x \in E$  ; vu que  $R_a$  est bijective, il existe  $y \in E$  tel que  $R_a(y) = x$ , soit  $y * a = x$ . Mais alors

$$\begin{aligned}
x * e &= (y * a) * e \\
&= y * (a * e) \\
&= y * a \\
&= x,
\end{aligned}$$

soit

$$(\forall x \in E) x * e = x :$$

$e$  est élément neutre à droite.

En particulier,  $e * e = e$ .

Soit maintenant  $z \in E$  ; vu que  $L_e$  est bijective, il existe  $t \in E$  tel que  $L_e(t) = z$ , soit  $e * t = z$ . Mais alors

$$\begin{aligned}
 e * z &= e * (e * t) \\
 &= (e * e) * t \\
 &= e * t \\
 &= z ,
 \end{aligned}$$

et

$$(\forall z \in E) e * z = z ;$$

$e$  est neutre à gauche, donc neutre et on a **(G2)**.

Soit maintenant  $a \in E$  ; vu que  $L_a$  est bijectif, il existe  $b \in E$  tel que  $L_a(b) = e$ .  $L_b$  étant bijective, il existe  $c \in E$  tel que  $L_b(c) = e$ . On a donc  $a * b = e$  et  $b * c = e$ , d'où

$$\begin{aligned}
 c &= e * c \\
 &= (a * b) * c \\
 &= a * (b * c) \\
 &= a * e \\
 &= a ,
 \end{aligned}$$

et

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

On a donc

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

soit **(G3)** :  $E$  est un groupe.

Une autre variation sur les axiomes de groupe est possible.

**THÉORÈME 1.17.**  $E$  est un groupe si et seulement si on a **(G1)**, **(G'2)** et **(G'3)**.

**DÉMONSTRATION.**  $e$  étant neutre à droite, on a  $e * e = e$ . Soit  $a \in E$  ; par hypothèse, il existe  $b \in E$  tel que  $a * b = e$ , et il existe  $c \in E$  tel que  $b * c = e$ , d'où

$$\begin{aligned}
 a &= a * e \\
 &= a * (b * c) \\
 &= (a * b) * c \\
 &= e * c
 \end{aligned}$$

et



$$\begin{aligned}
 e * a &= e * (e * c) \\
 &= (e * e) * c \\
 &= e * c \\
 &= a,
 \end{aligned}$$

donc  $e$  est neutre à gauche et on a **(G2)**.

Soit maintenant  $a \in E$  ; on a vu qu'existe  $b \in E$  tel que  $a * b = e$ , qu'existe  $c \in E$  tel que  $b * c = e$ , et que  $a = e * c$ . On a donc  $a = c$  et  $b * a = b * c = e$  ; on a donc **(G3)**, donc  $E$  est un groupe.

L'implication réciproque est évidente.  $\square$

De même  $E$  est un groupe si et seulement si on a **(G1)**, **(G'2)** et **(G'3)**.

En revanche la conjonction de **(G1)**, **(G'2)** et **(G'3)** n'entraîne pas que  $E$  soit un groupe (exercice ; *indication* : reprendre l'Exemple 1.6).

**2. Généralités sur les groupes ; puissances d'un élément**

DÉFINITION 2.1. Rappelons que l'on appelle groupe un ensemble  $G$  muni d'une loi de composition interne  $*$  satisfaisant aux axiomes suivants :

**(G1)** *Associativité*

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

**(G2)** *Élément neutre*

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

et

**(G3)** *Symétriques*

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

Si on a de plus

**(G4)**

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

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

REMARQUES 2.2. (1) L'élément neutre  $e$  est unique.

Il suffit d'appliquer la remarque suivant le Lemme 1.5.

Ainsi, sous l'hypothèse **(G2)**, il n'y a aucune ambiguïté dans l'énoncé de **(G3)**.

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

Il suffit de reprendre une partie de la démonstration du Théorème 1.17. En effet, supposons

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

et

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

Il vient

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

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  $\mathbf{(G3)}$  par  $\mathbf{(G'3)}$ .

En effet, il est clair que  $\mathbf{(G3)}$  entraîne  $\mathbf{(G'3)}$ , donc la conjonction de  $\mathbf{(G1)}$ ,  $\mathbf{(G2)}$  et  $\mathbf{(G3)}$  entraîne celle de  $\mathbf{(G1)}$ ,  $\mathbf{(G2)}$  et  $\mathbf{(G'3)}$ .

Réciproquement, supposons  $\mathbf{(G1)}$ ,  $\mathbf{(G2)}$  et  $\mathbf{(G'3)}$  satisfaits, et démontrons  $\mathbf{(G3)}$ .

Du fait que  $\mathbf{(G2)}$  entraîne  $\mathbf{(G'2)}$ , on a  $\mathbf{(G1)}$ ,  $\mathbf{(G'2)}$  et  $\mathbf{(G'3)}$  d'où  $\mathbf{(G3)}$  en vertu du Théorème 1.17.

L'on peut aussi procéder directement. Soit  $a \in G$  ; d'après  $\mathbf{(G'3)}$ , il existe  $b \in G$  tel que  $a * b = e$ , et il existe  $c \in G$  tel que  $b * c = e$ . Mais alors

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

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  $a'' = b' = c = a$ , 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  $1$ .

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 2.3. *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. Il suffit d'appliquer le Théorème 1.16. □

PROPOSITION 2.4. (1)  $(\forall x \in G) (x')' = x$ .  
 (2)  $\forall (x, y) \in G^2 (xy)' = y'x'$ .

DÉMONSTRATION.

- (1) Cela a été établi incidemment lors de la justification de la Remarque 2.2.(3). En effet, on a vu que

$$(\forall a \in G) a'' = a.$$

(2)

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

La conclusion suit alors du Lemme 2.3. □

DÉFINITION 2.5. (*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

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

REMARQUES 2.6. Dans un groupe  $G$ , le produit vide est conventionnellement considéré comme égal à l'élément neutre  $e_G$ , ce qui est cohérent avec la définition  $x^0 := e_G$ .

Par ailleurs on a, pour chaque  $x$

$$x^1 = x^{0+1} = x^0 x = e x = x$$

et

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

PROPOSITION 2.7.  $(\forall x \in G) (\forall (m, n) \in \mathbf{N}^2) x^{m+n} = x^m x^n$ .

REMARQUE 2.8. Cette proposition reste exacte dans un monoïde (et même dans un semigroupe en se restreignant à  $m \geq 1$  et  $n \geq 1$ ).

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

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

par récurrence sur  $n$ .

Pour  $n = 0$  c'est évident :

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

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

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

soit  $(\mathcal{P}_{n+1})$ . □

LEMME 2.9. Pour chaque  $x \in G$  et chaque  $n \in \mathbf{Z}$ ,

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

DÉMONSTRATION.

1°)  $n \in \mathbf{N}$ .

Nous allons procéder par récurrence sur  $n$ .

Si  $n = 0$  on a bien

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

et

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

Supposons le résultat établi au rang  $n$  ; alors

$$\begin{aligned} (x^{n+1})^{-1} &= (x^n x)^{-1} \\ &\quad \text{(d'après la Définition 2.5)} \\ &= x^{-1}(x^n)^{-1} \\ &\quad \text{(d'après la Proposition 2.4(2))} \\ &= x^{-1}(x^{-1})^n \\ &\quad \text{(par l'hypothèse de récurrence)} \\ &= (x^{-1})^1(x^{-1})^n \\ &= (x^{-1})^{1+n} \\ &\quad \text{(d'après la Proposition 2.7)} \\ &= (x^{-1})^{n+1} ; \end{aligned}$$

de plus, il suit de la Définition 2.5 que

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

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

2°)  $n \leq -1$ .

Alors

$$\begin{aligned} (x^n)^{-1} &= ((x^{-1})^{-n})^{-1} \\ &\quad \text{(Définition 2.5)} \\ &= ((x^{-1})^{-1})^{-n} \text{(d'après le résultat de 1°) appliqué à } -n \in \mathbf{N} \\ &= x^{-n} \end{aligned}$$

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 2.7.

**THÉORÈME 2.10.**  $(\forall x \in G)(\forall (m, n) \in \mathbf{Z}^2) x^{m+n} = x^m x^n$ .

**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°)  $-m \leq n \leq -1$

Alors

$$\begin{aligned}
 x^{m+n}(x^n)^{-1} &= x^{m+n}(x^{-1})^n \\
 &\quad \text{(Lemme 2.9)} \\
 &= x^{m+n}((x^{-1})^{-1})^{-n} \\
 &\quad \text{(en vertu de la Définition 2.5)} \\
 &= x^{m+n}x^{-n} \\
 &= x^{(m+n)+(-n)} \\
 &\quad \text{(car } m+n \geq 0 \text{ et } -n \geq 0) \\
 &= x^m,
 \end{aligned}$$

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°)  $n \leq -m - 1$

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

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

□

COROLLAIRE 2.11.  $(\forall x \in G)(\forall (m, n) \in \mathbf{Z}^2) x^{mn} = (x^m)^n$ .

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

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

Supposons le résultat établi au rang  $n$  ; alors

$$\begin{aligned}
 (x^m)^{n+1} &= (x^m)^n x^m \\
 &= x^{mn} x^m \\
 &\quad \text{(par l'hypothèse de récurrence)} \\
 &= x^{mn+m} \\
 &\quad \text{(Théorème 2.10)} \\
 &= x^{m(n+1)},
 \end{aligned}$$

soit le résultat au rang  $n + 1$ .

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

$$\begin{aligned}
 (x^m)^n &= ((x^m)^{-1})^{-n} \\
 &\quad \text{(d'après la Définition 2.5)} \\
 &= ((x^{-1})^m)^{-n} \\
 &\quad \text{(d'après le Lemme 2.9)} \\
 &= (x^{-1})^{m(-n)} \\
 &\quad \text{(car } -n \in \mathbf{N}) \\
 &= (x^{-1})^{-mn} \\
 &= x^{-(-mn)} \\
 &\quad \text{(d'après le Lemme 2.9)} \\
 &= x^{mn}.
 \end{aligned}$$

□



COROLLAIRE 2.12. 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 tout d'abord par récurrence sur  $n \in \mathbf{N}$  que

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

Pour  $n = 0$  on a

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

soit  $(\mathbf{I}'_0)$ .

Supposons  $(\mathbf{I}'_n)$  : alors

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

soit  $(\mathbf{I}'_{n+1})$  et le résultat par récurrence.

Nous allons utiliser cette égalité afin d'établir que

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

C'est clair pour  $n = 0$  :

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

Supposons l'égalité vraie au rang  $n$  ; alors

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

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 2.13.** *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 du Corollaire 2.12 est satisfaite par tout couple  $(a, b) \in G^2$ . □

Au vu du Théorème 2.10, du Corollaire 2.11 et du Corollaire 2.13, l'on peut dire que, dans un groupe abélien, l'opération "puissance"

$((n, x) \mapsto x^n)$  possède toutes les propriétés habituelles.

Le résultat suivant sera démontré autrement par la suite.

LEMME 2.14. Si  $(a, b) \in G^2$ , alors

$$(\forall n \in \mathbf{Z}) (a^{-1}ba)^n = a^{-1}b^n a.$$

DÉMONSTRATION. Etablissons d'abord par récurrence sur  $n \in \mathbf{N}$  que

$$(\forall n \in \mathbf{N}) (a^{-1}ba)^n = a^{-1}b^n a. \quad (\mathbf{I}_n)$$

Pour  $n = 0$  on a bien

$$(a^{-1}ba)^0 = e = a^{-1}a = a^{-1}ea = a^{-1}b^0 a.$$

Supposons la propriété vraie au rang  $n$  ; alors

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

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

Pour  $n \leq -1$  on a donc

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

D'où le résultat. □

Lorsque  $a$  et  $b$  commutent, on retrouve la proposition  $(\mathbf{I}'_n)$  établie dans le cours de la démonstration du Corollaire 2.12.

### 3. Groupes de petit ordre

Soit  $G$  un groupe fini d'ordre  $n$ . Enumérons les éléments de  $G$  :  $g_1 = e = e_G, g_2, \dots, g_n$ . On peut maintenant 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  $g_i g_j$ .

Le Lemme 2.3 entraîne que chaque ligne et chaque colonne de la table fait apparaître une fois et une seule chaque élément de  $G$ .

Nous allons déterminer les tables de multiplication des groupes d'ordre au plus 4.

**n = 1.**

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

.	$e$
$e$	$e$

**n = 2**

Alors  $G = \{e, a\}$  pour un  $a \neq e$ . D'après le Lemme 2.3 on a, vu que  $a \neq e$ ,  $aa \neq a.e = a$ , d'où  $aa = e$ . Il en résulte la table

.	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

On reconnaît la table de  $(\frac{\mathbf{Z}}{2\mathbf{Z}}, +)$ .

**n = 3**

Alors  $G = \{e, a, b\}$ . D'après le Lemme 2.3, vu que  $a \neq e$ ,  $ab \neq ae = a$ , 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  $b^2 = a$ . 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  $(\frac{\mathbf{Z}}{3\mathbf{Z}}, +)$ .

**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  $(\frac{\mathbf{Z}}{4\mathbf{Z}}, +)$ .

### 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 :

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

On reconnaît la table de  $(\frac{\mathbf{Z}}{2\mathbf{Z}}, +) \times (\frac{\mathbf{Z}}{2\mathbf{Z}}, +)$ .

Il y a donc deux groupes essentiellement distincts 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 unitaire** (ensemble muni  
 d'une loi de composition possédant un élément neutre et telle que la  
 multiplication à droite et à gauche par chaque élément fixé soient bi-  
 jectives, en d'autres termes satisfaisant **(G2)** et la Définition 1.14)  
 d'ordre au plus 4 est un groupe. Ce n'est plus exact dès l'ordre 5; par  
 exemple

.	$e$	$a$	$b$	$c$	$d$
$e$	$e$	$a$	$b$	$c$	$d$
$a$	$a$	$e$	$c$	$d$	$b$
$b$	$b$	$d$	$e$	$a$	$c$
$c$	$c$	$b$	$d$	$e$	$a$
$d$	$d$	$c$	$a$	$b$	$e$

est la table d'un quasigroupe unitaire d'ordre 5. Il ne s'agit pas d'un groupe vu la non-associativité :

$$(ab)b = cb = d \neq a = ae = a(bb).$$

En revanche on a :

**THÉORÈME 3.1.** *Tout quasigroupe unitaire commutatif d'ordre 5 est un groupe.*

**DÉMONSTRATION.** Soit  $G$  un quasigroupe unitaire commutatif d'ordre 5 ; notons  $e$  son élément neutre.

Par l'absurde, supposons que  $xx = e$  pour chaque  $x \in G$ . Écrivons  $G = \{e, a, b, c, d\}$  ; vu que  $a \neq e$  on a  $ab \neq eb = b$ , et de même  $b \neq e$  entraîne  $ab \neq ae = a$ . Du fait que  $b \neq a$  on peut écrire  $ab \neq aa = e$ , donc  $ab \notin \{e, a, b\}$  d'où  $ab \in \{c, d\}$ . En permutant éventuellement  $c$  et  $d$  on peut supposer que  $ab = c$ . Alors  $ba = ab = c$ . Il s'ensuit que  $bd$  n'est égal ni à  $bb = e$ , ni à  $ba = c$ , ni à  $be = b$ , ni à  $ed = d$ , donc  $bd = a$ .  $ad$  doit alors être différent de  $ae = a$ , de  $aa = e$ , de  $ab = c$  et de  $ed = d$  ; on a donc  $ad = b$ . Mais alors  $cd$  diffère de  $c = ce$ ,  $e = cc$ ,  $b = ad$ ,  $d = ed$  et  $a = bd$ , une contradiction.

Il existe donc  $x \in G$  tel que  $xx \neq e$ . Alors  $x \neq e$  donc  $xx \neq x$ . Soit  $y = xx$  ; alors  $G = \{e, x, y, z, t\}$  avec deux autres éléments  $z$  et  $t$ . Vu que  $z \neq t$ , on a  $xz \neq xt$ , donc au moins l'un de  $xz$  et  $xt$  n'est pas égal à  $e$ . En permutant éventuellement  $z$  et  $t$ , on peut supposer que  $xz \neq e$ . Mais alors  $xz$  est distinct de  $e$ , de  $xe = x$ , de  $xx = y$  et de  $ez = z$ , d'où

$$xz = t.$$

Supposons un moment  $xy = e$  ; alors  $xt$  n'est égal à aucun de  $xx = y$ ,  $xe = x$ ,  $xy = e$  et  $xz = t$ , donc  $xt = z$ . Il apparaît que  $yz$  ne vaut ni  $ye = y$ , ni  $yx = e$ , ni  $ez = z$ , ni  $xz = t$  ; on a donc  $yz = x$ . Mais alors  $yt$  ne peut valoir ni  $y = ye$ , ni  $e = yx$ , ni  $t = et$ , ni  $z = xt$ , ni  $x = yz$ , une contradiction.

$xy$  est donc différent de  $e$ , de  $x = xe$ , de  $y = ey$  et de  $xz = t$  ; il s'ensuit que

$$xy = z,$$

d'où

$$yx = z.$$

Mais alors  $xt$  ne vaut aucun de  $x = xe$ ,  $y = xy$ ,  $z = yx$  et  $t = xt$ , d'où  $xt = e$  et  $tx = e$ .

De ce fait  $yt$  est distinct de  $y = ye$ ,  $z = yx$ ,  $t = et$  et  $e = xt$ , donc  $yt = x$  et  $ty = x$ .

Il est alors facile de compléter la table :  $yz = e$ , donc  $zy = e$ . Il s'ensuit que  $yy = t$ , d'où  $tz = y$  et  $zt = y$ . Mais alors  $zz = x$ , et la table est complète :

.	$e$	$x$	$y$	$z$	$t$
$e$	$e$	$x$	$y$	$z$	$t$
$x$	$x$	$y$	$z$	$t$	$e$
$y$	$y$	$z$	$t$	$e$	$x$
$z$	$z$	$t$	$e$	$x$	$y$
$t$	$t$	$e$	$x$	$y$	$z$

Il est facile de vérifier que cette table est associative en étudiant chaque cas particulier de la relation  $(uv)w = u(vw)$ ; il est encore plus facile de reconnaître la table de  $(\frac{\mathbf{Z}}{5\mathbf{Z}}, +)$ .  $G$  est donc un groupe.  $\square$

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

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

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

Il apparaît que pour tout élément  $g$  de  $G$

$$g - g = g + (-g) = 0.$$

En outre, 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 4.1.** (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, comme vu ci-dessus

$$0 = u - u$$

soit

$$0 = u * u$$

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 apparait que, pour tout  $a \in G$ ,

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

(1)  **$+$  est commutative**

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

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

(2)  **$e$  est élément neutre pour  $+$**

Soit  $a \in G$  ;

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

4. UNE CARACTÉRISATION DES GROUPES ABÉLIENS À PARTIR DES PROPRIÉTÉS DE LA SOUSTRACTION

(3)  $+$  est associative

Soient  $a, b$  et  $c$  trois éléments de  $G$  ; alors

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

(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 **(G4)**, (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.

### 5. Sous-groupes, classes modulo un sous-groupe.

Dans tout ce chapitre,  $G$  désignera un groupe noté multiplicativement, sauf dans les Exemples 5.2 et 5.6.(1), ainsi que l'exercice 5.8 ; l'inverse d'un élément  $x$  de  $G$  sera noté  $x^{-1}$ .

On appelle *sous-groupe* de  $G$  une partie  $H$  de  $G$  formant un groupe pour la restriction de la loi de composition de  $G$ . On notera parfois  $H < G$  pour indiquer que  $H$  est un sous-groupe de  $G$ .

PROPOSITION 5.1. *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)  $\implies$  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)  $\implies$  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 2.3 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)  $\implies$  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 5.2.  $G = \mathbf{Z}$ , ensemble des entiers relatifs, muni de l'addition habituelle.

Il est facile de voir que, pour chaque  $n \in \mathbf{N}$ ,

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

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

$$ny = \underbrace{n + \dots + n}_{y \text{ termes}} \in H.$$

$$(2) \ y = 0.$$

Alors  $ny = 0 \in H$ .

$$(3) \ y \leq -1.$$

Alors, du fait que  $n \in H$ ,  $-n \in H$  et

$$\begin{aligned} ny &= (-n)(-y) \\ &= \underbrace{(-n) + \dots + (-n)}_{-y \text{ termes}} \end{aligned}$$

$\in H$ .

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  $0 \leq r < n$ .

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 5.3.** *Soit  $I$  un ensemble non vide, et 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 5.1(3), donc  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $G$ .

PROPOSITION 5.4. *Soit  $X$  une partie de  $G$  ; il existe un plus petit sous-groupe de  $G$  contenant  $X$ . On le note  $\langle X \rangle$ , et on l'appelle le **sous-groupe de  $G$  engendré par  $X$** .*

DÉMONSTRATION. Soit  $\mathcal{F}_X$  l'ensemble des sous-groupes  $H$  de  $G$  tels que

$X \subset H$  ;  $\mathcal{F}_X$  n'est pas vide car  $G \in \mathcal{F}_X$ . En vertu de la Proposition 5.3,

$$\langle X \rangle := \bigcap_{H \in \mathcal{F}_X} H$$

est un sous-groupe de  $G$ . Vu que pour chaque  $H \in \mathcal{F}_X$  on a  $X \subset H$ , il apparaît que  $X \subset \bigcap_{H \in \mathcal{F}_X} H = \langle X \rangle$  ;  $\langle X \rangle$  est donc un sous-groupe de  $G$  contenant  $X$ .

Réciproquement, si  $H$  est un sous-groupe de  $G$  contenant  $X$ , on a  $H \in \mathcal{F}_X$ , donc (par définition de  $\langle X \rangle$ )  $\langle X \rangle \subset H$ .

D'où le résultat.  $\square$

On peut identifier explicitement le sous-groupe engendré par  $X$  :

THÉORÈME 5.5. *Soit  $X$  un sous-ensemble de  $G$  ; alors*

$$\langle X \rangle = \{x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \mid n \geq 0, x_i \in X, \epsilon_i \in \{-1, 1\}\}.$$

DÉMONSTRATION. Soit

$$H := \{x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \mid n \geq 0, x_i \in X, \epsilon_i \in \{-1, 1\}\}.$$

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

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

et

$$v = y_1^{\epsilon'_1} \dots y_m^{\epsilon'_m},$$

les  $x_i$  et  $y_i$  appartenant à  $H$  et les  $\epsilon_i$  et  $\epsilon'_i$  à  $\{-1, 1\}$ . Mais alors

$$uv^{-1} = x_1^{\epsilon_1} \dots x_n^{\epsilon_n} y_m^{-\epsilon'_m} \dots y_1^{-\epsilon'_1} \in H;$$

$H$  est donc bien un sous-groupe de  $G$ .

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

Il en résulte que  $\langle X \rangle \subset H$ .

Réciproquement, soit maintenant  $h \in H$ ;  $h$  s'écrit

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

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

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

Dans tous les cas on a donc  $x_i^{\epsilon_i} \in \langle X \rangle$ , d'où

$$h = x_1^{\epsilon_1} \dots x_m^{\epsilon_m} \in \langle X \rangle.$$

On a donc  $H \subset \langle X \rangle$  d'où  $H = \langle X \rangle$ . □

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

$$\langle a_1, \dots, a_n \rangle := \langle A \rangle,$$

que l'on appellera sous-groupe de  $G$  engendré par  $a_1, \dots, a_n$ ; si  $A = B \cup C$ , on notera

$$\langle B, C \rangle := \langle A \rangle,$$

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

$$\langle A, x \rangle := \langle A, \{x\} \rangle = \langle A \cup \{x\} \rangle.$$

**EXEMPLES 5.6.** Ces exemples seront repris en détail par la suite.

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

$$\mathbf{Z} = \langle 1 \rangle = \langle 2, 5 \rangle.$$

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

$$\Sigma_n = \langle (12), (12\dots n) \rangle.$$

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

$$G = \langle A, s \rangle.$$

**DÉFINITION 5.7.** On appelle **partie génératrice** du groupe  $G$  un sous-ensemble  $X$  de  $G$  tel que  $\langle X \rangle = G$ .

Le groupe  $G$  est dit **de type fini** s'il existe une partie génératrice finie de  $G$ .

Tout groupe fini  $G$  est, bien sûr, de type fini (il suffit de prendre  $X = G$ );  $\mathbf{Z}$  est de type fini ( $\mathbf{Z} = \langle 1 \rangle$ ).

Tout groupe de type fini est fini ou dénombrable ; en particulier,  $O_2^+(\mathbf{R})$  et  $O_2(\mathbf{R})$  ne sont pas de type fini (exercice).

EXERCICE 5.8. Le groupe  $(\mathbf{Q}, +)$  des nombres rationnels muni de l'addition habituelle n'est pas de type fini.

THÉORÈME 5.9. 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

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

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

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

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

est une relation d'équivalence sur  $G$ .

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

Supposons  $x\mathcal{L}_Hy$  ; 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  $y\mathcal{L}_Hx : \mathcal{L}_H$  est symétrique.

Supposons maintenant  $x\mathcal{L}_Hy$  et  $y\mathcal{L}_Hz$  ; 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  $x\mathcal{L}_Hz : \mathcal{L}_H$  est transitive.

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

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

DÉFINITION 5.11. 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 5.12. *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 5.13. La réciproque de la Proposition 5.12 est inexacte : il existe des groupes non abéliens dans lesquels tout sous-groupe est distingué (**groupes hamiltoniens**) ; nous exposerons plus loin leur classification, due à Dedekind (dans le cas fini) et à Baer (dans le cas général). 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 5.14. *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  $N \triangleleft G$ , 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  $x\mathcal{R}_Ny : y \in \tilde{x}$ . 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  $x\mathcal{L}_Ny$ , 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  $x\mathcal{L}_Nxn$  ; mais alors  $x\mathcal{R}_Nxn$ , soit  $xnx^{-1} \in N$ , et

$$N \triangleleft G.$$

□

DÉFINITION 5.15. Soient deux groupes  $G$  et  $H$  ; on appelle **morphisme** de  $G$  dans  $H$  une application  $\varphi : G \rightarrow H$  telle que

$$\forall (g_1, g_2) \in G^2 \quad \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2).$$

PROPOSITION 5.16.

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

DÉMONSTRATION. (1) Soit  $(g_1, g_2) \in G^2$  ; on a

$$\begin{aligned} (\psi \circ \varphi)(g_1g_2) &= \psi(\varphi(g_1g_2)) \\ &= \psi(\varphi(g_1)\varphi(g_2)) \\ &= \psi(\varphi(g_1))\psi(\varphi(g_2)) \\ &= (\psi \circ \varphi)(g_1)(\psi \circ \varphi)(g_2) : \end{aligned}$$

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

- (2) Laissé en exercice.

□

LEMME 5.17. Soit  $\varphi : G \rightarrow H$  un morphisme bijectif ; alors  $\varphi^{-1} : H \rightarrow G$  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 injectif est appelé **plongement**.

Un morphisme bijectif est appelé **isomorphisme**.

DÉFINITION 5.18. On dit que les groupes  $G$  et  $H$  sont **isomorphes**, et on note  $G \simeq H$ , s'il existe un isomorphisme  $\varphi : G \rightarrow H$ .

Il est facile de voir que deux groupes finis sont isomorphes si et seulement si leurs tables de multiplication sont de la même forme.

THÉORÈME 5.19.  $\simeq$  est une relation d'équivalence sur la classe des groupes.

REMARQUE 5.20. Il n'existe pas d'ensemble de tous les groupes ; je ne m'étendrai pas sur ce point.

DÉMONSTRATION.

$$Id_G : G \rightarrow G$$

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

Si  $G \simeq H$ , soit  $\varphi : G \rightarrow H$  un isomorphisme ; d'après le Lemme 5.17,

$$\varphi^{-1} : H \rightarrow G$$

est un morphisme, et il est évidemment bijectif, d'où  $H \simeq G$ .

Enfin, supposons  $G \simeq H$  et  $H \simeq K$  ; il existe des isomorphismes  $\varphi : G \rightarrow H$  et  $\psi : H \rightarrow K$ . Vu que  $\psi \circ \varphi$  est un morphisme (Proposition 5.16(1)), et qu'il est bijectif car  $\varphi$  et  $\psi$  le sont, c'est un isomorphisme, d'où  $G \simeq K$ .  $\square$

LEMME 5.21. Soient  $G$  et  $H$  deux groupes, et  $\varphi : G \rightarrow H$  un morphisme de groupes ; alors

$$(1) \quad \varphi(e_G) = e_H,$$

(2)

$$(\forall x \in G) \quad \varphi(x^{-1}) = (\varphi(x))^{-1}$$

et

(3)

$$(\forall n \in \mathbf{Z})(\forall x \in G) \quad \varphi(x^n) = (\varphi(x))^n.$$

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 2.3.

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

(3)  $x$  étant fixé, établissons d'abord le résultat pour  $n \in \mathbf{N}$ , par récurrence. On a

$$\begin{aligned}\varphi(x^0) &= \varphi(e_G) \\ &= e_H \text{ (d'après (1))} \\ &= \varphi(x)^0 ,\end{aligned}$$

soit le résultat au rang 0.

Supposons le résultat établi au rang  $n$  ; alors

$$\begin{aligned}\varphi(x^{n+1}) &= \varphi(x^n x) \\ &= \varphi(x^n) \varphi(x) \\ &= \varphi(x)^n \varphi(x) \text{ (d'après l'hypothèse de récurrence)} \\ &= \varphi(x)^{n+1} ,\end{aligned}$$

soit l'hypothèse au rang  $n + 1$ . On a donc

$$(\forall n \in \mathbf{N})(\forall x \in G) \varphi(x^n) = (\varphi(x))^n .$$

Soit maintenant  $n \leq -1$  ; on a

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

DÉFINITION 5.22. Soit  $\varphi : G \rightarrow H$  un morphisme de groupes ; on appelle **noyau** de  $\varphi$ , et on note  $\ker(\varphi)$ , l'ensemble

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

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

$$\text{Im}(\varphi) := \{\varphi(x) \mid x \in G\}$$

PROPOSITION 5.23.

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

DÉMONSTRATION. (1)  $e_H = \varphi(e_G) \in \text{Im}(\varphi)$ , donc  $\text{Im}(\varphi) \neq \emptyset$ .

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

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

En vertu de la clause (3) de la Proposition 5.1, il apparaît que  $\text{Im}(\varphi)$  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  $\varphi$  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  $\varphi$ . 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  $x = y$  :  $\varphi$  est injectif.

□

REMARQUE 5.24. Si  $\varphi : G \rightarrow H$  est un morphisme de groupes et  $G_1$  est un sous-groupe de  $G$ , la restriction  $\varphi|_{G_1}$  de  $\varphi$  à  $G_1$  est un morphisme de  $G_1$  dans  $H$ .

En particulier  $\varphi(G_1) := \{\varphi(x) \mid x \in G_1\}$  est un sous-groupe de  $H$  ; en effet,  $\varphi(G_1) = \text{Im}(\varphi|_{G_1})$ .

PROPOSITION 5.25. Soient  $G$  un groupe et  $H$  un sous-groupe de  $G$  ; il existe un groupe  $K$  et un morphisme  $\varphi : K \rightarrow G$  tels que  $\text{Im}(\varphi) = H$ .

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

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

Du fait que

$$\forall (h_1, h_2) \in H^2 \quad \varphi(h_1 h_2) = h_1 h_2 = \varphi(h_1) \varphi(h_2),$$

il suit que  $\varphi$  est un morphisme de groupes. De plus

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

□

L'analogie de la Proposition 5.25 pour les noyaux et les sous-groupes distingués sera établi plus tard.

PROPOSITION 5.26. Soient  $G$  un groupe et  $H$  un sous-groupe de  $G$ . On pose

$$N_G(H) := \{x \in G \mid xHx^{-1} = H\}.$$

Alors  $N_G(H)$  est un sous-groupe de  $G$ , il contient  $H$ ,  $H$  est distingué dans  $N_G(H)$ , et  $N_G(H)$  est le plus grand sous-groupe de  $G$  ayant ces propriétés.

On l'appelle le **normalisateur** de  $H$  dans  $G$ .

DÉMONSTRATION. Je vous laisse voir que  $N_G(H)$  est un sous-groupe de  $G$ .

Soit  $h \in H$  ; alors

$$hHh^{-1} = hH = H$$

donc  $h \in N_G(H)$  ; on a donc bien  $h \in N_G(H)$ . Donc  $H \subset N_G(H)$ .

Si  $h \in H$  et  $k \in N_G(H)$ , alors

$$khk^{-1} \in kHk^{-1} = H ;$$

on a bien  $H \triangleleft N_G(H)$ .

Réciproquement, soit  $K$  un sous-groupe de  $G$  tel que  $H \triangleleft K$ , et soit  $k \in K$  ; alors, pour chaque  $h \in H$ ,  $khk^{-1} \in H$ , soit  $kHk^{-1} \subset H$ . Appliquant le même raisonnement à  $k^{-1}$ , on obtient que  $k^{-1}Hk \subset H$ , soit  $H \subset kHk^{-1}$ , d'où  $kHk^{-1} = H$  et  $k \in N_G(H)$ . Cela vaut pour chaque  $k \in K$ , donc  $K \subset N_G(H)$ .  $\square$

**6. Groupes quotients, théorèmes d'isomorphisme.**

Dans tout ce chapitre,  $G$  désignera un groupe. Nous supposons 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  $\mathcal{L}_N (= \mathcal{R}_N)$ , et  $\frac{G}{N}$  l'ensemble de ces classes :

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

LEMME 6.1. *Pour  $\alpha \in \frac{G}{N}$  et  $\beta \in \frac{G}{N}$ , 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  $\frac{G}{N}$  un groupe.*

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

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

la loi  $.$  est associative.



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

$$\begin{aligned}\alpha \cdot \bar{e}_G &= \bar{x} \cdot \bar{e}_G \\ &= \overline{x \cdot e_G} \\ &= \bar{x} \\ &= \alpha,\end{aligned}$$

et de même

$$\bar{e}_G \cdot \alpha = \alpha;$$

$e_{\frac{G}{N}} := \bar{e}_G$  est donc un élément neutre pour la loi .

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

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

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

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

REMARQUE 6.2. 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.

REMARQUE 6.3. On voit aisément, comme dans la démonstration de l'associativité, que  $\frac{G}{N}$  est abélien dès que  $G$  l'est.

EXEMPLE 6.4. (Exercice) Soit  $n \geq 1$  un entier ; le groupe  $\frac{\mathbf{Z}}{n\mathbf{Z}}$  est d'ordre  $n$ , et

$$\frac{\mathbf{Z}}{n\mathbf{Z}} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\} = \langle \bar{1} \rangle .$$

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

REMARQUE 6.5. Des instances particulières de ce groupe sont déjà apparues au §3 : pour  $n \in \{1, 2, 3\}$ , l'unique table de groupe d'ordre  $n$  possible doit être celle de  $(\frac{\mathbf{Z}}{n\mathbf{Z}}, +)$ , ce qu'il est d'ailleurs facile de vérifier.

Pour  $n = 4$ , la première table obtenue est celle de  $\frac{\mathbf{Z}}{4\mathbf{Z}}$  muni de l'addition, et la seconde est celle de  $\frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}}$  muni de l'addition composante par composante.

On l'appelle **Groupe de Klein**.

**COROLLAIRE 6.6.** *Soient  $G$  un groupe et  $N$  un sous-groupe distingué de  $G$  ; alors il existe un groupe  $K$  et un morphisme  $\psi : G \rightarrow K$  tels que  $N = \ker(\psi)$ .*

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

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

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

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

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

Pour  $g \in G$ , on a les équivalences

$$\begin{aligned} g \in \ker(p_{G,N}) &\iff p_{G,N}(g) = e_K \\ &\iff p_{G,N}(g) = e_{\frac{G}{N}} \\ &\iff \bar{g} = \bar{e}_G \\ &\iff e_G \mathcal{L}_N g \\ &\iff e_G^{-1} g \in N \\ &\iff e_G g \in N \\ &\iff g \in N, \end{aligned}$$

d'où bel et bien  $N = \ker(p_{G,N})$ . □

**REMARQUE 6.7.** Pour tout groupe  $G$  et tout sous-groupe  $N$  distingué de  $G$ , la projection canonique  $p_{G,N} : G \rightarrow \frac{G}{N}$  est surjective :

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

THÉORÈME 6.8. (**Premier Théorème d'Isomorphisme**) Soit  $\varphi : G \rightarrow H$  un morphisme de groupes ; alors

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

DÉMONSTRATION. Définissons

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

(1)  $\psi$  est bien définie.

Supposons  $\bar{x} = \bar{y}$  ; alors  $x\mathcal{L}_{\ker(\varphi)}y$ , 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)  $\psi$  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)  $\psi$  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  $x^{-1}y \in \ker(\varphi)$ ,  $x\mathcal{L}_{\ker(\varphi)}y$  et  $\bar{x} = \bar{y}$ , d'où  $a = \bar{x} = \bar{y} = b$ .

(4)  $\psi$  est surjectif.

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

$\psi$  est donc un isomorphisme, d'où le résultat. □

**COROLLAIRE 6.9. (Deuxième Théorème d'Isomorphisme)**  
Soient  $H$  un sous-groupe de  $G$  et  $K$  un sous-groupe distingué de  $G$  ; posons

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

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)

$e_G \in H$  et  $e_G \in K$ , 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  $HK$ .

Soient  $x \in HK$  et  $n \in K$  ; alors  $xnx^{-1} \in K$  (car  $x \in G$ ).

$K$  est donc 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  $h x h^{-1} \in H$  (car  $H$  est un sous-groupe de  $G$ ) et  $h x h^{-1} \in K$  (car  $K \triangleleft G$ ), d'où  $h x h^{-1} \in H \cap K$  :  $H \cap K$  est distingué dans  $H$ .
- (5) Soit  $p : G \rightarrow \frac{G}{K}$  la projection canonique, et soit  $\varphi = p|_H$  la restriction de  $p$  à  $H$  ;  $\varphi$  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  $\alpha \in \text{Im}(\varphi)$  ; alors  $\alpha = \varphi(h) = p(h) = \bar{h}$ , pour un  $h \in H$ . Mais  $h = h.e_G \in HK$ , d'où  $\alpha = \bar{h} \in \frac{HK}{K}$ . On a donc  $\text{Im}(\varphi) \subset \frac{HK}{K}$ .

Réciproquement, soit  $\alpha \in \frac{HK}{K}$  ; 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

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

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

Mais alors il suit du Théorème 6.8 que

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

□

Le résultat suivant permet de décrire les sous-groupes d'un groupe quotient.

**THÉORÈME 6.10. (Troisième Théorème d'Isomorphisme)** Soient  $G$  un groupe et  $N$  un sous-groupe distingué de  $G$ .

- (1) Les sous-groupes de  $\frac{G}{N}$  sont les  $\frac{H}{N}$ , pour  $H$  un sous-groupe de  $G$  tel que  $N \subset H$ .
- (2)  $\frac{H}{N}$  est distingué dans  $\frac{G}{N}$  si et seulement si  $H$  est distingué dans  $G$ .
- (3) Si les conditions équivalentes de (2) sont satisfaites, on a

$$\frac{\frac{G}{N}}{\frac{H}{N}} \simeq \frac{G}{H}.$$

DÉMONSTRATION. On notera  $p$  la projection canonique de  $G$  dans  $\frac{G}{N}$ .

(1)

Soit  $H$  un sous-groupe de  $G$  contenant  $N$  ; alors  $e_G \in H$ , donc  $\bar{e}_G \in \frac{H}{N}$  et

$$\frac{H}{N} \neq \emptyset.$$

Soit  $(\alpha, \beta) \in (\frac{H}{N})^2$  ; on peut écrire  $\alpha = \bar{h}$  et  $\beta = \bar{h}'$ , avec  $(h, h') \in H^2$ . Mais alors  $h(h')^{-1} \in H$ , d'où

$$\alpha\beta^{-1} = (\bar{h})(\bar{h}')^{-1} = \overline{h(h')^{-1}} \in \frac{H}{N} ;$$

$\frac{H}{N}$  est un sous-groupe de  $\frac{G}{N}$ .

Réciproquement, soit  $T$  un sous-groupe de  $\frac{G}{N}$ , et posons

$$H = p^{-1}(T) := \{g \in G \mid p(g) \in T\} = \{g \in G \mid \bar{g} \in T\}.$$

$H$  est un sous-groupe de  $G$  (exercice : on peut soit procéder directement, soit invoquer des propriétés de l'image réciproque). Soit  $n \in N$  ; on a

$$p(n) = \bar{n} = \bar{e}_G = e_{\frac{G}{N}} \in T$$

(car  $T$  est un sous-groupe de  $\frac{G}{N}$ ), donc  $n \in H$  :  $N \subset H$ .

Soit maintenant  $\alpha \in \frac{H}{N}$  ; alors  $\alpha = \bar{h}$  pour un  $h \in H$ . Mais alors  $\bar{h} = p(h) \in T$ , c'est-à-dire que  $\alpha \in T$ . Nous avons établi l'inclusion

$$\frac{H}{N} \subset T.$$

Pour établir l'inclusion opposée, soit  $t \in T$  ; il existe  $g \in G$  tel que  $t = \bar{g}$ . On a donc  $\bar{g} \in T$ , d'où  $g \in H$  et

$$t = \bar{g} \in \frac{H}{N}.$$

Nous avons bien établi que  $T \subset \frac{H}{N}$ , d'où  $T = \frac{H}{N}$  et le résultat.

(2)

Supposons  $H \triangleleft G$ , et soient  $\alpha \in \frac{G}{N}$  et  $\beta \in \frac{H}{N}$  ; alors  $\alpha = \bar{g}$  ( $g \in G$ ) et

$$\beta = \bar{h} \quad (h \in H).$$

Il en résulte que  $ghg^{-1} \in H$  (car  $H \triangleleft G$ ), d'où  $\alpha\beta\alpha^{-1} = \overline{ghg^{-1}} \in \frac{H}{N}$ .  
On a donc bien  $\frac{H}{N} \triangleleft \frac{G}{N}$ .

Réciproquement, supposons  $\frac{H}{N} \triangleleft \frac{G}{N}$ , et soient  $g \in G$  et  $h \in H$  ; alors  $\bar{g} \in \frac{G}{N}$  et  $\bar{h} \in \frac{H}{N}$ , d'où  $\overline{ghg^{-1}} = \bar{g}\bar{h}(\bar{g})^{-1} \in \frac{H}{N}$  ; il existe donc  $h' \in H$  tel que

$$\overline{ghg^{-1}} = \bar{h}'.$$

Mais alors  $ghg^{-1}\mathcal{L}_N h'$ , soit  $(h')^{-1}ghg^{-1} \in N$ . Or  $N \subset H$ , donc  $(h')^{-1}ghg^{-1} \in H$  et  $ghg^{-1} = h'((h')^{-1}ghg^{-1}) \in H$ . On a bien établi que  $H \triangleleft G$ , d'où l'équivalence voulue.

(3) Dans ce paragraphe,  $\bar{g}$  désignera la classe de  $g \in G$  modulo  $H$  et  $\tilde{g}$  sa classe modulo  $N$ .

Supposons donc  $H \triangleleft G$ . Définissons

$$\theta : \frac{G}{N} \rightarrow \frac{G}{H} \\ \tilde{g} \mapsto \bar{g}.$$

Si l'on a  $\tilde{g} = \tilde{g}'$ , alors  $g^{-1}g' \in N$  donc  $g^{-1}g' \in H$  et  $\bar{g} = \bar{g}'$  :  $\theta$  est bien définie. Il est facile de voir (exercice !) qu'il s'agit d'un morphisme de groupes. Son image est

$$\text{Im}(\theta) = \{\theta(\alpha) | \alpha \in \frac{G}{N}\} = \{\theta(\tilde{g}) | g \in G\} = \{\bar{g} | g \in G\} = \frac{G}{H};$$

$\theta$  est donc surjectif.

Soit  $g \in G$  ;  $\tilde{g}$  appartient au noyau  $\ker(\theta)$  si et seulement si  $\theta(\tilde{g}) = e_{\frac{G}{H}}$ , soit  $\bar{g} = \bar{e}_G$ , ou  $g \in H$ . On a donc

$$\ker(\theta) = \{\tilde{g} | g \in H\} = \frac{H}{N}.$$

Il suffit maintenant d'appliquer le Premier Théorème d'Isomorphisme (Théorème 6.8) pour obtenir que

$$\frac{\frac{G}{N}}{\frac{H}{N}} = \frac{\frac{G}{N}}{\ker(\theta)} \simeq \text{Im}(\theta) = \frac{G}{H}.$$

□

EXEMPLE 6.11. Cet exemple sera traité plus en détail en Travaux Dirigés.

Soient  $G = \mathbf{Z}$  et  $N = n\mathbf{Z}$  ( $n \geq 1$  entier). Alors  $N$  est un sous-groupe de  $G$ , distingué car  $G$  est abélien ; on a vu que  $\frac{G}{N} = \frac{\mathbf{Z}}{n\mathbf{Z}}$  est fini, de cardinal  $n$ .

D'après le Théorème 6.10(1), les sous-groupes de  $\frac{\mathbf{Z}}{n\mathbf{Z}}$  sont les  $\frac{H}{n\mathbf{Z}}$ , pour  $H$  un sous-groupe de  $\mathbf{Z}$  contenant  $n\mathbf{Z}$ . Mais un tel  $H$  est de la forme  $m\mathbf{Z}$  pour un  $m \in \mathbf{N}$  (Exemple 5.2), et  $N \subset H$  équivaut à  $n\mathbf{Z} \subset m\mathbf{Z}$ , soit à  $n \in m\mathbf{Z}$ , soit à ce que  $m$  divise  $n$ . Les sous-groupes de  $\frac{\mathbf{Z}}{n\mathbf{Z}}$  sont donc les  $\frac{m\mathbf{Z}}{n\mathbf{Z}}$  pour  $m$  diviseur de  $n$  ; leur nombre est donc  $d(n)$ , le nombre de diviseurs de  $n$ .

On peut voir aisément que

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

est isomorphe à

$$\frac{\mathbf{Z}}{\frac{n}{m}\mathbf{Z}};$$

en particulier, il est de cardinal  $\frac{n}{m}$ .

Pour chaque diviseur  $d$  de  $n$ ,  $\frac{\mathbf{Z}}{n\mathbf{Z}}$  possède donc un unique sous-groupe d'ordre  $d$  :

$$\frac{\frac{n}{d}\mathbf{Z}}{n\mathbf{Z}},$$

et ce sous-groupe est isomorphe à  $\frac{\mathbf{Z}}{d\mathbf{Z}}$ .

Nous retrouverons ces résultats lors du chapitre consacré aux groupes monogènes.



### 7. 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

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

LEMME 7.1.  $\varphi_x$  est un morphisme de groupes.

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

$$\begin{aligned}\varphi_x(m+n) &= x^{m+n} \\ &= x^m x^n \\ &\quad (\text{d'après le Théorème 2.9}) \\ &= \varphi_x(m)\varphi_x(n).\end{aligned}$$

□

Il est clair que l'image  $\text{Im}(\varphi_x)$  de  $\varphi_x$  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

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

$\text{Im}(\varphi_x)$  est donc le plus petit sous-groupe de  $G$  contenant  $x$  :  $\text{Im}(\varphi_x) = \langle x \rangle$ , le sous-groupe de  $G$  engendré par  $x$ .

Du fait que  $\mathbf{Z}$  est abélien,  $\langle x \rangle = \text{Im}(\varphi_x)$  l'est.

PROPOSITION 7.2. On a un, et un seul, des cas suivants.

- (1) Les  $(x^n)_{n \in \mathbf{Z}}$  sont deux à deux distincts.  
Alors  $\langle x \rangle = \text{Im}(\varphi_x) \simeq \mathbf{Z}$  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

$$\langle x \rangle = \{e_G, x, \dots, x^{\omega(x)-1}\}$$

et

$$|\langle x \rangle| = \omega(x).$$

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

DÉMONSTRATION.  $\varphi_x$  étant un morphisme de groupes,  $\ker(\varphi_x)$  est un sous-groupe de  $\mathbf{Z}$ , donc (Exemple 5.2) 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 le morphisme

$$\varphi_x : \mathbf{Z} \rightarrow \text{Im}(\varphi_x) = \langle x \rangle$$

est injectif donc bijectif d'où

$$\langle x \rangle \simeq \mathbf{Z}$$

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

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

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

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

soit

$$\langle x \rangle = \{e_G, x, \dots, x^{\omega(x)-1}\};$$

en particulier,

$$|\langle x \rangle| = \omega(x).$$

□

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

$\omega(x)$  est appelé **l'ordre** de  $x$ . Vu que, pour chaque  $k \in \mathbf{Z}$ ,  $(x^{-1})^k = (x^k)^{-1}$ ,  $(x^{-1})^k = e_G$  équivaut à  $x^k = e_G$ . Il en résulte que  $\omega(x^{-1}) = \omega(x)$ .

**PROPOSITION 7.3.** *Si  $\psi : G \rightarrow H$  est un morphisme de groupes et  $x \in G$  est d'ordre fini, alors  $\psi(x) \in H$  est d'ordre fini et  $\omega(\psi(x))$  divise  $\omega(x)$ . Si en outre  $\psi$  est injectif (en particulier si  $\psi$  est un isomorphisme), alors  $\omega(\psi(x)) = \omega(x)$ .*

DÉMONSTRATION. On a

$$(\psi(x))^{\omega(x)} = \psi(x^{\omega(x)}) = \psi(e_G) = e_H,$$

donc  $\psi(x)$  est d'ordre fini, et cet ordre divise  $\omega(x)$ .

Si  $\psi$  est injectif, on a

$$e_H = \psi(x)^{\omega(\psi(x))} = \psi(x^{\omega(\psi(x))}),$$

donc, au vu de l'injectivité de  $\psi$ ,  $x^{\omega(\psi(x))} = e_G$  et  $\omega(x)$  divise  $\omega(\psi(x)) : \omega(\psi(x)) = \omega(x)$ .

DÉFINITION 7.4. Le groupe  $G$  est dit **monogène** s'il existe un élément  $x$  de  $G$  tel que  $G = \langle x \rangle$ .

COROLLAIRE 7.5. 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. Si l'on se trouve dans le cas (1) de la Proposition 7.2,  $G = \langle x \rangle \simeq \mathbf{Z}$  et on a le résultat.

Dans l'autre cas,  $\omega(x)$  est fini :  $\omega(x) = n$ . D'après la démonstration de la Proposition 7.2,  $\ker(\varphi_x) = \omega(x)\mathbf{Z} = n\mathbf{Z}$ .

Mais alors

$$\frac{\mathbf{Z}}{n\mathbf{Z}} = \frac{\mathbf{Z}}{\ker(\varphi_x)} \simeq \text{Im}(\varphi_x) = \langle x \rangle = G.$$

On peut également procéder directement : soit

$$\psi : \frac{\mathbf{Z}}{n\mathbf{Z}} \rightarrow G \\ \bar{m} \mapsto x^m.$$

Il est facile de vérifier que  $\psi$  est bien défini, et qu'il s'agit d'un isomorphisme.  $\square$

PROPOSITION 7.6. 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  $\omega(x)\omega(y)$ .

PROOF.

$$\begin{aligned}
 (xy)^{\omega(x)\omega(y)} &= x^{\omega(x)\omega(y)}y^{\omega(x)\omega(y)} \\
 &\quad \text{(d'après le Corollaire 2.12)} \\
 &= x^{\omega(x)\omega(y)}y^{\omega(y)\omega(x)} \\
 &= (x^{\omega(x)})^{\omega(y)}(y^{\omega(y)})^{\omega(x)} \\
 &= (e_G)^{\omega(y)}(e_G)^{\omega(x)} \\
 &= e_G \cdot e_G \\
 &= e_G.
 \end{aligned}$$

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

REMARQUE 7.7. Ce résultat ne subsiste pas en général. Par exemple, dans le groupe symétrique  $\Sigma_3$  de degré 3 (cf. chapitre 11), soient  $x = (12)$  et  $y = (23)$  ; alors  $\omega(x) = \omega(y) = 2$  et  $xy = (123)$ , d'où  $\omega(xy) = 3$ , lequel ne divise pas  $\omega(x)\omega(y) = 2 \cdot 2 = 4$ .

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

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

et

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

Alors

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

et

$$(\forall n \in \mathbf{N}) \quad (AB)^n = \begin{bmatrix} \cos(n\alpha) & \sin(n\alpha) \\ -\sin(n\alpha) & \cos(n\alpha) \end{bmatrix}$$

d'où (exercice !)  $\omega(A) = \omega(B) = 2$  et  $\omega(AB) = \infty$ .

PROPOSITION 7.8. Soient  $G$  un groupe, et  $x$  et  $y$  deux éléments de  $G$  d'ordres finis tels que  $xy = yx$  et que les ordres  $\omega(x)$  et  $\omega(y)$  soient premiers entre eux. Alors  $xy$  est d'ordre fini, et on a  $\omega(xy) = \omega(x)\omega(y)$ .

DÉMONSTRATION. D'après la Proposition 7.6,  $\omega(xy)$  divise  $\omega(x)\omega(y)$ . Mais alors  $x^{-1}$  et  $xy$  sont d'ordre fini et commutent, donc

$\omega(y) = \omega(x^{-1}(xy))$  divise  $\omega(x^{-1})\omega(xy) = \omega(x)\omega(xy)$ .  $\omega(x)$  et  $\omega(y)$  étant premiers entre eux, il s'ensuit que  $\omega(y)$  divise  $\omega(xy)$ .

De même  $\omega(x)$  divise  $\omega(yx) = \omega(xy)$ . L'ordre  $\omega(xy)$  est donc divisible par  $\omega(x)$  et  $\omega(y)$ , donc par leur ppcm, lequel vaut  $\omega(x)\omega(y)$  (encore une fois, car  $\omega(x)$  et  $\omega(y)$  sont premiers entre eux). Chacun des entiers  $\omega(xy)$  et  $\omega(x)\omega(y)$  divise donc l'autre : ils sont égaux.  $\square$

Cette proposition admet une réciproque partielle

**THÉORÈME 7.9.** *Soit  $x \in G$  tel que  $\omega(x) = ab$  avec  $a \geq 1$  et  $b \geq 1$  premiers entre eux ; alors il existe un unique couple  $(y, z) \in G^2$  tel que  $\omega(y) = a$ ,  $\omega(z) = b$  et  $yz = zy = x$ . De plus  $y$  et  $z$  sont des puissances de  $x$ .*

**DÉMONSTRATION.** D'après le Théorème de Bachet–Bezout, il existe  $(\lambda, \mu) \in \mathbf{Z}^2$  tel que  $\lambda a + \mu b = 1$ . Posons

$$y = x^{\mu b}$$

et

$$z = x^{\lambda a};$$

alors

$$yz = x^{\mu b} x^{\lambda a} = x^{\mu b + \lambda a} = x^1 = x$$

et de même

$$zy = x.$$

On a

$$y^a = (x^{\mu b})^a = x^{\mu b a} = x^{ab \mu} = (x^{ab})^\mu = (x^{\omega(x)})^\mu = e_G^\mu = e_G,$$

donc l'ordre  $\omega(y)$  divise  $a$  ; de même  $\omega(z)$  divise  $b$ . En particulier  $\omega(y)$  et  $\omega(z)$  sont premiers entre eux ; du fait que  $yz = zy$  on a , d'après la Proposition 7.8

$$\omega(yz) = \omega(y)\omega(z)$$

d'où

$$ab = \omega(x) = \omega(yz) = \omega(y)\omega(z)$$

Vu que  $\omega(y)$  divise  $a$  et  $\omega(z)$  divise  $b$ , on a nécessairement  $\omega(y) = a$  et  $\omega(z) = b$  (ce que l'on peut aussi voir directement). L'existence de  $y$  et de  $z$  s'ensuit.

Concernant l'unicité, supposons  $\omega(y) = a$ ,  $\omega(z) = b$  et  $yz = zy = x$ . Alors

$$\begin{aligned}
 x^{\mu b} &= (yz)^{\mu b} \\
 &= y^{\mu b} z^{\mu b} \\
 &\quad (\text{car } y \text{ et } z \text{ commutent}) \\
 &= y^{1-\lambda a} z^{\mu b} \\
 &= y(y^a)^{-\lambda} (z^b)^\mu \\
 &= y(y^{\omega(y)})^{-\lambda} (z^{\omega(z)})^\mu \\
 &= y(e_G)^{-\lambda} (e_G)^\mu \\
 &= y
 \end{aligned}$$

d'où

$$y = x^{\mu b}.$$

Mais alors

$$z = y^{-1}x = x^{-\mu b}x = x^{1-\mu b} = x^{\lambda a}$$

et nous avons établi l'unicité du couple  $(y, z)$ . Au passage, nous avons démontré que  $y$  et  $z$  sont des puissances de  $x$ .  $\square$

**COROLLAIRE 7.10.** *Soit  $x \in G$  d'ordre  $n$  fini, et décomposons  $n$  en facteurs premiers sous la forme*

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$$

avec les  $p_i$  premiers et deux à deux distincts, et les  $\alpha_i \geq 1$ . Alors il existe un unique  $r$ -uplet  $(x_1, \dots, x_r) \in G^r$  tel que les  $x_i$  commutent deux à deux :

$$\forall (i, j) \in \{1, \dots, r\}^2 \quad x_i x_j = x_j x_i,$$

et que

$$(\forall i \in \{1, \dots, r\}) \quad \omega(x_i) = p_i^{\alpha_i}.$$

En outre les  $x_i$  sont des puissances de  $x$ .

On appelle  $x_i$  la  $p_i$ -**partie** de  $x$ .

**DÉMONSTRATION.** Soient  $a = p_1^{\alpha_1}$  et  $b = p_2^{\alpha_2} \dots p_r^{\alpha_r}$  ; d'après le Théorème 7.9, il existe  $(y, z) \in G^2$  tel que  $x = yz = zy$  et

$\omega(y) = a = p_1^{\alpha_1}$ ,  $\omega(z) = b = p_2^{\alpha_2} \dots p_r^{\alpha_r}$ , et  $y$  et  $z$  sont des puissances de  $x$ . Une récurrence facile sur  $r$ , que je vous laisse écrire, permet de conclure à l'existence des  $x_i$ .

L'unicité sera laissée en exercice.  $\square$

### 8. Théorème de Lagrange.

Dans tout ce chapitre,  $G$  désignera un groupe et  $H$  un sous-groupe de  $G$ . On notera

$$H \backslash G := \{Hx \mid x \in G\}$$

l'ensemble des  $\mathcal{R}_H$ -classes d'équivalence dans  $G$ , et

$$G/H := \{xH \mid x \in G\}$$

l'ensemble des  $\mathcal{L}_H$ -classes d'équivalence dans  $G$ .

THÉORÈME 8.1.  $H \backslash G$  et  $G/H$  ont même cardinal.

On appelle ce nombre **l'indice de  $H$  dans  $G$** , et on le note  $[G : H]$ . Clairement,  $[G : G] = 1$ .

DÉMONSTRATION. Soit

$$\begin{aligned} \varphi & : H \backslash G \rightarrow G/H \\ Hx & \mapsto x^{-1}H. \end{aligned}$$

$Hx = Hy$  entraîne  $xy^{-1} \in H$ , soit  $(x^{-1})^{-1}y^{-1} \in H$  et  $x^{-1}H = y^{-1}H$  :  $\varphi$  est bien définie.

De même on voit que

$$\begin{aligned} \psi & : G/H \rightarrow H \backslash G \\ xH & \mapsto Hx^{-1} \end{aligned}$$

et, pour chaque  $x \in G$ ,

$$(\psi \circ \varphi)(Hx) = \psi(\varphi(Hx)) = \psi(x^{-1}H) = H(x^{-1})^{-1} = Hx,$$

d'où  $\psi \circ \varphi = Id_{H \backslash G}$ . De même  $\varphi \circ \psi = Id_{G/H}$ , donc  $\varphi$  est bijective et le résultat.

On peut aussi écrire que

$$\begin{aligned} x^{-1}H & = \{x^{-1}h \mid h \in H\} \\ & = \{x^{-1}(h')^{-1} \mid h' \in H\} \\ & = \{(h'x)^{-1} \mid h' \in H\} \\ & = (Hx)^{-1} \end{aligned}$$

(avec une notation évidente), et de même

$$Hx^{-1} = (xH)^{-1},$$

à partir de quoi l'on conclut aisément. □

PROPOSITION 8.2. *Si  $H$  est un sous-groupe d'indice 2 de  $G$ , alors  $H$  est distingué dans  $G$ .*

DÉMONSTRATION. Pour  $x \in G$ , soit  $\bar{x}$  sa classe modulo  $\mathcal{L}_H$  ; alors  $x \in \bar{e}_G$  si et seulement si  $e_G^{-1}x \in H$ , soit  $x \in H$  ; la classe  $\bar{e}_G$  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  $G \setminus H$  ; les  $\mathcal{L}_H$ -classes d'équivalence sont donc  $H$  et  $G \setminus H$ .

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 5.14, on a bien

$$H \triangleleft G.$$

□

Dorénavant nous supposerons  $G$  **fini**.

THÉORÈME 8.3. (**Théorème de Lagrange**) *Soient  $G$  un groupe fini et  $H$  un sous-groupe de  $G$  ; alors l'ordre  $|H|$  de  $H$  divise l'ordre  $|G|$  de  $G$ .*

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

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

L'application

$$\begin{aligned} \alpha &: H \rightarrow \bar{x} \\ &h \mapsto xh \end{aligned}$$

est donc surjective ; en vertu du Lemme 2.3, elle est injective, donc bijective. Il en résulte que

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

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



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

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

En particulier,  $|H|$  divise  $|G|$ .

Au passage nous avons établi que

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

□

REMARQUE 8.4. Nous aurions pu raisonner tout le long avec la relation  $\mathcal{R}_H$  et le même résultat serait apparu.

On peut se demander si, réciproquement, chaque diviseur  $d$  de l'ordre  $|G|$  de  $G$  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 8.5. *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.  $\langle x \rangle$  est un sous-groupe de  $G$  ; en lui appliquant le Théorème 8.3, on obtient que  $|\langle x \rangle|$  divise  $|G|$ , c'est-à-dire que  $\omega(x)$  divise  $|G|$ . La dernière clause s'ensuit au moyen de la Proposition 7.2(2). □

COROLLAIRE 8.6. *Si l'ordre de  $G$  est un nombre premier  $p$ , alors  $G$  est isomorphe à  $\frac{\mathbf{Z}}{p\mathbf{Z}}$  ; 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  $|\langle x \rangle| = p = |G|$ . Il en résulte que  $G = \langle x \rangle$  ;  $G$  est donc isomorphe à  $\frac{\mathbf{Z}}{p\mathbf{Z}}$  en vertu du Corollaire 7.5. □

Dans le cas fini, Frobenius a généralisé la Proposition 8.2 : si  $G$  est fini et  $H$  est un sous-groupe de  $G$  tel que l'indice  $[G : H]$  soit égal au plus petit diviseur premier  $p$  de l'ordre  $|G|$  de  $G$ , alors  $H$  est distingué dans  $G$ . Nous établirons ce résultat par la suite (Corollaire 11.7).

### 9. Produits directs.

Soient  $(A, *)$  et  $(B, *')$  deux groupes. Sur le produit direct  $A \times B$ , définissons une opération  $''$  par

$$\forall (a_1, a_2, b_1, b_2) \in A \times A \times B \times B \quad (a_1, b_1) '' (a_2, b_2) = (a_1 * a_2, b_1 *' b_2)$$

Il est facile de vérifier que cette opération fait de  $A \times B$  un groupe, d'élément neutre

$$e_{A \times B} = (e_A, e_B).$$

Dorénavant, nous noterons les opérations de chacun des groupes considérés par la juxtaposition. On vérifie sans problème que, si  $G$ ,  $H$  et  $K$  sont des groupes, on a un isomorphisme

$$(G \times H) \times K \simeq G \times (H \times K)$$

donné par

$$((g, h), k) \mapsto (g, (h, k)).$$

La notation

$$G_1 \times \dots \times G_n$$

est donc sans ambiguïté.

#### THÉORÈME 9.1. (*Produit direct externe*)

Soient  $A$  et  $B$  deux groupes ; posons  $G = A \times B$ ,

$$H := \{(a, e_B) \mid a \in A\}$$

et

$$K := \{(e_A, b) \mid b \in B\}.$$

Alors  $H$  et  $K$  sont des sous-groupes distingués de  $G$ ,  $G = HK$ ,  $H \cap K = \{e_G\}$  et

$$\forall (h, k) \in H \times K \quad hk = kh.$$

DÉMONSTRATION.  $H \neq \emptyset$  car  $e_{A \times B} = (e_A, e_B) \in H$ .

Soit  $(x, y) \in H^2$  ; alors  $x = (a, e_B)$  ( $a \in A$ ) et  $y = (c, e_B)$  ( $c \in A$ ).

Il s'ensuit que

$$\begin{aligned} xy^{-1} &= (a, e_B)(c, e_B)^{-1} \\ &= (a, e_B)(c^{-1}, e_B) \\ &= (ac^{-1}, e_B) \in H, \end{aligned}$$

donc  $H$  est un sous-groupe de  $G$ .

Soient  $g \in G$  et  $h \in H$  ; alors  $g = (a, b)$  ( $a \in A, b \in B$ ) et

$$h = (c, e_B) \quad (c \in A).$$

Mais alors

$$ghg^{-1} = (a, b)(c, e_B)(a^{-1}, b^{-1}) = (aca^{-1}, be_Bb^{-1}) = (aca^{-1}, e_B) \in H$$

(car  $aca^{-1} \in A$ ) :

$H$  est distingué dans  $G$ .

On voit de même que  $K$  est un sous-groupe distingué de  $G$ .

Soit alors  $(h, k) \in H \times K$  ; alors  $h = (a, e_B)$  pour un  $a \in A$  et  $k = (e_A, b)$  pour un  $b \in B$ , d'où

$$hk = (a, e_B)(e_A, b) = (ae_A, e_Bb) = (a, b) = (e_Aa, be_B) = (e_A, b)(a, e_B) = kh,$$

et le dernier point.

Au passage, nous avons montré que chaque élément  $(a, b)$  de  $G$  appartient à  $HK$ , d'où  $G \subset HK$  et  $G = HK$ .

Il est visible que

$$H \cap K = \{(e_A, e_B)\} = \{e_{A \times B}\} = \{e_G\}.$$

□

Ce Théorème admet une réciproque.

**THÉORÈME 9.2. (*produit direct interne*)** Soit  $G$  un groupe, et soient  $H$  et  $K$  deux sous-groupes distingués de  $G$  tels que  $H \cap K = \{e_G\}$  et  $G = HK$ . Alors  $G \simeq H \times K$ .

**DÉMONSTRATION.** Nous allons d'abord établir que chaque élément de  $H$  commute avec chaque élément de  $K$ . Soit donc  $(h, k) \in H \times K$  ; vu que  $K \triangleleft G$ , on a  $hkh^{-1} \in K$  d'où  $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$

On voit de même, du fait que  $H \triangleleft G$ , que

$$hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$$

et

$$hkh^{-1}k^{-1} \in H \cap K = \{e_G\},$$

d'où

$$hkh^{-1}k^{-1} = e_G :$$

$$hk = kh.$$

Définissons alors

$$\begin{aligned} \varphi & : H \times K \rightarrow G \\ & (h, k) \mapsto hk. \end{aligned}$$

Soient  $x = (h, k) \in H \times K$  et  $y = (h', k') \in H \times K$  ; alors

$$\begin{aligned}
\varphi(xy) &= \varphi(hh', kk') \\
&= (hh')(kk') \\
&= hh'kk' \\
&= hkh'k' \\
&\quad (\text{car } h' \text{ et } k \text{ commutent}) \\
&= \varphi(x)\varphi(y);
\end{aligned}$$

$\varphi$  est donc un morphisme de groupes.

On a

$$\begin{aligned}
\text{Im}(\varphi) &= \{\varphi(h, k) \mid h \in H, k \in K\} \\
&= \{hk \mid h \in H, k \in K\} \\
&= HK \\
&= G,
\end{aligned}$$

c'est-à-dire que  $\varphi$  est surjectif.

Soit  $x \in \ker(\varphi)$  ; alors  $x = (h, k)$  ( $h \in H, k \in K$ ). Il s'ensuit que

$$hk = \varphi(h, k) = \varphi(x) = e_G,$$

d'où

$$h = k^{-1} \in H \cap K = \{e_G\}.$$

On a donc  $h = e_G = e_H, k = e_G = e_K$ , d'où

$$x = (h, k) = (e_H, e_K) = e_{H \times K}.$$

On a donc

$$\ker(\varphi) = \{e_{H \times K}\},$$

et  $\varphi$  est injectif.

$\varphi$  est donc bijectif, donc un isomorphisme, d'où

$$G \simeq H \times K.$$

□

### 10. Groupes diédraux.

Nous qualifierons le groupe  $G$  de *diédral* s'il est engendré par deux éléments d'ordre 2 : il existe  $t \in G$  et  $u \in G$  tels que  $\omega(t) = \omega(u) = 2$  et  $G = \langle t, u \rangle$ .

Du fait que  $t$  et  $u$  sont d'ordre 2, on a

$$(tu)^{-1} = u^{-1}t^{-1} = ut.$$

Posons alors  $x = tu$  ; il apparaît que

$$\begin{aligned} t^{-1}xt &= t^{-1}(tu)t \\ &= ut \\ &= (tu)^{-1} \\ &= x^{-1}. \end{aligned}$$

On a

$$t \in \langle t, x \rangle$$

et

$$u = t^{-1}(tu) = t^{-1}x \in \langle t, x \rangle,$$

d'où

$$G = \langle t, u \rangle \subset \langle t, x \rangle$$

et

$$G = \langle t, x \rangle$$

avec  $t^2 = e$  et  $t^{-1}xt = x^{-1}$ .

Soit

$$\begin{aligned} H &:= \langle x \rangle \cup t \langle x \rangle \\ &= \langle x \rangle \cup \{ty \mid y \in \langle x \rangle\}. \end{aligned}$$

Il est visible que  $x \in H$  et  $t = te \in H$ ; nous allons établir que  $H$  est un sous-groupe de  $G$ . On a  $x \in H$  donc  $H \neq \emptyset$ . Soit  $(h, h') \in H^2$  ; quatre cas peuvent se présenter

$$(1) \ h \in \langle x \rangle \text{ et } h' \in \langle x \rangle$$

Alors

$$h = x^m (m \in \mathbf{Z})$$

et

$$h' = x^k (k \in \mathbf{Z}),$$

d'où

$$h(h')^{-1} = x^{m-k} \in \langle x \rangle \subset H$$

et

$$h(h')^{-1} \in H.$$

(2)  $h \in \langle x \rangle$  **et**  $h' \in t \langle x \rangle$

Alors

$$h = x^m (m \in \mathbf{Z})$$

et

$$h' = tx^k (k \in \mathbf{Z}),$$

d'où

$$\begin{aligned} h(h')^{-1} &= x^m x^{-k} t^{-1} \\ &= x^{m-k} t \\ &= t(t^{-1} x^{m-k} t) \\ &= t(t^{-1} x t)^{m-k} \\ &= t(x^{-1})^{m-k} \\ &= tx^{k-m} \\ &\in t \langle x \rangle \\ &\subset H \end{aligned}$$

et

$$h(h')^{-1} \in H.$$

(3)  $h \in t \langle x \rangle$  **et**  $h' \in \langle x \rangle$

Alors

$$h = tx^m (m \in \mathbf{Z})$$

et

$$h' = x^k (k \in \mathbf{Z}),$$

d'où

$$h(h')^{-1} = tx^{m-k} \in t \langle x \rangle \subset H$$

et

$$h(h')^{-1} \in H.$$

(4)  $h \in t \langle x \rangle$  **et**  $h' \in t \langle x \rangle$

Alors

$$h = tx^m (m \in \mathbf{Z})$$

et

$$h' = tx^k (k \in \mathbf{Z}),$$

d'où

$$\begin{aligned}
 h(h')^{-1} &= tx^m x^{-k} t^{-1} \\
 &= tx^{m-k} t^{-1} \\
 &= t^{-1} x^{m-k} t \\
 &= (t^{-1} x t)^{m-k} \\
 &= (x^{-1})^{m-k} \\
 &= x^{k-m} \\
 &\in \langle x \rangle \\
 &\subset H
 \end{aligned}$$

et

$$h(h')^{-1} \in H.$$

On a donc, dans tous les cas,

$$h(h')^{-1} \in H;$$

$H$  est donc un sous-groupe de  $G$ . Vu que  $t \in H$  et  $x \in H$ ,  
 $G = \langle t, x \rangle \subset H$ , donc

$$G = H = \langle x \rangle \cup t \langle x \rangle.$$

Or la réunion  $\langle x \rangle \cup t \langle x \rangle$  est disjointe : supposons en effet

$$y \in \langle x \rangle \cap t \langle x \rangle;$$

alors  $y = x^m (m \in \mathbf{Z})$  et  $y = tx^k (k \in \mathbf{Z})$ , d'où  $tx^k = x^m$  et  $t = x^{m-k} = x^r (r \in \mathbf{Z})$ . En particulier  $t$  et  $x$  commutent, donc  $t^{-1}xt = x$  et  $x^{-1} = x : x^2 = e$ . Mais alors  $t = x^r \in \{e, x\}$ .  $t = e$  est impossible vu que  $\omega(t) = 2$ , et  $t = x$  entraînerait  $t = tu$  soit  $u = e$ , ce qui est absurde vu que  $\omega(u) = 2$ .

On a donc

$$G = \langle x \rangle \dot{\cup} t \langle x \rangle.$$

Si  $x$  est d'ordre infini,  $G$  est infini : on note

$$G \simeq D_\infty.$$

Il est facile (exercice !) de voir que le groupe  $\langle A, B \rangle$  de la Remarque 7.7 est isomorphe à  $D_\infty$ .

Si  $x$  est d'ordre fini  $\omega(x) = n$ , on a

$$\begin{aligned} |G| &= | \langle x \rangle \dot{\cup} t \langle x \rangle | \\ &= | \langle x \rangle | + | t \langle x \rangle | \\ &= 2 | \langle x \rangle | \\ &= 2\omega(x) \\ &= 2n; \end{aligned}$$

on note alors  $G \simeq D_{2n}$ .

REMARQUE 10.1. Certains auteurs notent ce groupe  $D_n$ .

On peut facilement voir que  $D_2$  est isomorphe à  $\frac{\mathbf{Z}}{2\mathbf{Z}}$ ,  $D_4$  à  $\frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}}$  (le **Groupe de Klein**; cf. §2 et §5), et  $D_6$  au groupe symétrique  $\Sigma_3$  de degré 3.

On peut réaliser géométriquement le groupe  $D_{2n}$  : dans un plan affine euclidien orienté  $\mathcal{P}$ , soit  $(A_1 \dots A_n)$  un  $n$ -gone régulier, soit  $O$  le centre de son cercle circonscrit (c'est aussi l'isobarycentre de  $(A_1 \dots A_n)$ ), soit  $r$  la rotation d'angle  $\frac{2\pi}{n}$  autour de  $O$ , et soit  $s$  la symétrie orthogonale autour de la droite  $(A_1 A_{\frac{n}{2}+1})$  pour  $n$  pair et de la droite  $(A_1 B)$  ( $B =$  milieu de  $[A_{\frac{n+1}{2}} A_{\frac{n+3}{2}}]$ ) pour  $n$  impair. Alors le groupe  $G$  des isométries (nécessairement affines) du plan qui préservent l'ensemble  $\{A_1, \dots, A_n\}$  des sommets du polygone est engendré par  $r$  et  $s$ . Le produit  $sr$  est une symétrie, donc  $(sr)^2 = Id_{\mathcal{P}}$  soit  $srs = r^{-1}$ . On a donc

$$G = \langle r, s \rangle$$

avec  $r^n = Id_{\mathcal{P}}$ ,  $s^2 = Id_{\mathcal{P}}$  et  $s^{-1}rs = r^{-1}$  :

$$G \simeq D_{2n}.$$

THÉORÈME 10.2. *Si  $m$  est impair, alors*

$$D_{2m} \times \frac{\mathbf{Z}}{2\mathbf{Z}} \simeq D_{4m}.$$

DÉMONSTRATION. Je remplace  $(\frac{\mathbf{Z}}{2\mathbf{Z}}, +)$  par  $(\{-1, 1\}, \times)$ , qui lui est isomorphe, afin de noter tous les groupes multiplicativement.

$D_{2m}$  est engendré par deux éléments  $x$  et  $y$  tels que  $\omega(x) = m$ ,  $\omega(y) = 2$  et  $y^{-1}xy = x^{-1}$ .

Soit donc  $G := D_{2m} \times \{-1, 1\}$ , et considérons  $a := (x, -1) \in G$  et

$$b := (y, -1) \in G.$$



Alors  $a = (x, 1)(1, -1)$  est d'ordre  $2m$  (les éléments  $(x, 1)$  et  $(1, -1)$  commutent et sont d'ordres premiers entre eux),  $b^{-1}ab = a^{-1}$  et  $b$  est d'ordre 2 ; donc  $\langle a, b \rangle$  est isomorphe à  $D_{4m}$ .

Mais  $\langle a, b \rangle$  est contenu dans  $G$ , d'ordre  $4m$ , donc  $G = \langle a, b \rangle \simeq D_{4m}$ .  $\square$

**11. Groupe symétrique, actions de groupes, groupe alterné.**

Soit  $X$  un ensemble non vide.

Si

$$\sigma : X \rightarrow X$$

et

$$\tau : X \rightarrow X$$

sont des bijections, leur composée  $\tau \circ \sigma$  en est une aussi, de même que l'inverse  $\sigma^{-1}$ .

L'associativité de la composition étant évidente, l'ensemble  $\Sigma(X)$  des bijections de  $X$  avec lui-même, muni de la loi  $\circ$ , forme un groupe d'élément neutre  $Id_X$  :

$$e_{\Sigma(X)} = Id_X.$$

Pour  $n \geq 1$  entier, on notera

$$\Sigma_n := \Sigma(\{1, \dots, n\})$$

(“groupe symétrique de degré  $n$ ”).

L'ordre de ce groupe est

$$|\Sigma_n| = n!.$$

En effet une application de  $\{1, \dots, n\}$  dans lui-même est bijective si et seulement si elle est injective. Donc l'ordre  $|\Sigma_n|$  est égal au nombre d'injections d'un ensemble de cardinal  $n$  dans un ensemble de cardinal  $n$ , donc au nombre d'arrangements

$$A_n^n = n(n-1)\dots(n-n+1) = n!.$$

**THÉORÈME 11.1.** *Si les ensembles  $X$  et  $Y$  ont même cardinal, les groupes  $\Sigma(X)$  et  $\Sigma(Y)$  sont isomorphes.*

**DÉMONSTRATION.**  $X$  et  $Y$  sont de même cardinal, donc il existe une bijection

$$\varphi : X \rightarrow Y.$$

On pose, pour  $\sigma \in \Sigma(X)$  :

$$\rho(\sigma) := \varphi \circ \sigma \circ \varphi^{-1}.$$

C'est une application bijective de  $\Sigma(X)$  dans  $\Sigma(Y)$  :

$$\rho(\sigma) \in \Sigma(Y).$$

De plus  $\rho$  est un morphisme de groupes. Soit en effet

$(\sigma, \tau) \in \Sigma(X)^2$  ; alors

$$\begin{aligned}
 \rho(\sigma) \circ \rho(\tau) &= (\varphi \circ \sigma \circ \varphi^{-1}) \circ (\varphi \circ \tau \circ \varphi^{-1}) \\
 &= \varphi \circ \sigma \circ \varphi^{-1} \circ \varphi \circ \tau \circ \varphi^{-1} \\
 &= \varphi \circ \sigma \circ Id_X \circ \tau \circ \varphi^{-1} \\
 &= \varphi \circ (\sigma \circ \tau) \circ \varphi^{-1} \\
 &= \rho(\sigma \circ \tau),
 \end{aligned}$$

donc  $\rho$  est un morphisme de groupes. De plus  $\rho$  est bijectif (exercice), donc est un isomorphisme ; on voit d'ailleurs que son inverse est donné par

$$(\forall \theta \in \Sigma(Y)) \rho^{-1}(\theta) = \varphi^{-1} \circ \theta \circ \varphi ;$$

en d'autres termes, c'est l'analogie de  $\rho$  lorsque l'on échange  $Y$  et  $X$  et que l'on remplace  $\varphi$  par  $\varphi^{-1}$ .  $\square$

**COROLLAIRE 11.2.** *Si  $X$  est un ensemble fini de cardinal  $n$ , alors  $\Sigma(X)$  est isomorphe à  $\Sigma_n$ .*

**DÉMONSTRATION.**  $X$  a même cardinal que  $\{1, \dots, n\}$ ; il suffit donc d'appliquer le Théorème 11.1.

**DÉFINITION 11.3.** On appelle action du groupe  $G$  sur l'ensemble non vide  $X$  une application

$$\begin{aligned}
 G \times X &\rightarrow X \\
 (g, x) &\mapsto g.x
 \end{aligned}$$

telle que

$$\mathbf{(A1)} \quad \forall (g, h, x) \in G \times G \times X \quad g.(h.x) = (gh).x$$

et

$$\mathbf{(A2)} \quad (\forall x \in X) \quad e_G.x = x.$$

**THÉORÈME 11.4.** *Soit  $G$  un groupe agissant sur un ensemble  $X$ . Pour chaque  $g \in G$  définissons une application*

$$\begin{aligned}
 \varphi(g) &: X \rightarrow X \\
 &x \mapsto g.x
 \end{aligned}$$

*Alors, pour chaque élément  $g$  de  $G$ ,  $\varphi(g) \in \Sigma(X)$  et l'application  $\varphi : G \rightarrow \Sigma(X)$  est un morphisme de groupes.*

*Réciproquement, si  $\varphi : G \rightarrow \Sigma(X)$  est un morphisme de groupes, on peut définir une action de  $G$  sur  $X$  par*

$$(\forall (g, x) \in G \times X) \quad g.x := (\varphi(g))(x).$$

DÉMONSTRATION. Soient  $g \in G$  et  $x \in X$ . Alors

$$\begin{aligned}
 (\varphi(g) \circ \varphi(g^{-1}))(x) &= \varphi(g)(\varphi(g^{-1})(x)) \\
 &= \varphi(g)(g^{-1}.x) \\
 &= g.(g^{-1}.x) \\
 &= (gg^{-1}).x \\
 &\quad \text{(d'après (A1))} \\
 &= e_G.x \\
 &\quad \text{(d'après (A2))} \\
 &= x
 \end{aligned}$$

d'où

$$\varphi(g) \circ \varphi(g^{-1}) = Id_X.$$

De même, ou bien en appliquant le résultat à  $g^{-1}$ , on voit que

$$\varphi(g^{-1}) \circ \varphi(g) = Id_X.$$

L'application  $\varphi(g) : X \rightarrow X$  est donc inversible à droite et à gauche, donc bijective, soit  $\varphi(g) \in \Sigma(X)$ .

Soit  $(g, h, x) \in G \times G \times X$  ; on a

$$\begin{aligned}
 (\varphi(g) \circ \varphi(h))(x) &= \varphi(g)(\varphi(h)(x)) \\
 &= \varphi(g)(h.x) \\
 &= g.(h.x) \\
 &= (gh).x \\
 &\quad \text{(d'après (A1))} \\
 &= \varphi(gh)(x).
 \end{aligned}$$

Donc  $\varphi(g) \circ \varphi(h) = \varphi(gh)$  et  $\varphi : G \rightarrow \Sigma(X)$  est un morphisme de groupes. Réciproquement, si  $\varphi : G \rightarrow \Sigma(X)$  est un morphisme de groupes, définissons

$$(\forall (g, x) \in G \times X) \quad g.x := (\varphi(g))(x).$$

Alors on obtient une action de  $G$  sur  $X$  (exercice : vérifier (A1) et (A2)).  $\square$

THÉORÈME 11.5. (*Théorème de Cayley*) Soit  $G$  un groupe d'ordre fini  $n$ . Alors il existe un sous-groupe de  $\Sigma_n$  isomorphe à  $G$ .

DÉMONSTRATION. On définit une action de  $G$  sur lui-même ( $X = G$ ) par

$$(\forall (g, x) \in G \times X) \quad g.x := gx.$$

Il s'agit bien d'une action de groupe. En effet

$$(\forall (g, h, x) \in G \times H \times X) \quad g.(h.x) = g.(hx) = g(hx) = (gh)x = (gh).x,$$

soit l'axiome **(A1)**. En outre

$$(\forall x \in X) \quad e_G.x = e_G x = x,$$

soit l'axiome **(A2)**.

Les deux axiomes sont satisfaits, on a donc bien une action de groupe. D'après le Théorème 11.4, on en déduit un morphisme

$$\varphi : G \rightarrow \Sigma(X) = \Sigma(G)$$

donné par

$$(\forall (g, x) \in G \times X) \quad (\varphi(g))(x) = g.x = gx.$$

En particulier

$$(\forall g \in G) \quad (\varphi(g))(e_G) = g.e_G = ge_G = g,$$

donc de  $\varphi(g) = \varphi(h)$  il suit que  $g = (\varphi(g))(e_G) = (\varphi(h))(e_G) = h$  :  $\varphi$  est injectif.

On a vu (Corollaire 11.2) que  $\Sigma(G)$  était isomorphe à  $\Sigma_n$ .

Soit  $\psi : \Sigma(G) \rightarrow \Sigma_n$  un isomorphisme.

Alors

$$\theta := \psi \circ \varphi : G \rightarrow \Sigma_n$$

est un morphisme injectif. Mais alors  $G$  est isomorphe à  $Im(\theta)$ , lequel est un sous-groupe de  $\Sigma_n$ .  $\square$

Au moyen du concept d'action de groupe, il nous est maintenant possible d'établir le Théorème de Frobenius énoncé au chapitre 8.

**THÉORÈME 11.6.** *Soient  $G$  un groupe fini d'ordre  $n$  et  $H$  un sous-groupe de  $G$  d'indice  $[G : H] = d$ . On suppose que chaque diviseur premier de  $\frac{n}{d}$  est supérieur ou égal à  $d$ . Alors  $H$  est distingué dans  $G$ .*

**DÉMONSTRATION.** Soit

$$X := G/H = \{xH \mid x \in G\}$$

l'ensemble des classes à gauche modulo  $H$ . On a  $|X| = [G : H] = d$ .

Pour  $g \in G$  et  $\alpha = xH \in X$ , définissons

$$g.\alpha = (gx)H.$$

Il est aisé de voir que l'on obtient ainsi une action de  $G$  sur  $X$ . Soit  $\varphi : G \rightarrow \Sigma(X)$  le morphisme associé à cette action, et posons

$N = \ker(\varphi)$ . Alors  $\frac{G}{N} = \frac{G}{\ker(\varphi)}$  est isomorphe à  $\text{Im}(\varphi)$ , lequel est un sous-groupe de  $\Sigma(X) \simeq \Sigma_d$ , donc

$$\frac{|G|}{|N|} = \left| \frac{G}{N} \right|$$

divise  $|\Sigma_d| = d!$ .

Soit  $g \in N$  ; alors  $\varphi(g) = Id_X$ , donc

$$gH = g.H = (\varphi(g))(H) = H$$

d'où

$$g = g.e_G \in gH = H \quad : \\ N \subset H.$$

(En fait, on peut voir que

$$N = \bigcap_{x \in G} xHx^{-1}.)$$

Il s'ensuit que

$$\frac{|H|}{|N|} = \frac{1}{\frac{|G|}{|H|}} \frac{|G|}{|N|} \\ = \frac{1}{d} \frac{|G|}{|N|}$$

divise

$$\frac{d!}{d} = (d-1)!$$

Supposons  $\frac{|H|}{|N|} \neq 1$  ; alors il existe un diviseur premier  $q$  de  $\frac{|H|}{|N|}$ . Il s'ensuit que  $q$  divise  $(d-1)! = 1.2...(d-1)$ , donc divise 1 ou 2 ... ou  $d-1$  ; en particulier  $q < d$ . Mais  $q$  divise par ailleurs  $\frac{1}{d} \frac{|G|}{|N|} = \frac{n}{d|N|}$ , donc  $q$  divise  $\frac{n}{d}$ , une contradiction.

Il s'ensuit que  $\frac{|H|}{|N|} = 1$ , donc  $|H| = |N|$  et

$$H = N = \ker(\varphi) \triangleleft G.$$

□

**COROLLAIRE 11.7. (Théorème de Frobenius)** Soient  $G$  un groupe fini d'ordre  $n$  et  $H$  un sous-groupe de  $G$  dont l'indice  $[G : H]$  est le plus petit diviseur premier  $p$  de  $n$ . Alors  $H$  est distingué dans  $G$ .

DÉMONSTRATION. Il suffit d'appliquer le Théorème 11.6 avec  $d = p$  : chaque diviseur premier de  $\frac{n}{d}$  divise  $n$ , donc est supérieur ou égal à  $p = d$ .  $\square$

Dorénavant on suppose donnée une action d'un groupe  $G$  sur un ensemble  $X$ .

Soit  $\sim$  la relation sur  $X$  définie par :

$x \sim y$  si et seulement s'il existe  $g \in G$  tel que  $y = g.x$ .

PROPOSITION 11.8.  $\sim$  est une relation d'équivalence sur  $X$ .

DÉMONSTRATION. Soit  $x \in X$  ; on a  $e_G.x = x$ , donc  $x \sim x$  d'où la réflexivité de  $\sim$ .

Si  $x \sim y$ , il existe un élément  $g$  de  $G$  tel que  $g.x = y$ .

Alors

$$g^{-1}.y = g^{-1}.(g.x) = (g^{-1}g).x = e_G.x = x,$$

donc  $y \sim x$ . Nous avons bien établi la symétrie de  $\sim$ .

Supposons maintenant que  $x \sim y$  et  $y \sim z$  ; alors il existe  $g$  et  $h$  dans  $G$  tels que  $g.x = y$  et  $h.y = z$ .

Alors  $(hg).x = h.(g.x) = h.y = z$  donc  $x \sim z$  et on obtient la transitivité de  $\sim$ .  $\square$

Les classes d'équivalence pour cette relation sont appelées les **orbites** de  $G$  sur  $X$ . On note  $\Omega_x$  ou  $\Omega(x)$  l'orbite de  $x$ .

Par définition

$$\Omega_x = \{g.x | g \in G\}.$$

Pour  $\sigma \in \Sigma_n$  on notera

$$Fix(\sigma) := \{x \in \{1, \dots, n\} | \sigma(x) = x\}$$

(ensemble des **points fixes** de  $\sigma$ ) et

$$supp(\sigma) := \{1, \dots, n\} \setminus Fix(\sigma)$$

(**support** de  $\sigma$ ).

Nous allons maintenant considérer un cas particulier important. Soit  $\sigma \in \Sigma_n$  fixé, soit  $G = \langle \sigma \rangle$ , et soit  $X := \{1, \dots, n\}$ .

Pour  $g \in G$  et  $x \in X$ , on pose  $g.x := g(x)$ .

Cela définit une action de groupe de  $G$  sur  $X$ .

DÉFINITION 11.9. On dit que l'élément  $\sigma$  de  $\Sigma_n$  est un **cycle** s'il existe pour cette action de groupe une et une seule orbite de cardinal  $> 1$ .

On voit aisément que l'ensemble  $\{a\}$  ( $a \in X$ ) est une orbite de cardinal 1 si et seulement si  $\sigma(a) = a$ , c'est-à-dire que  $a \in \text{Fix}(\sigma)$ .

Soit alors  $a_1$  un élément de l'unique orbite  $\Omega = \Omega(a_1)$  de cardinal  $> 1$ ; il existe (exercice !) un plus petit entier  $k \geq 1$  tel que  $\sigma^k(a_1) = a_1$ . Posons, pour chaque  $i \in \{2, \dots, k\}$ ,  $a_i := \sigma^{i-1}(a_1)$ ; alors

$$\Omega = \{a_1, \dots, a_k\}$$

avec  $\sigma(a_1) = a_2$ ,  $\sigma(a_{j-1}) = a_j$  pour  $2 \leq j \leq k$  et  $\sigma(a_k) = a_1$ .

Vu que  $\Omega$  est la seule orbite de longueur  $> 1$ , tous les éléments de  $\{1, \dots, n\} \setminus \Omega$  appartiennent à  $\text{Fix}(\sigma)$ , donc

$$\text{Fix}(\sigma) = \{1, \dots, n\} \setminus \Omega$$

et

$$|\text{Fix}(\sigma)| = n - k.$$

On peut donc énumérer

$$\text{Fix}(\sigma) = \{a_{k+1}, \dots, a_n\}$$

On note alors

$$\sigma = (a_1 \dots a_k)$$

ou

$$\sigma = (a_1 \dots a_k)(a_{k+1}) \dots (a_n)$$

et on pose  $l(\sigma) := k$  ("longueur" du cycle  $\sigma$ ).

EXERCICE 11.10. Pour chaque  $\sigma' \in \Sigma_n$  on a

$$\sigma'(a_1 \dots a_k)(\sigma')^{-1} = (\sigma'(a_1) \dots \sigma'(a_k)).$$

LEMME 11.11. Soit  $(\sigma, \sigma') \in \Sigma_n^2$  tel que

$$\text{supp}(\sigma) \cap \text{supp}(\sigma') = \emptyset.$$

Alors

$$\sigma \circ \sigma' = \sigma' \circ \sigma :$$

$\sigma$  et  $\sigma'$  commutent.

DÉMONSTRATION. Soit  $x \in \{1, \dots, n\}$ . Par hypothèse, on ne peut pas avoir à la fois  $x \in \text{supp}(\sigma)$  et  $x \in \text{supp}(\sigma')$ ; trois cas peuvent donc se présenter.

**Cas 1**

$x \in \text{supp}(\sigma)$  et  $x \notin \text{supp}(\sigma')$ .

Alors  $\sigma'(x) = x$  et  $\sigma(x) \neq x$ , donc  $\sigma(\sigma(x)) \neq \sigma(x)$  et  $\sigma(x) \in \text{supp}(\sigma)$ , d'où  $\sigma(x) \notin \text{supp}(\sigma')$  soit  $\sigma(x) \in \text{Fix}(\sigma')$ .

Il en résulte que

$$(\sigma' \circ \sigma)(x) = \sigma'(\sigma(x)) = \sigma(x).$$



De plus

$$(\sigma \circ \sigma')(x) = \sigma(\sigma'(x)) = \sigma(x).$$

Donc

$$(\sigma' \circ \sigma)(x) = (\sigma \circ \sigma')(x).$$

**Cas 2**

$$x \notin \text{supp}(\sigma) \text{ et } x \in \text{supp}(\sigma').$$

Il suffit de reprendre le raisonnement du Cas 1 en échangeant  $\sigma$  et  $\sigma'$  ; on trouve aussi

$$(\sigma' \circ \sigma)(x) = (\sigma \circ \sigma')(x).$$

**Cas 3**

$$x \notin \text{supp}(\sigma) \text{ et } x \notin \text{supp}(\sigma').$$

Alors

$$\sigma(x) = x \text{ et } \sigma'(x) = x,$$

d'où

$$(\sigma' \circ \sigma)(x) = \sigma'(x) = x = \sigma(x) = (\sigma \circ \sigma')(x).$$

Dans tous les cas on a donc

$$(\sigma' \circ \sigma)(x) = (\sigma \circ \sigma')(x)$$

d'où

$$\sigma' \circ \sigma = \sigma \circ \sigma'$$

□

**THÉORÈME 11.12.** *Chaque élément de  $\Sigma_n$  peut être écrit comme produit de cycles à supports deux à deux disjoints. Ces cycles commutent deux à deux.*

**DÉMONSTRATION.** Pour  $\sigma \in \Sigma_n$ , soient  $\Omega_1, \dots, \Omega_m$  les orbites de cardinal  $> 1$  pour l'action de  $\langle \sigma \rangle$  sur  $\{1, \dots, n\}$ .

Soit alors, pour chaque  $i \in \{1, \dots, m\}$ ,  $x_i \in \Omega_i$  (donc  $\Omega_i = \Omega(x_i)$ ) et posons

$$|\Omega(x_i)| = r_i > 1.$$

On a

$$\Omega(x_i) = \{\sigma^l(x_i) | l \in \mathbf{Z}\} = \{x_i, \sigma(x_i), \dots, \sigma^{r_i-1}(x_i)\}.$$

Définissons  $\sigma_i$  par  $\sigma_i(x) = \sigma(x)$  si  $x \in \Omega_i$  et  $\sigma_i(x) = x$  si  $x \notin \Omega_i$ .

Alors  $\sigma_i$  appartient à  $\Sigma_n$  (exercice), et sa seule orbite de longueur  $> 1$  est  $\Omega_i$  ;  $\sigma_i$  est donc un cycle.

Les  $(\sigma_i)_{1 \leq i \leq m}$  commutent deux à deux d'après le Lemme 11.11 (par construction  $\text{supp}(\sigma_i) = \Omega_i$  et les  $\Omega_i$  sont deux à deux disjoints), et on a (exercice)  $\sigma_1 \circ \dots \circ \sigma_m = \sigma$ . □

On voit aisément que, pour chaque  $i$ ,  $\omega(\sigma_i) = r_i$ , et que

$$\omega(\sigma) = \text{ppcm}(r_1, \dots, r_m).$$

EXERCICE 11.13. La décomposition du Théorème 11.12 est unique à l'ordre près des  $\sigma_i$  (indication : si  $\sigma'_1 \circ \dots \circ \sigma'_r = \sigma$  avec les  $\sigma'_i$  des cycles deux à deux disjoints, alors, pour chaque  $i$ ,  $\text{supp}(\sigma'_i)$  est une orbite de  $\sigma$ ).

DÉFINITION 11.14. On appelle **transposition** un cycle de longueur 2.

Pour  $(a, b) \in \{1, \dots, n\}^2$  avec  $a \neq b$ ,  $\tau_{a,b} = (ab)$  désignera la transposition  $\tau$  telle que  $\tau(a) = b$ ,  $\tau(b) = a$  et  $\tau(x) = x$  si  $x \notin \{a, b\}$ .

Il apparaît que  $\tau^2 = Id$ , donc  $\tau^{-1} = \tau$  et  $\omega(\tau) = 2$ .

THÉORÈME 11.15. *Chaque élément de  $\Sigma_n$  ( $n \geq 2$ ) peut être écrit comme produit d'au plus  $n - 1$  transpositions.*

DÉMONSTRATION.  $\sigma = Id = e_{\Sigma_n}$  est égal au produit vide, d'où le résultat dans ce cas.

Supposons maintenant  $\sigma \neq Id$ , et procédons par récurrence sur  $k := |\text{supp}(\sigma)| \geq 1$  en montrant que  $\sigma$  peut être représentée comme produit d'au plus  $k - 1$  transpositions. On aura alors le résultat car  $k - 1 \leq n - 1$ .

Si  $k = 1$ , c'est trivialement exact car cette possibilité ne saurait se présenter (exercice).

Supposons donc  $k \geq 2$  et le résultat exact pour tout  $k' < k$ . On a  $|\text{supp}(\sigma)| = k \geq 1$  donc  $\text{supp}(\sigma) \neq \emptyset$ .

Soit alors  $x \in \text{supp}(\sigma)$  et posons  $\tau := (x\sigma(x))$ .

Si  $y \in \text{Fix}(\sigma)$  alors  $y \neq x$  et  $y \neq \sigma(x)$  donc  $\tau(y) = y$  et

$$(\tau \circ \sigma)(y) = \tau(\sigma(y)) = \tau(y) = y.$$

De plus

$$(\tau \circ \sigma)(x) = \tau(\sigma(x)) = x$$

donc  $\text{Fix}(\sigma) \cup \{x\} \subset \text{Fix}(\tau \circ \sigma)$ .

Il s'ensuit que  $|\text{Fix}(\tau \circ \sigma)| \geq |\text{Fix}(\sigma)| + 1$ , d'où

$$|\text{supp}(\tau \circ \sigma)| \leq |\text{supp}(\sigma)| - 1 = k - 1 < k.$$

Par récurrence sur  $k$ , on a donc soit  $\tau \circ \sigma = Id$  (alors  $\sigma = \tau^{-1} = \tau$  est une transposition, d'où le résultat car  $1 \leq k - 1$ ) soit  $\tau \circ \sigma = \tau_1 \circ \dots \circ \tau_l$  avec les  $\tau_i$  des transpositions et  $l \leq |\text{supp}(\tau \circ \sigma)| - 1 \leq k - 2$ .

Mais dans ce dernier cas  $\sigma = \tau^{-1} \circ \tau_1 \circ \dots \circ \tau_l = \tau \circ \tau_1 \circ \dots \circ \tau_l$  est produit de  $l + 1 \leq k - 1$  transpositions.  $\square$

Les transpositions forment donc une partie génératrice de  $\Sigma_n$ .

Nous aurions pu établir ce fait autrement, en écrivant  $\sigma$  comme un produit de cycles et chaque cycle comme un produit de transpositions :

$$(a_1 \dots a_m) = (a_1 a_2)(a_2 a_3) \dots (a_{m-1} a_m)$$

(exercice !).

Nous pouvons maintenant justifier un résultat déjà annoncé (Exemples 4.6(2)).

**THÉORÈME 11.16.**  $\Sigma_n = \langle (12), (12\dots n) \rangle$ .

**DÉMONSTRATION.** Soit  $H := \langle (12), (12\dots n) \rangle$ . D'après le Théorème 11.15, il suffit de démontrer que  $H$  contient toutes les transpositions de  $\Sigma_n$ .

Posons  $\tau := (12)$  et  $\sigma := (12\dots n)$ . On a  $\sigma\tau\sigma^{-1} = (\sigma(1)\sigma(2)) = (23)$  et de même, pour chaque  $i \in \{0, \dots, n-2\}$ ,  $\sigma^i\tau(\sigma^i)^{-1} = (i+1\ i+2)$

Donc  $H$  contient les transpositions de la forme  $(k\ k+1)$  ( $1 \leq k \leq n-1$ ).

Or

$$(\forall j \in \{2, \dots, n-1\})(1\ j+1) = (j\ j+1)(1\ j)(j\ j+1);$$

il en résulte, par récurrence sur  $j$ , que  $H$  contient les transpositions  $(1\ j)$  ( $2 \leq j \leq n$ ).

Mais pour  $1 \neq j < k \leq n$  on a

$$(j\ k) = (1\ j)(1\ k)(1\ j),$$

donc  $H$  contient toutes les transpositions  $(j\ k)$  ( $1 \leq j < k \leq n$ ), d'où le résultat.  $\square$

Dorénavant nous supposons  $n \geq 2$ . Pour  $\sigma \in \Sigma_n$ , posons

$$N(\sigma) := |\{(i, j) \in \{1, \dots, n\}^2 \mid i < j \text{ et } \sigma(i) > \sigma(j)\}|.$$

(**nombre d'inversions** de  $\sigma$ ).

et

$$\epsilon(\sigma) := (-1)^{N(\sigma)}.$$

(**signature** de  $\sigma$ ).

**THÉORÈME 11.17.**  $\epsilon$  est un morphisme de  $\Sigma_n$  dans  $(\{-1, 1\}, \times)$ .

**DÉMONSTRATION.** Vu que

$$\epsilon(\sigma\sigma') := (-1)^{N(\sigma\sigma')}$$

et que

$$\epsilon(\sigma)\epsilon(\sigma') = (-1)^{N(\sigma)}(-1)^{N(\sigma')} = (-1)^{N(\sigma)+N(\sigma')},$$

il suffit, pour montrer que  $\epsilon$  est un morphisme, d'établir que

$$\forall(\sigma, \sigma') \in \Sigma_n^2 \quad N(\sigma \circ \sigma') \equiv N(\sigma) + N(\sigma') [2].$$

Soient

$$A := \{(i, j) \in \{1, \dots, n\}^2 \mid i < j, \sigma'(i) < \sigma'(j), \sigma(\sigma'(i)) > \sigma(\sigma'(j))\},$$

$$B := \{(i, j) \in \{1, \dots, n\}^2 \mid i < j, \sigma'(i) > \sigma'(j), \sigma(\sigma'(i)) > \sigma(\sigma'(j))\},$$

$$C := \{(i, j) \in \{1, \dots, n\}^2 \mid i < j, \sigma'(i) > \sigma'(j), \sigma(\sigma'(i)) < \sigma(\sigma'(j))\},$$

et

$$D := \{(i, j) \in \{1, \dots, n\}^2 \mid i > j, \sigma'(i) < \sigma'(j), \sigma(\sigma'(i)) > \sigma(\sigma'(j))\}.$$

On a

$$N(\sigma \circ \sigma') = |A \dot{\cup} B| = |A| + |B|$$

et

$$N(\sigma') = |B \dot{\cup} C| = |B| + |C|.$$

Il apparaît que

$$A \dot{\cup} D = \{(i, j) \in \{1, \dots, n\}^2 \mid \sigma'(i) < \sigma'(j), \sigma(\sigma'(i)) > \sigma(\sigma'(j))\}.$$

L'application

$$(i, j) \mapsto (\sigma'(i), \sigma'(j))$$

définit une bijection de  $A \dot{\cup} D$  sur

$$E := \{(i, j) \in \{1, \dots, n\}^2 \mid i < j, \sigma(i) > \sigma(j)\}.$$

En particulier

$$N(\sigma) = |E| = |A \dot{\cup} D| = |A| + |D|.$$

Par ailleurs l'application

$$(i, j) \mapsto (j, i)$$

définit une bijection entre  $C$  et  $D$ . On a donc  $|C| = |D|$ , d'où

$$\begin{aligned} N(\sigma) + N(\sigma') &= (|A| + |D|) + (|B| + |C|) \\ &= |A| + |B| + 2|D| \\ &\equiv |A| + |B| [2] \\ &= N(\sigma \circ \sigma'). \end{aligned}$$

□

PROPOSITION 11.18.  $\epsilon$  est surjective.

DÉMONSTRATION. Si  $\tau = (ab)$  avec  $a < b$  est une transposition, les couples  $(i, j)$  tels que  $i < j$  et  $\sigma(i) > \sigma(j)$  doivent être tels que  $i$  ou  $j$  appartienne à  $\{a, b\}$ . En considérant toutes les possibilités, on voit aisément qu'il s'agit des

$(a, k)(a + 1 \leq k \leq b)$  et des  $(l, b)(a + 1 \leq l \leq b - 1)$ , d'où

$$N(\tau) = 2(b - a) - 1$$

et  $\epsilon(\tau) = (-1)^{2(b-a)-1} = -1$ . En particulier,  $\epsilon$  est surjective.  $\square$

Soit  $\mathcal{A}_n := \ker(\epsilon)$  le **groupe alterné** de degré  $n$ .

LEMME 11.19.

$$|\mathcal{A}_n| = \frac{n!}{2}.$$

DÉMONSTRATION. On a

$$\frac{|\Sigma_n|}{|\mathcal{A}_n|} = \frac{|\Sigma_n|}{\ker(\epsilon)} \text{ si } \text{Im}(\epsilon) = \{-1, 1\},$$

d'après le Premier Théorème d'Isomorphisme et la Proposition 11.18. Il en résulte que

$$\frac{n!}{|\mathcal{A}_n|} = \frac{|\Sigma_n|}{|\mathcal{A}_n|} = \left| \frac{|\Sigma_n|}{|\mathcal{A}_n|} \right| = |\{-1, 1\}| = 2,$$

d'où en effet

$$|\mathcal{A}_n| = \frac{n!}{2}. \quad \square$$

THÉORÈME 11.20. Soit  $\sigma \in \Sigma_n$ . Si  $\tau_1, \dots, \tau_m$  sont des transpositions telles que  $\sigma = \tau_1 \dots \tau_m$ , alors  $\epsilon(\sigma) = (-1)^m$ .

DÉMONSTRATION.

$$\epsilon(\sigma) = \epsilon(\tau_1 \dots \tau_m) = \epsilon(\tau_1) \dots \epsilon(\tau_m) = (-1)^m.$$

$\square$

COROLLAIRE 11.21. . Si  $\sigma \in \Sigma_n$  et  $\tau_1, \dots, \tau_m, \tau'_1, \dots, \tau'_p$  sont des transpositions telles que  $\sigma = \tau_1 \dots \tau_m = \tau'_1 \dots \tau'_p$ , alors  $m$  et  $p$  sont de même parité, c'est-à-dire que  $m \equiv p[2]$ .

DÉMONSTRATION. D'après le Théorème 11.20,  $\epsilon(\sigma) = (-1)^m$  et  $\epsilon(\sigma) = (-1)^p$ . Donc  $(-1)^m = (-1)^p$  soit  $m \equiv p[2]$ .  $\square$

PROPOSITION 11.22. . Soit  $\sigma$  un cycle de longueur  $m$ . Alors

$$\epsilon(\sigma) = (-1)^{m-1}.$$

DÉMONSTRATION. En effet, soit  $\sigma = (a_1 \dots a_m)$  ; alors

$$\sigma = (a_1 a_2)(a_2 a_3) \dots (a_{m-1} a_m)$$

est produit de  $m - 1$  transpositions, et il suffit alors d'appliquer le Théorème 11.20.  $\square$

COROLLAIRE 11.23. . *Les cycles de longueur 3 engendrent le groupe alterné  $\mathcal{A}_n$ .*

DÉMONSTRATION. Soit  $H$  le sous-groupe de  $\Sigma_n$  engendré par les cycles de longueur 3. D'après la Proposition 11.22, les cycles de longueur 3 appartiennent au groupe alterné, d'où  $H \subset \mathcal{A}_n$ .

Réciproquement, soit  $\sigma \in \mathcal{A}_n$ . Ecrivons  $\sigma = \tau_1 \dots \tau_m$  comme un produit de transpositions ; on a  $1 = \epsilon(\sigma) = (-1)^m$  d'après le Théorème 11.20, donc  $m$  est pair :  $m = 2k$ . Mais alors

$$\sigma = (\tau_1 \tau_2) \dots (\tau_{2k-1} \tau_{2k}).$$

Il suffit donc de démontrer que le produit de deux transpositions appartient à  $H$ .

Soient alors  $\tau$  et  $\tau'$  deux transpositions.

Si elles ont deux éléments en commun,  $\tau = \tau'$  et  $\tau\tau' = Id$ .

Si elles ont un élément en commun, on peut supposer que  $\tau = (ab)$  et  $\tau' = (ac)$ . Alors  $\tau\tau' = (ab)(ac) = (acb)$  est un cycle de longueur 3 (3-cycle), donc appartient à  $H$ .

Si elles n'ont aucun élément en commun, écrivons  $\tau = (ab)$  et  $\tau' = (cd)$  avec  $a, b, c, d$  distincts. Il apparaît que

$$\tau\tau' = (ab)(cd) = (ab)(ac)(ac)(cd) = (acb)(acd)$$

est un produit de cycles de longueur 3, donc appartient à  $H$ .  $\square$

THÉORÈME 11.24. *Les seuls sous-groupes distingués de  $\mathcal{A}_n$  sont  $\{Id\}$  et  $\mathcal{A}_n$  (on dit que  $\mathcal{A}_n$  est **simple**).*

DÉMONSTRATION. Soit  $N$  un sous-groupe distingué de  $\mathcal{A}_n$ ,  $N \neq \{Id\}$ .

Nous allons tout d'abord établir que  $N$  contient un cycle de longueur 3.

Choisissons donc  $\sigma \in N$  tel que  $\sigma \neq Id$  et que  $|Fix(\sigma)|$  soit maximal sous ces conditions ; soit alors  $k$  la plus petite longueur d'un cycle apparaissant dans la décomposition de  $\sigma$ .

On a

$$\sigma = (a_1 \dots a_k) \dots ;$$

alors

$$Fix(\sigma) \cup \{a_1, \dots, a_k\} \subset Fix(\sigma^k),$$

d'où

$$|Fix(\sigma^k)| \geq |Fix(\sigma)| + k > |Fix(\sigma)|.$$

Vu que  $\sigma^k \in N$ , on a  $\sigma^k = Id$ . La longueur de chaque cycle de  $\sigma$  divise donc  $k$  ; en particulier, elle est inférieure ou égale à  $k$ , donc égale à  $k$  par définition de  $k$  :

$\sigma$  est produit de cycles disjoints de même longueur  $k$ .

Trois possibilités sont à distinguer :

**(1)  $k \geq 4$**

Soit  $\sigma = (a_1 \dots a_k) \dots$ , et posons alors  $\tau = (a_1 a_2 a_k) \in \mathcal{A}_n$  ;  
alors  $\sigma^{-1} \in N$ , d'où  $\tau \sigma^{-1} \tau^{-1} \in N$  et

$$\sigma \tau \sigma^{-1} \tau^{-1} \in N.$$

Mais

$$\sigma \tau \sigma^{-1} = (\sigma(a_1) \sigma(a_2) \sigma(a_k)) = (a_2 a_3 a_1)$$

et

$$\sigma \tau \sigma^{-1} \tau^{-1} = (a_2 a_3 a_1)(a_k a_2 a_1) = (a_1 a_k a_3)$$

Donc  $N$  contient le 3-cycle  $(a_1 a_k a_3)$ .

**(2)  $k = 3$**

Alors  $\sigma$  est un produit de 3-cycles disjoints. Si  $\sigma$  est un 3-cycle, le résultat est établi.

Dans le cas contraire, on a  $\sigma = (a_1 a_2 a_3)(a_4 a_5 a_6) \dots$

Posons  $\tau = (a_1 a_2 a_4)$  et  $\rho = \sigma \tau \sigma^{-1} \tau^{-1}$  ; comme ci-dessus on voit que  $\rho \in N$  ; de plus

$$\begin{aligned} \rho &= (\sigma(a_1) \sigma(a_2) \sigma(a_4))(a_4 a_2 a_1) \\ &= (a_2 a_3 a_5)(a_4 a_2 a_1) \\ &= (a_1 a_4 a_3 a_5 a_2). \end{aligned}$$

Alors  $Id \neq \rho \in N$  et  $|Fix(\rho)| = n - 5 > n - 6 \geq |Fix(\sigma)|$ , contredisant la définition de  $k$ .

**(3)  $k = 2$**

Alors  $\sigma$  est un produit de cycles de longueur 2, en nombre pair  $2l$  (car  $\sigma \in \mathcal{A}_n$ ) :

$$\sigma = (a_1 a_2)(a_3 a_4) \dots (a_{4l-1} a_{4l}).$$

Supposons  $l \geq 2$ , et soit  $\tau = (a_1 a_2 a_3)$  ; alors, comme ci-dessus,  $\rho := \sigma \tau \sigma^{-1} \tau^{-1} \in N$  et

$$\rho = (\sigma(a_1) \sigma(a_2) \sigma(a_3))(a_3 a_2 a_1) = (a_2 a_1 a_4)(a_3 a_2 a_1) = (a_1 a_3)(a_2 a_4)$$

et

$$|Fix(\rho)| = n - 4 > n - 4l = |Fix(\sigma)|,$$

une contradiction. On a donc  $l = 1$  et  $\sigma = (a_1a_2)(a_3a_4)$ .

Simplifions maintenant la notation :  $\sigma = (ab)(cd)$ . Vu que  $n \geq 5$ , il existe  $e \in \{1, \dots, n\}$  différent de  $a, b, c, d$ . Soit  $\tau := (acebd)$  ; alors

$$\tau\sigma\tau^{-1}\sigma^{-1} = (\tau(a)\tau(b))(\tau(c)\tau(d))(ab)(cd) = (cd)(ea)(ab)(cd) = (abe)$$

appartient à  $N$ .

Dans tous les cas,  $N$  contient un 3-cycle :  $\sigma = (abc)$ . Soit alors  $\sigma'$  un 3-cycle quelconque :  $\sigma' = (def)$  ; il existe  $\tau \in \Sigma_n$  tel que  $\tau(a) = d$ ,  $\tau(b) = e$  et  $\tau(c) = f$ .

Il apparaît que

$$\tau\sigma\tau^{-1} = \sigma'.$$

Si  $\tau \in \mathcal{A}_n$ , on obtient que  $\sigma' = \tau\sigma\tau^{-1} \in \mathcal{A}_n$ .

Si  $\tau \notin \mathcal{A}_n$ , soient  $g$  et  $h$  dans  $\{1, \dots, n\}$  distincts de  $a, b$  et  $c$ , et posons  $\tau' = (gh)$  et  $\nu = \tau\tau'$  ; alors  $\nu \in \mathcal{A}_n$  et

$$\nu\sigma\nu^{-1} = \tau\tau'\sigma(\tau')^{-1}\tau^{-1} = \tau\sigma\tau^{-1} = \sigma'$$

(car  $\tau'$  et  $\sigma$  commutent, leurs supports étant disjoints). On voit, là encore, que  $\sigma' \in N$ .

$N$  contient donc tous les cycles de longueur 3 ; le sous-groupe engendré par les cycles de longueur 3 est donc inclus dans  $N$ . Mais ce sous-groupe est  $\mathcal{A}_n$  lui-même (Corollaire 11.23), donc  $\mathcal{A}_n \subset N$  et  $N = \mathcal{A}_n$ . □

Il est naturel de chercher à déterminer les sous-groupes distingués de  $\mathcal{A}_n$  et de  $\Sigma_n$ . Il y en a en fait fort peu.

(1) **n = 3.**

$$\{Id\} \triangleleft \mathcal{A}_3 \triangleleft \Sigma_3.$$

(2) **n = 4.**

Soit

$$V := \{Id, (12)(34), (13)(24), (14)(23)\}.$$

Alors  $V \triangleleft \Sigma_4$  et  $V$  est isomorphe au groupe de Klein ; de plus

$$\frac{\Sigma_4}{V} \simeq \Sigma_3.$$

On a une chaîne de sous-groupes distingués

$$\{Id\} \triangleleft V \triangleleft \mathcal{A}_4 \triangleleft \Sigma_4.$$

Cet exemple sera repris en Travaux Dirigés.



(3)  $n \geq 5$

Dans ce cas les seuls sous-groupes distingués de  $\Sigma_n$  sont  $\{Id\}$ ,  $\mathcal{A}_n$  et  $\Sigma_n$ .

Je vous laisse le démontrer en exercice (*indication*: si  $N \triangleleft \Sigma_n$ , considérer  $N \cap \mathcal{A}_n$ ).

Ces sous-groupes forment une chaîne :

$$\{Id\} \triangleleft \mathcal{A}_n \triangleleft \Sigma_n.$$

**12. Centre, automorphismes, automorphismes intérieurs.**

Dans tout ce chapitre,  $G$  désignera un groupe, noté multiplicativement.

DÉFINITION 12.1. Soit  $x \in G$ . On appelle *centralisateur* de  $x$  dans  $G$ , et on note  $C_G(x)$ , l'ensemble

$$C_G(x) := \{y \in G \mid xy = yx\} ;$$

c'est un sous-groupe de  $G$  (exercice).

DÉFINITION 12.2. On appelle *centre* de  $G$  l'ensemble

$$Z(G) := \{y \in G \mid (\forall x \in G)xy = yx\}.$$

THÉORÈME 12.3.  $Z(G)$  est un sous-groupe abélien et distingué de  $G$ .

DÉMONSTRATION. Il est immédiat que

$$Z(G) = \bigcap_{x \in G} C_G(x),$$

donc  $Z(G)$  est un sous-groupe de  $G$ .

Soient maintenant  $x \in Z(G)$  et  $y \in G$  ; alors

$$yxy^{-1} = xy y^{-1} = x e_G = x \in Z(G),$$

donc  $Z(G) \triangleleft G$ . Par définition, un élément de  $Z(G)$  commute avec chaque élément de  $G$ , donc avec chaque élément de  $Z(G)$  ;  $Z(G)$  est donc abélien.  $\square$

Il est clair que  $G$  est abélien si et seulement si  $Z(G) = G$ .

PROPOSITION 12.4. Si  $n \geq 3$ , alors  $Z(\Sigma_n) = \{Id\}$ .

DÉMONSTRATION. Soit  $\sigma \in \Sigma_n$ ,  $\sigma \neq Id$ . Il existe  $a \in \{1, \dots, n\}$  tel que  $\sigma(a) \neq a$  ; vu qu  $n \geq 3$ , il existe alors  $b \in \{1, \dots, n\}$  différent et de  $a$  et de  $\sigma(a)$ . Soit  $\tau = (ab) \in \Sigma_n$  ; il apparaît que

$$(\tau \circ \sigma)(a) = \tau(\sigma(a)) = \sigma(a) \neq \sigma(b) = \sigma(\tau(a)) = (\sigma \circ \tau)(a),$$

d'où

$$\tau \circ \sigma \neq \sigma \circ \tau$$

et

$$\sigma \notin Z(\Sigma_n).$$

Par contraposition, le résultat s'ensuit.  $\square$

Soit  $G$  un groupe. On appelle **automorphisme** de  $G$  un isomorphisme de  $G$  dans  $G$ . On note leur ensemble  $Aut(G)$  (**groupe des automorphismes** de  $G$ ).

C'est un groupe pour la composition, d'élément neutre  $e_{Aut(G)} = Id_G$ .

**THÉORÈME 12.5.** *Pour  $x \in G$ , définissons  $i_G(x) : G \rightarrow G$  par*

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

- (1) *Pour chaque  $x \in G$ ,  $i_G(x)$  est un automorphisme de  $G$ .*
- (2)  *$i_G : G \rightarrow Aut(G)$  est un morphisme de groupes. On pose*

$$Int(G) := Im(i_G)$$

*(ensemble des automorphismes intérieurs de  $G$ ) ; c'est un sous-groupe de  $Aut(G)$ .*

- (3)  *$Int(G) \simeq \frac{G}{Z(G)}$  et  $Int(G) \triangleleft Aut(G)$ .*

**DÉMONSTRATION.** (1) Soit  $x \in G$  ; pour tout couple  $(y, z) \in G^2$  on a

$$\begin{aligned} i_G(x)(yz) &= x(yz)x^{-1} \\ &= xyzx^{-1} \\ &= xye_Gzx^{-1} \\ &= xy(x^{-1}x)zx^{-1} \\ &= (xyx^{-1})(xzx^{-1}) \\ &= i_G(x)(y)i_G(x)(z). \end{aligned}$$

Donc

$$i_G(x) : G \rightarrow G$$

est un morphisme de groupes.

On voit aisément (ou par le calcul effectué en (2) ci-dessous) que

$$i_G(x) \circ i_G(x^{-1}) = i_G(x^{-1}) \circ i_G(x) = Id_G,$$

donc  $i_G(x)$  est bijectif :  $i_G(x) \in Aut(G)$ .

- (2) Soient  $x, y$  et  $z$  des éléments de  $G$ . On a

$$\begin{aligned}
(i_G(x) \circ i_G(y))(z) &= i_G(x)(i_G(y)(z)) \\
&= i_G(x)(yzy^{-1}) \\
&= x(yzy^{-1})x^{-1} \\
&= xyzy^{-1}x^{-1} \\
&= xyz(xy)^{-1} \\
&= i_G(xy)(z).
\end{aligned}$$

Donc  $i_G(x) \circ i_G(y) = i_G(xy)$  :  $i_G$  est un morphisme de groupes.

$Int(G) := \text{Im}(i_G)$  est donc un sous-groupe de  $Aut(G)$ .

De plus

$$Int(G) = \text{Im}(i_G) \simeq \frac{G}{\ker(i_G)}.$$

Mais  $x \in \ker(i_G)$  équivaut à

$i_G(x) = Id_G$ , soit à

$(\forall y \in G) i_G(x)(y) = y$ ,

ou

$(\forall y \in G) xyx^{-1} = y$ ,

c'est-à-dire

$(\forall y \in G) xy = yx$ , soit  $x \in Z(G)$ .

Donc  $\ker(i_G) = Z(G)$

(on retrouve ainsi que  $Z(G) \triangleleft G$ ) et

$$Int(G) \simeq \frac{G}{Z(G)}.$$

Soient maintenant  $\alpha \in Aut(G)$  et  $\beta \in Int(G)$  ;  $\beta = i_G(x)$  pour un  $x \in G$ .

On a, pour tout  $y \in G$  :

$$\begin{aligned}
(\alpha\beta\alpha^{-1})(y) &= \alpha(\beta(\alpha^{-1}(y))) \\
&= \alpha(i_G(x)(\alpha^{-1}(y))) \\
&= \alpha(x\alpha^{-1}(y)x^{-1}) \\
&= \alpha(x)\alpha(\alpha^{-1}(y))\alpha(x^{-1}) \\
&= \alpha(x)y\alpha(x)^{-1} \\
&= i_G(\alpha(x))(y).
\end{aligned}$$

Donc  $\alpha\beta\alpha^{-1} = i_G(\alpha(x)) \in Int(G)$ , d'où  $Int(G) \triangleleft Aut(G)$ .  $\square$

PROPOSITION 12.6. *On suppose que  $Z(G) = \{e_G\}$ . Alors  $Z(\text{Aut}(G)) = \{\text{Id}_G\}$ .*

DÉMONSTRATION. Soit  $\alpha \in Z(\text{Aut}(G))$  ;  $\alpha$  commute avec chaque automorphisme de  $G$ , donc avec chaque automorphisme intérieur de  $G$ . Pour chaque  $x \in G$  on a donc  $\alpha \circ i_G(x) = i_G(x) \circ \alpha$ , d'où, pour tout  $y \in G$

$$\begin{aligned} \alpha(x)\alpha(y)\alpha(x)^{-1} &= \alpha(xyx^{-1}) \\ &= \alpha(i_G(x)(y)) \\ &= (\alpha \circ i_G(x))(y) \\ &= (i_G(x) \circ \alpha)(y) \\ &= i_G(x)(\alpha(y)) \\ &= x\alpha(y)x^{-1}, \end{aligned}$$

soit

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

Fixons maintenant  $x \in G$  ; l'élément  $x^{-1}\alpha(x)$  commute avec tous les  $\alpha(y)$  ( $y \in G$ ) ; mais  $\alpha$  est surjectif, donc  $x^{-1}\alpha(x)$  commute avec chaque élément de  $G$ , d'où

$$x^{-1}\alpha(x) \in Z(G) = \{e_G\}$$

et

$$\alpha(x) = x.$$

Cela vaut pour chaque  $x \in G$ , d'où  $\alpha = \text{Id}$ . □

DÉFINITION 12.7.

$$\text{Out}(G) := \frac{\text{Aut}(G)}{\text{Int}(G)}.$$

On l'appelle le groupe des **automorphismes extérieurs** de  $G$ .

EXERCICE 12.8. Si  $n \geq 3$  et  $n$  différent de 6,

$$\text{Aut}(\Sigma_n) = \text{Int}(\Sigma_n).$$

**13. Classes de conjugaison, équation des classes.**

Soit  $G$  un groupe. Le morphisme

$$i_G : G \rightarrow \text{Aut}(G)$$

peut être considéré, du fait que  $\text{Aut}(G)$  est un sous-groupe de  $\Sigma(G)$ , comme un morphisme

$$i_G : G \rightarrow \Sigma(G).$$

Ce dernier définit une action  $\cdot$  de  $G$  sur  $G$ , donnée par

$$(\forall (g, h) \in G \times G) \quad g.h := (i_G(g))(h),$$

soit

$$(\forall (g, h) \in G \times G) \quad g.h = ghg^{-1}.$$

Les orbites pour cette action sont appelées classes de conjugaison de  $G$ . On dit que  $x$  et  $y$  sont conjugués s'ils appartiennent à la même classe de conjugaison. Cela veut dire que

$$(\exists g \in G) \quad gxg^{-1} = y.$$

Pour  $x \in G$ , il apparaît que  $y \in C_G(x)$  si et seulement si  $yx = xy$ , soit  $yxxy^{-1} = x$  ou

$$(i_G(x))(y) = y ;$$

$C_G(x)$  est donc l'ensemble des points fixes de  $i_G(x)$ , et on retrouve ainsi qu'il s'agit d'un sous-groupe de  $G$ .

REMARQUE 13.1. La classe de conjugaison de  $x$  est égale à  $\{x\}$  si et seulement si

$$(\forall g \in G) \quad gxg^{-1} = x,$$

soit

$$(\forall g \in G) \quad gx = xg,$$

ou  $x \in Z(G)$ .

THÉORÈME 13.2. *Soit  $G$  un groupe fini, et soit  $\{x_1, \dots, x_r\}$  un système de représentants des classes de conjugaison de cardinal  $> 1$  de  $G$ . Alors (**équation des classes**)*

$$|G| = |Z(G)| + \sum_{i=1}^r \frac{|G|}{|C_G(x_i)|}.$$

DÉMONSTRATION. D'après la Remarque 13.1, les classes de conjugaison de  $G$  sont les  $\{x\} (x \in Z(G))$  et les  $cl_G(x_i)$ .

On a donc

$$|G| = |Z(G)| + \sum_{i=1}^r |cl_G(x_i)|.$$

Il suffit donc de démontrer que, pour chaque  $i \in \{1, \dots, r\}$ ,

$$|cl_G(x_i)| = \frac{|G|}{|C_G(x_i)|}.$$

Mais

$$cl_G(x_i) = \{gx_i g^{-1} | g \in G\}.$$

Or  $gx_i g^{-1} = hx_i h^{-1}$  équivaut à

$$h^{-1}gx_i = x_i h^{-1}g,$$

soit à

$$h^{-1}g \in C_G(x_i),$$

ou à

$$h\mathcal{L}_{C_G(x_i)}g.$$

Donc  $|cl_G(x_i)|$  est égal au nombre de classes à gauche de  $G$  selon  $C_G(x_i)$ , c'est-à-dire à  $\frac{|G|}{|C_G(x_i)|}$ .  $\square$

### 14. Théorème de Sylow (1).

Ludwig Sylow (1832-1918) était un mathématicien norvégien. Il a établi en 1872 un résultat déjà énoncé, sans démonstration, dans les notes inédites d'Evariste Galois (1811-1832). Il s'agit du socle de toute la théorie des groupes finis.

**THÉORÈME 14.1.** *Soient  $G$  un groupe fini,  $p$  un nombre premier, et  $n \geq 0$  le plus grand entier tel que  $p^n$  divise l'ordre  $|G|$  de  $G$ . Alors  $G$  contient un sous-groupe d'ordre  $p^n$ .*

Un tel sous-groupe est appelé **p-sous-groupe de Sylow** de  $G$ , ou simplement **p-Sylow** de  $G$ .

On note leur ensemble  $Syl_p(G)$ .

En fait nous allons démontrer un résultat plus fort, en suivant une preuve récente (2011) due au mathématicien britannique Geoffrey Robinson.

**THÉORÈME 14.2.** *Soient  $G$  un groupe fini,  $p$  un nombre premier, et  $n \in \mathbf{N}$  tel que  $p^n$  divise  $|G|$ . Alors il existe un sous-groupe  $H$  de  $G$  d'ordre  $|H| = p^n$ .*

**DÉMONSTRATION.** Nous allons établir par récurrence sur l'ordre  $g$  de  $G$  que le résultat est exact pour chaque  $n$  tel que  $p^n$  divise  $g$ .

Le résultat est clair pour  $g = 1$  car alors on doit avoir  $n = 0$ . Supposons donc le résultat établi pour chaque groupe d'ordre  $g' < g$ , et soit  $n \geq 0$  tel que  $p^n | g$ . Le résultat étant évident pour  $n = 0$ , nous supposerons dorénavant que  $n \geq 1$ .

On écrit l'équation des classes pour  $G$  :

$$|G| = |Z(G)| + \sum_{i=1}^r \frac{|G|}{|C_G(x_i)|}. \quad (*)$$

(1) **Cas 1.** Il existe  $i \in \{1, \dots, r\}$  tel que  $p^n \mid |C_G(x_i)|$ .

Alors, du fait que  $|C_G(x_i)| < |G|$ ,  $C_G(x_i)$  contient un sous-groupe  $H$  d'ordre  $p^n$ , et il en est donc de même de  $G$ , d'où le résultat.

(2) **Cas 2** Pour chaque  $i \in \{1, \dots, r\}$ ,  $p^n$  ne divise pas  $|C_G(x_i)|$ .

Alors, pour chaque  $i \in \{1, \dots, r\}$ ,  $p$  divise  $\frac{|G|}{|C_G(x_i)|}$ .

Or  $p$  divise  $p^n$ , lequel divise  $|G|$ , donc, en vertu de l'égalité (\*),  $p$  divise  $|Z(G)|$ .

**Cas 2)a)**  $|Z(G)| < |G|$ .



Alors, par l'hypothèse de récurrence,  $Z(G)$  contient un sous-groupe  $N$  d'ordre  $p$ . Il est clair que  $N \triangleleft G$ , et que

$$\left| \frac{G}{N} \right| = \frac{|G|}{|N|} = \frac{|G|}{p} = \frac{g}{p}$$

est divisible par  $p^{n-1}$  et est  $< g$ . Par l'hypothèse de récurrence,  $\frac{G}{N}$  contient un sous-groupe  $T$  d'ordre  $p^{n-1}$ . D'après le Théorème 5.10.1, il existe un sous-groupe  $H$  de  $G$  tel que  $T = \frac{H}{N}$ , d'où

$$\left| \frac{H}{N} \right| = \left| \frac{H}{N} \right| = |T| = p^{n-1}$$

et

$$|H| = p^{n-1}|N| = p^{n-1}p = p^n.$$

D'où le résultat.

**Cas 2)b).**  $|Z(G)| = |G|$ .

Alors  $G = Z(G)$  donc  $G$  est abélien ; de plus  $|G| = g \geq 2$  car  $n \geq 1$ .

Soit  $M$  un sous -groupe strict de  $G$  d'ordre maximal ;

$M \neq G$  donc il existe  $x \in G \setminus M$ .

Alors

$$M \langle x \rangle := \{uv \mid u \in M, v \in \langle x \rangle\}$$

est un sous-groupe de  $G$ , contenant  $M$  et aussi  $x \notin M$ , donc d'ordre  $> |M|$ .

Par définition de  $M$ , on a  $G = M \langle x \rangle$  d'où (exercice)

$$|G| = |M \langle x \rangle| = \frac{|M| |\langle x \rangle|}{|M \cap \langle x \rangle|}.$$

Donc

$$p^n \mid |M| |\langle x \rangle| = |M| \omega(x).$$

Si  $p$  divise  $|M|$ , on voit par récurrence que  $M$  contient un sous-groupe  $N$  d'ordre  $|N| = p$  ; du fait que  $G$  est abélien,  $N$  est distingué dans  $G$  et on conclut comme dans le cas 2)a).

Dans le cas contraire ( $p$  ne divise pas  $|M|$ ), on a nécessairement  $p^n \mid \omega(x) : \omega(x) = p^n k$  ( $k$  entier). Mais alors (exercice!)

$$\omega(x^k) = p^n.$$

Il s'ensuit que

$$|\langle x^k \rangle| = p^n.$$

□

Augustin-Louis Cauchy (1789-1857) avait, en 1844, établi un cas particulier du Théorème de Sylow :

**COROLLAIRE 14.3. (*Théorème de Cauchy*)** *Si  $G$  est un groupe fini et  $p$  est un nombre premier divisant l'ordre de  $G$ , alors  $G$  contient un sous-groupe d'ordre  $p$ , donc aussi un élément d'ordre  $p$ .*

**DÉMONSTRATION.** D'après le Théorème 14.2 appliqué à  $n = 1$ ,  $G$  contient un sous-groupe  $H$  d'ordre  $p$ . Mais  $H$  est nécessairement cyclique, donc engendré par un élément  $x$ , et alors

$$\omega(x) = |\langle x \rangle| = |H| = p. \quad \square$$

**EXERCICE 14.4.** Etablir directement le Théorème de Cauchy en considérant les ensembles

$$A := \{(x_1, \dots, x_p) \in G^p \mid x_1 \dots x_p = e_G\},$$

$$B := \{(x_1, \dots, x_p) \in A \mid x_1 = \dots = x_p\},$$

et

$$C := A \setminus B.$$

On pourra établir que  $p$  divise le cardinal de  $A$ , puis qu'il divise la cardinal de  $C$  (cela résulte du fait que si  $(x_1, \dots, x_p) \in C$  alors  $(x_2, \dots, x_p, x_1) \in C, \dots, (x_p, x_1, \dots, x_{p-1}) \in C$ ), et en déduire qu'il existe  $x \neq e_G$  tel que  $x^p = e_G$ .

### 15. Groupes d'ordres spéciaux.

THÉORÈME 15.1. Soient  $p$  un nombre premier et  $G$  un groupe d'ordre

$$|G| = p^n \quad (n \geq 1).$$

Alors  $Z(G) \neq \{e_G\}$ .

REMARQUE 15.2. Un groupe d'ordre  $p^n$  ( $p$  premier) est appelé  **$p$ -groupe**.

DÉMONSTRATION. On écrit l'équation des classes

$$|G| = |Z(G)| + \sum_{i=1}^r \frac{|G|}{|C_G(x_i)|}.$$

Chaque  $\frac{|G|}{|C_G(x_i)|}$  est un diviseur  $> 1$  de  $|G| = p^n$  ; il est donc de la forme  $p^k$  ( $k \geq 1$ ), et donc divisible par  $p$ . Bien évidemment  $|G| = p^n$  est divisible par  $p$ . Donc

$$|Z(G)| = |G| - \sum_{i=1}^r \frac{|G|}{|C_G(x_i)|}$$

est divisible par  $p$ , donc est différent de  $\{e_G\}$  :

$$Z(G) \neq \{e_G\}.$$

□

THÉORÈME 15.3. Soient  $p$  un nombre premier et  $G$  un groupe d'ordre  $|G| = p^2$ . Alors

$$G \simeq \frac{\mathbf{Z}}{p^2\mathbf{Z}}$$

ou

$$G \simeq \frac{\mathbf{Z}}{p\mathbf{Z}} \times \frac{\mathbf{Z}}{p\mathbf{Z}}.$$

En particulier  $G$  est commutatif.

DÉMONSTRATION. Soit  $x \in G$  ; l'ordre  $\omega(x)$  de  $x$  divise l'ordre  $p^2$  de  $G$ , d'où

$$\omega(x) \in \{1, p, p^2\}.$$

Distignons deux cas.

(1) **Cas 1** : il existe  $x \in G$  tel que  $\omega(x) = p^2$ .

Alors  $|\langle x \rangle| = \omega(x) = p^2 = |G|$  d'où  $G = \langle x \rangle$  et

$$G \simeq \frac{\mathbf{Z}}{p^2\mathbf{Z}}.$$

- (2) **Cas 2** : pour chaque  $x \in G$   $\omega(x) \in \{1, p\}$ .  
 D'après le Théorème 15.1,  $Z(G) \neq \{e_G\}$ .  
 Soit  $x \in Z(G)$ ,  $x \neq e_G$  ; alors  $\omega(x) = p$  et

$$|\langle x \rangle| = p < p^2 = |G|$$

d'où  $\langle x \rangle \neq G$ .

Il en résulte l'existence de  $y \in G \setminus \langle x \rangle$ . Nécessairement  $\omega(y) = p$ .

Mais  $\langle x \rangle \cap \langle y \rangle$  est un sous-groupe de  $\langle y \rangle$ , lequel est d'ordre  $p$ , et est différent de  $\langle y \rangle$  car  $y \notin \langle x \rangle$ , d'où  $\langle x \rangle \cap \langle y \rangle = \{e_G\}$ .

Il apparaît alors que

$$\begin{aligned} |\langle x \rangle \langle y \rangle| &= \frac{|\langle x \rangle| \cdot |\langle y \rangle|}{|\langle x \rangle \cap \langle y \rangle|} \\ &= \frac{p \cdot p}{1} \\ &= p^2. \end{aligned}$$

Donc

$$G = \langle x \rangle \langle y \rangle.$$

Mais  $\langle x \rangle$  et  $\langle y \rangle$  sont d'intersection réduite à l'élément neutre et les éléments de l'un commutent avec ceux de l'autre (du fait que  $x \in Z(G)$ ), donc

$$G \simeq \langle x \rangle \times \langle y \rangle \simeq \frac{\mathbf{Z}}{p\mathbf{Z}} \times \frac{\mathbf{Z}}{p\mathbf{Z}}.$$

□

**THÉORÈME 15.4.** Soient  $p$  un nombre premier et  $G$  un groupe d'ordre  $|G| = 2p$ .

Alors on a, soit

$$G \simeq \frac{\mathbf{Z}}{2p\mathbf{Z}},$$

soit

$$G \simeq D_{2p}.$$

**DÉMONSTRATION.** Si  $p = 2$  nous avons déjà établi ce résultat (rappelez que

$$D_4 \simeq \frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}}).$$

Supposons donc  $p \geq 3$ . D'après le Théorème de Cauchy,  $G$  contient un élément  $x$  d'ordre  $p$  et un élément  $y$  d'ordre 2. Le sous-groupe  $\langle x \rangle$  est d'ordre  $p$ , donc d'indice 2 dans  $G$ . On a donc  $\langle x \rangle \triangleleft G$  ; de plus

$2 = |\langle y \rangle|$  divise l'ordre  $|\langle x, y \rangle|$  de  $\langle x, y \rangle$  (Lagrange) ; de même  $p = |\langle x \rangle|$  divise  $|\langle x, y \rangle|$ .

Donc

$$2p \mid |\langle x, y \rangle|.$$

Il s'ensuit que

$$|\langle x, y \rangle| \geq 2p = |G| \geq |\langle x, y \rangle|,$$

d'où

$$|\langle x, y \rangle| = |G|.$$

Du fait que  $\langle x \rangle \triangleleft G$ , on a

$$y^{-1}xy \in \langle x \rangle.$$

Ecrivons alors  $y^{-1}xy = x^r$  ; il suit

$$\begin{aligned} x &= e_G^{-1}xe_G \\ &= (y^2)^{-1}xy^2 \\ &= y^{-2}xy^2 \\ &= y^{-1}(y^{-1}xy)y \\ &= y^{-1}x^r y \\ &= (y^{-1}xy)^r \\ &= (x^r)^r \\ &= x^{r^2}. \end{aligned}$$

Donc  $x^{r^2-1} = e_G$ , d'où  $p \mid r^2 - 1 = (r - 1)(r + 1)$ .

Mais alors  $p \mid r - 1$  ou  $p \mid r + 1$ .

**Cas 1 :  $p$  divise  $r - 1$ .**

Alors  $x^{r-1} = e_G$  d'où  $y^{-1}xy = x^r = x$  soit  $xy = yx$ . Or  $x$  et  $y$  sont d'ordres premiers entre eux, donc  $\omega(xy) = \omega(x)\omega(y) = 2p$  et

$$|\langle xy \rangle| = \omega(xy) = 2p = |G|.$$

On a donc

$$G = \langle xy \rangle \simeq \frac{\mathbf{Z}}{2p\mathbf{Z}}.$$

**Cas 2 :  $p$  divise  $r + 1$ .**

Alors  $x^{r+1} = e_G$  d'où  $y^{-1}xy = x^r = x^{-1}$ .

Donc  $\langle x, y \rangle \simeq D_{2p}$ , d'où  $|\langle x, y \rangle| = 2p = |G|$  et

$$G = \langle x, y \rangle \simeq D_{2p}.$$

□

**16. Groupes d'ordre au plus 15 (sauf 12).**

Soit  $G$  un groupe d'ordre  $|G| = n \leq 15$  avec  $n \neq 12$ . Nous allons déterminer les possibilités (à isomorphisme près) pour  $G$ .

LEMME 16.1. *Soit  $G$  un groupe. On suppose que*

$$(\forall x \in G) x^2 = e_G.$$

*Alors  $G$  est abélien. Si de plus  $G$  est fini, alors l'ordre  $|G|$  de  $G$  est une puissance de 2 et il existe un entier  $k \in \mathbf{N}$  tel que  $G \simeq ((\frac{\mathbf{Z}}{2\mathbf{Z}})^k, +)$ .*

DÉMONSTRATION. Pour chaque  $x \in G$  on a  $xx = x^2 = e_G$ , donc  $x = x^{-1}$ . Il en résulte que, pour tout  $(x, y) \in G^2$

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

Donc  $G$  est abélien.

Supposons maintenant  $G$  fini. Pour  $m \in \mathbf{Z}$ , notons  $\bar{m}$  sa classe dans  $\frac{\mathbf{Z}}{2\mathbf{Z}}$ , et, pour  $g \in G$ , posons

$$\bar{m}.g := g^m.$$

Cette loi externe est bien définie (vérifiez-le !) et fait de  $G$ , muni comme addition de sa loi de groupe, un  $\frac{\mathbf{Z}}{2\mathbf{Z}}$ -espace vectoriel. Étant fini, cet espace est de dimension finie  $k$ , donc  $G$  est isomorphe, en tant que  $\frac{\mathbf{Z}}{2\mathbf{Z}}$ -espace vectoriel, à  $(\frac{\mathbf{Z}}{2\mathbf{Z}})^k$ . A plus forte raison lui est-il isomorphe comme groupe abélien, d'où le résultat.  $\square$

Les cas  $n = 1$ ,  $n = 2$ ,  $n = 3$  et  $n = 4$  ont déjà été considérés.

**n = 5.**

5 est premier donc

$$G \simeq \frac{\mathbf{Z}}{5\mathbf{Z}}.$$

**n = 6.**

$6 = 2.3$ , et 3 est premier ; donc

$$G \simeq \frac{\mathbf{Z}}{6\mathbf{Z}}$$

ou

$$G \simeq \mathbf{D}_6 \simeq \Sigma_3$$

(pour une autre approche, voir les Travaux Dirigés).

**n = 7.**

7 est premier, donc

$$G \simeq \frac{\mathbf{Z}}{7\mathbf{Z}}.$$

$\mathbf{n} = 8$ .

Nous connaissons déjà cinq groupes d'ordre 8 :

$$\frac{\mathbf{Z}}{8\mathbf{Z}},$$

$$\frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{4\mathbf{Z}},$$

$$\frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}},$$

le groupe diédral

$$\mathbf{D}_8$$

et le groupe quaternionique

$$\mathbf{Q}_8.$$

Ces cinq groupes sont deux à deux non isomorphes (exercice).

Nous allons faire voir que  $G$  est nécessairement isomorphe à l'un de ces cinq groupes.

$|G| = 8$  donc, si  $x$  est un élément de  $G$ , l'ordre de  $x$  divise 8 :

$$\omega(x) \in \{1, 2, 4, 8\}.$$

S'il existe  $x \in G$  d'ordre 8, alors

$$G = \langle x \rangle \simeq \frac{\mathbf{Z}}{8\mathbf{Z}}.$$

Dorénavant, nous supposons donc que

$$(\forall x \in G) \omega(x) \in \{1, 2, 4\}.$$

Si tous les éléments de  $G$  sont d'ordre 1 ou 2, alors

$$(\forall x \in G) x^2 = e_G.$$

Il en résulte, d'après le Lemme 16.1, que

$$G \simeq \left(\frac{\mathbf{Z}}{2\mathbf{Z}}\right)^k$$

pour un  $k \in \mathbf{N}$ .

Mais alors

$$2^k = |G| = 8$$

d'où  $k = 3$  :

$$G \simeq \left(\frac{\mathbf{Z}}{2\mathbf{Z}}\right)^3.$$

Nous pouvons donc supposer que  $G$  ne contient pas d'élément d'ordre 8 mais contient au moins un élément d'ordre 4 ; soit donc  $x \in G$  tel que  $\omega(x) = 4$ . Alors  $|\langle x \rangle| = 4 < 8 = |G|$ , donc on peut trouver  $y \in G \setminus \langle x \rangle$ . Choisissons un tel  $y$  d'ordre minimal ; on a  $\omega(y) \in \{2, 4\}$  et

$$G = \langle x, y \rangle.$$

$\langle x \rangle$  est d'ordre 4, donc d'indice 2 dans  $G$ , donc distingué, d'où, comme ci-dessus,  $y^{-1}xy \in \langle x \rangle = \{1, x, x^2, x^{-1}\}$ .

Mais  $y^{-1}xy$  est d'ordre  $\omega(x) = 4$  donc  $y^{-1}xy \in \{x, x^{-1}\}$ .

Quatre cas peuvent maintenant se présenter.

**Cas 1 :**  $\omega(y) = 2$  et  $y^{-1}xy = x$ .

Alors

$$G = \langle x \rangle \langle y \rangle = \langle x \rangle \times \langle y \rangle \simeq \frac{\mathbf{Z}}{4\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}}.$$

En particulier,  $G$  est abélien.

**Cas 2 :**  $\omega(y) = 2$  et  $y^{-1}xy = x^{-1}$ .

Alors  $G = \langle x, y \rangle$ ,  $\omega(x) = 4$ ,  $\omega(y) = 2$  et  $y^{-1}xy = x^{-1}$ .

Il s'ensuit que

$$G \simeq \mathbf{D}_8.$$

**Cas 3 :**  $\omega(y) = 4$  et  $y^{-1}xy = x$ .

Le groupe  $\frac{G}{\langle x \rangle}$  est alors d'ordre  $\frac{8}{4} = 2$  ; dans ce groupe

$$\overline{y^2} = (\overline{y})^2 = e_{\frac{G}{\langle x \rangle}} = \overline{e_G},$$

soit  $y^2 \in \langle x \rangle$ . Mais  $y^2$  est d'ordre 2 d'où  $y^2 = x^2$  et

$$(x^{-1}y)^2 = x^{-2}y^2 = e_G.$$

Or  $x^{-1}y \neq e_G$ , donc  $y' := x^{-1}y \notin \langle x \rangle$  et  $y'$  est d'ordre 2. Alors  $y' \notin \langle x \rangle$  et  $\omega(y') = 2 < 4 = \omega(y)$ , contredisant la définition de  $y$ .

**Cas 4 :**  $\omega(y) = 4$  et  $y^{-1}xy = x^{-1}$ .

Comme ci-dessus, on voit que  $y^2 = x^2 \neq e_G$

Soit  $z := x^2 = y^2$  ;  $z$  commute avec  $y$  et  $x$ , donc  $x \in C_G(z)$ ,  $y \in C_G(z)$ ,  $G = \langle x, y \rangle \subset C_G(z)$ ,  $G = C_G(z)$  et  $z \in Z(G)$ .

Les éléments  $e_G, z, x, zx, y, zy, xy, zxy$  sont deux à deux distincts (exercice), et

$$(xy)^2 = xyxy = xyyy^{-1}xy = xyyx^{-1} = xxxx^{-1} = x^2 = z.$$



L'ensemble  $\{e_G, z, x, zx, y, zy, xy, zxy\}$  est de cardinal 8 ; on a donc

$$G = \{e_G, z, x, zx, y, zy, xy, zxy\}$$

et il est facile d'écrire la table de multiplication de  $G$ . On voit alors que  $G$  est isomorphe à  $\mathbf{Q}_8$  ; l'isomorphisme est donné par  $i \mapsto x, j \mapsto y, k \mapsto xy, -1 \mapsto z$ , etc. .

En fait il n'est pas nécessaire de le vérifier car le groupe  $\mathbf{Q}_8$  existe et n'est isomorphe à aucun des groupes obtenus jusqu'ici, donc il s'insère nécessairement dans ce dernier cas. Vu l'unicité de la table de multiplication obtenue,  $G \simeq \mathbf{Q}_8$ .

**n = 9.**

$9 = 3^2$  et 3 est premier, donc

$$G \simeq \frac{\mathbf{Z}}{9\mathbf{Z}}$$

ou

$$G \simeq \frac{\mathbf{Z}}{3\mathbf{Z}} \times \frac{\mathbf{Z}}{3\mathbf{Z}}.$$

**n = 10.**

$10 = 2 \cdot 5$ , 5 est premier, donc

$$G \simeq \frac{\mathbf{Z}}{10\mathbf{Z}}$$

ou

$$G \simeq \mathbf{D}_{10}.$$

**n = 11.**

11 est premier, donc

$$G \simeq \frac{\mathbf{Z}}{11\mathbf{Z}}.$$

**n = 13.**

13 est premier, donc

$$G \simeq \frac{\mathbf{Z}}{13\mathbf{Z}}.$$

**n = 14.**

$14 = 2 \cdot 7$  et 7 est premier, donc

$$G \simeq \frac{\mathbf{Z}}{14\mathbf{Z}}$$

ou

$$G \simeq \mathbf{D}_{14}.$$

**n = 15.**

D'après le Corollaire 14.3,  $G$  contient un élément  $x$  d'ordre 5 et un élément  $y$  d'ordre 3. Soit  $H = \langle x \rangle$  le sous-groupe engendré par  $x$  :  $H$  est d'ordre 5, donc d'indice  $\frac{15}{5} = 3$  dans  $G$  ; vu que 3 est le plus petit diviseur premier de  $15 = |G|$ , il résulte du Corollaire 11.7 que  $H$  est distingué dans  $G$ .

Du fait que  $x \in H$ , on a  $y^{-1}xy \in H$  d'où  $y^{-1}xy = x^r$  ( $r \in \mathbf{Z}$ ). Mais alors

$$\begin{aligned} y^{-2}xy^2 &= y^{-1}(y^{-1}xy)y \\ &= y^{-1}x^r y \\ &= (y^{-1}xy)^r \\ &= (x^r)^r \\ &= x^{r^2}, \end{aligned}$$

et de même

$$y^{-3}xy^3 = x^{r^3}.$$

Mais  $y^3 = e_G$ , d'où  $x = x^{r^3}$ ,  $x^{r^3-1} = e_G$  et  $5 = \omega(x)$  divise  $r^3 - 1$ . En considérant les différentes possibilités pour la classe de  $r$  modulo 5 (ou en invoquant le "Petit Théorème de Fermat"), on voit que  $r \equiv 1[5]$ , d'où  $x^r = x$ ,  $y^{-1}xy = x$  et  $xy = yx$ .

$x$  sont donc d'ordres premiers entre eux et commutent ; d'après la Proposition 7.6,

$$\omega(xy) = \omega(x)\omega(y) = 5.3 = 15.$$

Mais alors  $|\langle xy \rangle| = 15 = |G|$ , d'où

$$G = \langle xy \rangle \simeq \frac{\mathbf{Z}}{15\mathbf{Z}}.$$

### 17. Théorème de Sylow (2).

Soient  $G$  un groupe fini et  $p$  un nombre premier. Soit  $n$  le plus grand entier tel que

$$p^n \mid |G|.$$

On appelle  $p$ -sous-groupe de Sylow de  $G$  un sous-groupe de  $G$  d'ordre  $p^n$ . Comme vu au chapitre 11, il en existe au moins un.

On posera

$$|G|_{p'} := \frac{|G|}{p^n};$$

ce nombre n'est pas divisible par  $p$ .

THÉORÈME 17.1. (*Sylow*)

- (1) *Tout  $p$ -sous-groupe de  $G$  est contenu dans un  $p$ -sous-groupe de Sylow de  $G$ .*
- (2) *Les  $p$ -sous-groupes de Sylow de  $G$  sont conjugués (c'est-à-dire que si  $S$  et  $T$  sont des  $p$ -sous-groupes de Sylow de  $G$ , il existe  $x \in G$  tel que*

$$T = xSx^{-1} := \{xsx^{-1} \mid s \in S\}.$$

- (3) *Le nombre de  $p$ -sous-groupes de Sylow de  $G$  est congru à 1 modulo  $p$ , et il divise  $|G|_{p'}$ .*

DÉMONSTRATION. (1) Soient  $S$  un  $p$ -sous-groupe de Sylow de  $G$  et  $S'$  un  $p$ -sous-groupe de  $G$  :  $|S| = p^n$  et  $|S'| = p^k$ . Alors

$$p^k = |S'| \text{ divise } |G|,$$

donc  $k \leq n$ .

Soit

$$\mathcal{E} := \{xSx^{-1} \mid x \in G\}.$$

Pour  $s \in S'$  et  $A \in \mathcal{E}$ , posons

$$s.A := sAs^{-1} := \{sas^{-1} \mid a \in A\}.$$

Cela définit une action de  $S'$  sur  $\mathcal{E}$  (exercice). Donc  $\mathcal{E}$  se décompose en réunion d'orbites pour cette action.

Soit  $A \in \mathcal{E}$  ;

$$s_1As_1^{-1} = s_2As_2^{-1}$$

si et seulement si

$$s_1^{-1}s_2A = As_1^{-1}s_2,$$

soit

$$s_1^{-1}s_2 \in S'' := \{u \in S' \mid uA = Au\} = S' \cap N_G(A).$$

Mais alors  $S''$  est un sous-groupe de  $S'$ , donc

$$s_1 A s_1^{-1} = s_2 A s_2^{-1}$$

si et seulement si  $s_1$  et  $s_2$  sont équivalents à droite modulo  $S''$ . Le cardinal de l'orbite de  $A$  est donc  $[S' : S'']$ , lequel divise  $|S'| = p^k$ ; c'est donc une puissance de  $p$ ; en particulier, il est soit égal à 1, soit divisible par  $p$ . Le cardinal de chaque orbite est donc 1 ou un multiple de  $p$ .

Mais le cardinal de  $\mathcal{E}$  n'est pas divisible par  $p$ . En effet

$$\mathcal{E} = \{x S x^{-1} | x \in G\},$$

et

$$x S x^{-1} = y S y^{-1}$$

si et seulement si

$$x^{-1} y S = S x^{-1} y,$$

ou

$$x^{-1} y \in N_G(S).$$

Donc

$$x S x^{-1} = y S y^{-1}$$

si est seulement si  $x$  et  $y$  sont équivalents à droite modulo  $N_G(S)$ .

Il en résulte que

$$|\mathcal{E}| = [G : N_G(S)] = \frac{|G|}{|N_G(S)|} = \frac{\frac{|G|}{|S|}}{\frac{|G|}{|N_G(S)|}}$$

divise  $\frac{|G|}{p^n}$ ; en particulier il n'est pas divisible par  $p$ .

Mais  $|\mathcal{E}|$  est égal à la somme des cardinaux des orbites de  $S'$  dans son action sur  $\mathcal{E}$ ; il existe donc une orbite de cardinal non divisible par  $p$ , donc de cardinal 1.

Soit donc l'orbite de  $A$  de cardinal 1; on a

$$(\forall t \in S') t A t^{-1} = A,$$

soit  $S' \subset N_G(A)$ . Mais  $A \triangleleft N_G(A)$ , donc  $S'A$  est un sous-groupe de  $N_G(A)$  (Corollaire 6.9(1)), donc de  $G$ , et

$$|S'A| \text{ divise } |G|.$$

Mais

$$|S'A| = \frac{|S'| \cdot |A|}{|S' \cap A|}$$

est une puissance de  $p$ , donc

$$|S'A| \leq p^n = |S| = |A|.$$

Mais  $A \subset S'A$ , donc  $|S'A| \geq |A|$  et  $|S'A| = |A|$ ,  $S'A = A$  et  $S' \subset A$ .

Mais  $A$  est un conjugué de  $S$ , donc  $|A| = |S| = p^n$  et  $A$  est un  $p$ -sous-groupe de Sylow de  $G$ .

- (2) Soient  $S$  et  $S'$  deux  $p$ -sous-groupes de Sylow de  $G$ . Appliquons le raisonnement de 1) à  $S'$  : il existe un conjugué  $A = xSx^{-1}$  de  $S$  tel que  $S' \subset A$ . Mais

$$|S'| = p^n = |S| = |xSx^{-1}| = |A|$$

donc

$$S' = A = xSx^{-1}.$$

- (3) Soit  $\Omega$  l'ensemble des  $p$ -sous-groupes de Sylow de  $G$ . D'après 2),

$$\Omega = \{xSx^{-1} | x \in G\},$$

soit, avec les notations de 1),  $\Omega = \mathcal{E}$ .

De plus  $|\Omega| = [G : N_G(S)]$  n'est pas divisible par  $p$ .

Faisons agir  $S$  sur  $\Omega$ , comme en 1). L'orbite de  $S$  est  $\{S\}$ , de cardinal 1.

Supposons que  $T \in \Omega, T \neq S$ , et que l'orbite de  $T$  soit de cardinal 1. Alors

$$(\forall s \in S) sTs^{-1} = T.$$

Mais alors on voit comme en (1) que  $ST$  est un sous-groupe de  $G$  dont l'ordre est une puissance de  $p$  et divise  $|G|$ . Donc  $|ST| \leq |S|$ , et, vu que  $S \subset ST$ ,

$|S| \leq |ST| \leq |S|$ ,  $|S| = |ST|$ ,  $S = ST$ ,  $T \subset S$  et (du fait que  $|T| = p^n = |S|$ )  $T = S$ , une contradiction.

Donc toutes les orbites de  $S$  sur  $\Omega$  autres que  $\{S\}$  ont pour cardinal une puissance de  $p$  autre que 1. Il en résulte que  $|\Omega| \equiv 1[p]$ .

□

On note souvent  $n_p(G)$  le nombre de sous-groupes de Sylow de  $G$ . Nous venons de voir que  $n_p(G) \equiv 1[p]$  et  $n_p(G) \mid |G|_p'$ .

**18. Exemple d'application : les groupes d'ordre 12.**

Nous connaissons déjà quatre groupes d'ordre 12, (exercice) deux à deux non isomorphes :

$$\frac{\mathbf{Z}}{12\mathbf{Z}},$$

$$\frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{6\mathbf{Z}},$$

le groupe diédral  $D_{12}$  et le groupe alterné  $\mathcal{A}_4$ .

Soit

$$G_2 := \langle x, y \mid x^3 = 1, y^4 = 1, y^{-1}xy = x^{-1} \rangle .$$

Il est facile de voir que  $Z(G_2) = \{e, y^2\}$  et  $\frac{G_2}{Z(G_2)} \simeq \Sigma_3$  ; en particulier,  $|G_2| = 12$ .

J'affirme que tout groupe  $G$  d'ordre 12 est isomorphe à l'un des cinq groupes ci-dessus.

On sait que  $n_2(G)$  est impair et divise  $\frac{12}{4} = 3$ , donc il vaut 1 ou 3. De même  $n_3(G)$  divise 4 et est congru à 1 modulo 3, donc il vaut 1 ou 4.

**Cas 1 :**  $n_3(G) = 1$

Soit  $P$  l'unique 3-sous-groupe de Sylow de  $G$  ;  $P \triangleleft G$  et  $P$  est d'ordre 3, donc cyclique :  $P = \langle x \rangle = \{1, x, x^2\}$ .

Soit  $Q$  un 2-sous-groupe de Sylow de  $G$  ; on voit aisément que  $G = QP$ .

Si  $y$  est un élément de  $G$ ,  $xyx^{-1} \in \langle x \rangle$  d'où

$$xyx^{-1} \in \{x, x^{-1}\}.$$

Donc  $\frac{|G|}{|C_G(x)|} \leq 2$ .

**Cas 1a) :**  $G = C_G(x)$ .

Alors chaque élément de  $P$  appartient au centre  $Z(G)$  de  $G$ , donc commute avec chaque élément de  $Q$ . Donc l'application

$$(p, q) \mapsto pq$$

est un isomorphisme entre  $P \times Q$  et  $G$ , et

$$G \simeq P \times Q \simeq \frac{\mathbf{Z}}{3\mathbf{Z}} \times Q$$

est isomorphe à

$$\frac{\mathbf{Z}}{3\mathbf{Z}} \times \frac{\mathbf{Z}}{4\mathbf{Z}} \simeq \frac{\mathbf{Z}}{12\mathbf{Z}}$$

ou à

$$\frac{\mathbf{Z}}{3\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}} \simeq \frac{\mathbf{Z}}{6\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}}.$$

**Cas 1)b)**  $\frac{|G|}{|C_G(x)|} = 2$

Alors

$$C_G(x) = C_G(x) \cap G = C_G(x) \cap PQ = P(C_G(x) \cap Q)$$

d'où

$$|C_G(x)| = |P(C_G(x) \cap Q)| = |P||C_G(x) \cap Q|$$

et

$$2 = \frac{|G|}{|C_G(x)|} = \frac{|Q|}{|C_G(x) \cap Q|}.$$

Donc

$$|C_G(x) \cap Q| = 2.$$

**Cas 1)b)1) :  $Q$  est cyclique.**

Soit  $Q = \langle y \rangle$  ;  $y$  est d'ordre 4,  $G = \langle x, y \rangle$ ,  $C_G(x) \cap Q = \langle y^2 \rangle$

et

$$y^{-1}xy = x^{-1}.$$

Donc  $G \simeq G_2$ .

**Cas 1)b)2) :  $Q \simeq \frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}}$ .**

Soit  $C_G(x) \cap Q = \{e, y\}$ , et soit  $z \in Q \setminus \{e, y\}$ . Alors  $y$  et  $z$  sont d'ordre 2 et commutent, et  $Q = \{e, y, z, yz\}$ .  $x$  est d'ordre 3,  $y$  est d'ordre 2, et  $x$  et  $y$  commutent, donc  $\omega(xy) = 6$ . De plus  $\omega(z) = 2$  et  $z \notin C_G(x)$ , d'où  $z^{-1}xz = x^{-1}$  et

$$z^{-1}(xy)z = z^{-1}xzy = x^{-1}y = (xy)^{-1}.$$

Il s'ensuit que  $\langle xy, z \rangle \simeq D_{12}$  ;  $G$ , d'ordre 12, contient un sous-groupe isomorphe à  $D_{12}$  ; il lui est nécessairement égal :  $G = \langle xy, z \rangle \simeq D_{12}$ .

**Cas 2 :  $n_3(G) = 4$**

Alors  $G$  contient huit éléments d'ordre 3 (deux par 3-sous-groupe de Sylow) donc l'ensemble  $\mathcal{F}$  des éléments d'ordre différent de 3 est de cardinal  $12 - 8 = 4$ . Un 2-sous-groupe de Sylow de  $G$  doit être contenu dans  $\mathcal{F}$ , donc égal à  $\mathcal{F}$ . Le 2-sous-groupe de Sylow de  $G$  est donc unique :  $n_2(G) = 1$ . Au passage, on constate que chaque élément de  $G$  est d'ordre 1, 2, 3 ou 4.

Soit  $Q$  le 2-sous-groupe de Sylow de  $G$ . Si  $Q$  est cyclique, il contient un unique élément d'ordre 2 :  $z$ . Soit alors  $y \in G$  d'ordre 3 ; vu que  $Q \triangleleft G$ ,  $zyz^{-1} \in Q$ , et  $zyz^{-1}$  est d'ordre 2 ; on a donc  $zyz^{-1} = z$ , soit

$yz = zy$ . Mais alors  $yz$  est d'ordre 6, une contradiction.  $Q$  est donc isomorphe au groupe de Klein :

$$Q \simeq \frac{\mathbf{Z}}{2\mathbf{Z}} \times \frac{\mathbf{Z}}{2\mathbf{Z}}.$$

On peut donc écrire  $Q = \{e, a, b, c\}$  avec  $a^2 = e$ ,  $ab = c$ , etc. . Soit  $P$  un 3-sous-groupe de Sylow de  $G$  :  $|P| = 3$ , donc  $P$  est cyclique :  $P = \langle y \rangle$ . De plus  $G = PQ$ .

Du fait que  $yay^{-1} \in yQy^{-1} = Q$  et  $yay^{-1} \neq e$ , on voit que  $yay^{-1} \in \{a, b, c\}$ . Si l'on avait  $yay^{-1} = a$ ,  $ya$  serait d'ordre 6, une contradiction. Donc  $yay^{-1} \in \{b, c\}$ , et on peut supposer que  $yay^{-1} = b$ . Mais alors  $ycy^{-1}$  est distinct de  $c$ , et aussi de  $yay^{-1} = b$ , donc  $ycy^{-1} = a$  ; il s'ensuit que  $yby^{-1} = c$ .

On a

$$G = PQ = \{e, a, b, ab, y, ya, yb, yab, y^2, y^2a, y^2b, y^2ab\}.$$

A partir des relations  $a^2 = b^2 = e$ ,  $ab = ba$ ,  $y^3 = e$ ,  $yay^{-1} = b$  et  $yby^{-1} = ab$ , on peut maintenant reconstituer la table de multiplication de  $G$  ; or le groupe  $\mathcal{A}_4$  est d'ordre  $\frac{4!}{2} = 12$  et n'est isomorphe à aucun des groupes déjà rencontrés. Cette table est donc celle de  $\mathcal{A}_4$ , d'où

$$G \simeq \mathcal{A}_4.$$

En fait (vérifiez-le!) l'application  $\varphi : G \rightarrow \mathcal{A}_4$  définie par  
 $\varphi(e) = Id$ ,  $\varphi(a) = (12)(34)$ ,  $\varphi(b) = (13)(24)$ ,  $\varphi(ab) = (14)(23)$ ,  
 $\varphi(y) = (123)$ ,  $\varphi(ya) = (134)$ ,  $\varphi(yb) = (243)$ ,  $\varphi(yab) = (142)$ ,  
 $\varphi(y^2) = (132)$ ,  $\varphi(y^2a) = (234)$ ,  $\varphi(y^2b) = (124)$  et  $\varphi(y^2ab) = (143)$   
 est un isomorphisme.



### 19. Groupes abéliens finis.

Parmi eux, nous connaissons les groupes

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

on peut ensuite effectuer des produits directs.

Nous allons voir que les groupes ainsi obtenus sont, à isomorphisme près, les seuls groupes abéliens finis.

DÉFINITION 19.1. Soit  $G$  un groupe fini. Posons

$$e(G) := \text{ppcm}(\omega(x) | x \in G)$$

(**exposant** de  $G$ ).

THÉORÈME 19.2. *Si  $G$  est fini et abélien, il existe un élément  $y$  de  $G$  tel que  $\omega(y) = e(G)$ .*

REMARQUE 19.3. Cet énoncé est faux en général si  $G$  n'est pas abélien : considérons  $G = \Sigma_3$  (le plus petit groupe non-abélien). Alors  $e(G) = 6$  et  $G$  ne contient aucun élément d'ordre 6.

DÉMONSTRATION. Soit

$$e(G) = p_1^{\alpha_1} \dots p_n^{\alpha_n}$$

avec les  $p_i$  premiers deux à deux distincts et les  $\alpha_i \geq 1$ .

Pour  $i$  fixé,  $p_i^{\alpha_i}$  divise  $e(G) = \text{ppcm}(\omega(x) | x \in G)$ ; il existe donc  $x_i \in G$  tel que  $p_i^{\alpha_i}$  divise  $\omega(x_i)$ , soit  $\omega(x_i) = p_i^{\alpha_i} k_i$  avec  $k_i$  entier.

Posons alors

$$y_i := x_i^{k_i}.$$

Il apparaît que

$$\omega(y_i) = \frac{\omega(x_i)}{k_i} = p_i^{\alpha_i}$$

Les  $y_i$  commutent deux à deux et sont d'ordres deux à deux premiers entre eux donc

$$\omega(y_1 \dots y_n) = \omega(y_1) \dots \omega(y_n) = p_1^{\alpha_1} \dots p_n^{\alpha_n} = e(G).$$

□

THÉORÈME 19.4. *Soit  $G$  un groupe fini abélien ; alors il existe un entier  $r \in \mathbf{N}$  et des entiers  $a_1, \dots, a_r$  avec  $a_1 \geq 2$  et*

$$a_1 | a_2 | \dots | a_r$$

tels que

$$G \simeq \frac{\mathbf{Z}}{a_1\mathbf{Z}} \times \dots \times \frac{\mathbf{Z}}{a_r\mathbf{Z}}.$$

REMARQUE 19.5. Ce résultat est essentiellement dû à Gauss (1801), dans le contexte de la composition des formes quadratiques entières ; la version moderne provient de Frobenius et Stickelberger (1878).

DÉMONSTRATION. On procède par récurrence sur  $|G|$ , le résultat étant clair pour  $|G| = 1$ . Soit donc  $G$  d'ordre  $|G| > 1$ , et supposons que chaque groupe d'ordre  $< |G|$  satisfasse à la conclusion du Théorème.

D'après le Théorème 19.2, il existe  $x \in G$  tel que  $\omega(x) = e(G)$ .

Il existe au moins un sous-groupe  $T$  de  $G$  tel que  $T \cap \langle x \rangle = \{e\}$  : le sous-groupe  $\{e\}$ . Choisissons un de ces sous-groupes d'ordre maximal :  $H$ . On a  $H \cap \langle x \rangle = \{e\}$ , donc le sous-groupe  $H \langle x \rangle$  est un produit direct :

$$H \langle x \rangle = H \times \langle x \rangle .$$

Supposons pour le moment  $G \neq H \langle x \rangle$ , et soit alors  $y \in G \setminus H \langle x \rangle$  d'ordre minimal.

Alors  $y \neq e$  d'où  $\omega(y) \geq 2$ . Ecrivons

$$\omega(y) = q_1^{\alpha_1} \dots q_m^{\alpha_m}$$

avec les  $q_i$  premiers et deux à deux distincts et les  $\alpha_i \geq 1$ .

Si  $m \geq 2$ , on peut écrire

$$y = y_1 \dots y_m$$

où les  $y_i$  sont des puissances de  $y$  et

$$\forall i \in \{1, \dots, m\} \omega(y_i) = q_i^{\alpha_i} .$$

Si l'on avait  $m \geq 2$ , on aurait, pour chaque  $i$ ,  $\omega(y_i) < \omega(y)$ , d'où, par définition de  $y$ ,  $y_i \in H \langle x \rangle$  et  $y = y_1 \dots y_m \in H \langle x \rangle$ , une contradiction. Donc  $m = 1$  et  $\omega(y) = q_1^{\alpha_1}$ , que nous noterons plus simplement  $\omega(y) = q^\alpha$  ( $q$  premier,  $\alpha \geq 1$ ).

On a

$$\omega(y^q) = \frac{\omega(y)}{\text{pgcd}(\omega(y), q)} = \frac{q^\alpha}{\text{pgcd}(q^\alpha, q)} = \frac{q^\alpha}{q} = q^{\alpha-1} < q^\alpha = \omega(y),$$

donc, encore une fois par définition de  $y$ ,  $y^q \in H \langle x \rangle$ . Ecrivons donc

$$y^q = hx^s (h \in H, s \in \mathbf{Z}).$$

Il apparaît que

$$\begin{aligned} e &= y^{q^\beta} \\ &= (y^q)^{q^{\beta-1}} \\ &= (hx^s)^{q^{\beta-1}} \\ &= h^{q^{\beta-1}} x^{sq^{\beta-1}} \end{aligned}$$

d'où

$$(h^{q^{\beta-1}})^{-1} = x^{sq^{\beta-1}} \in H \cap \langle x \rangle = \{e\}$$

et

$$x^{sq^{\beta-1}} = e,$$

soit  $\omega(x) | sq^{\beta-1}$ .

Mais  $q^\beta = \omega(y)$  divise  $e(G) = \omega(x)$ , donc  $q^\beta$  divise  $sq^{\beta-1}$  :  $q$  divise  $s$ . Nous pouvons donc écrire  $s = qt$  ( $t \in \mathbf{Z}$ ) ; soit  $z := yx^{-t}$ . Du fait que  $y \notin H \langle x \rangle$ , on a  $z \notin H \langle x \rangle$  ; de plus

$$\begin{aligned} z^q &= (yx^{-t})^q \\ &= y^q x^{-qt} \\ &= hx^s x^{-s} \\ &= h. \end{aligned}$$

Soit maintenant  $H' = H \langle z \rangle$  ;  $H'$  est un sous-groupe de  $G$ ,  $H'$  contient  $H$ , et  $H' \neq H$  vu que  $z \in H'$  et  $z \notin H$  ; on a donc  $|H'| > |H|$ . Par définition,  $H' \cap \langle x \rangle \neq \{e\}$  ; soit donc  $w \in H' \cap \langle x \rangle$ ,  $w \neq e$ . On peut écrire  $w = h_1 z^n$  ( $h_1 \in H$ ,  $n \in \mathbf{Z}$ ).

Si  $q$  divisait  $n$ , on pourrait écrire  $n = qu$  ( $u \in \mathbf{Z}$ ) et

$$w = h_1 z^{qu} = h_1 (z^q)^u = h_1 h^u \in H$$

d'où

$$e \neq w \in H \cap \langle x \rangle = \{e\},$$

une contradiction. Donc  $q$  ne divise pas  $n$  ; il en résulte que  $q$  et  $n$  sont premiers entre eux. D'après le Théorème de Bachet-Bezout, il existe  $(\lambda, \mu) \in \mathbf{Z}^2$  tel que  $\lambda q + \mu n = 1$ . Mais alors

$$\begin{aligned} z &= z^{\lambda q + \mu n} \\ &= (z^q)^\lambda (z^n)^\mu \\ &= h^\lambda (h_1^{-1} w)^\mu \\ &= h^\lambda h_1^{-\mu} w^\mu. \end{aligned}$$

Vu que  $h \in H \subset H \langle x \rangle$ ,  $h_1 \in H \subset H \langle x \rangle$  et  $w \in \langle x \rangle \subset H \langle x \rangle$ , on trouve  $z \in H \langle x \rangle$ , une contradiction.

On a donc  $G = H \langle x \rangle = H \times \langle x \rangle$ .

Par hypothèse de récurrence, vu que  $|H| = \frac{|G|}{|\langle x \rangle|} = \frac{|G|}{\omega(x)} < |G|$ , on peut écrire

$$H \simeq \frac{\mathbf{Z}}{a_1 \mathbf{Z}} \times \dots \times \frac{\mathbf{Z}}{a_r \mathbf{Z}}$$

pour  $r \in \mathbf{N}$  et des entiers  $a_1, \dots, a_r$  tels que  $a_1 \geq 2$  et

$$a_1 | a_2 | \dots | a_r.$$

Mais alors  $H$  contient un sous-groupe isomorphe à  $\frac{\mathbf{Z}}{a_r \mathbf{Z}}$ , donc il contient un élément d'ordre  $a_r$  ;  $G$  contient donc un élément d'ordre  $a_r$ . En particulier,  $a_r$  divise  $e(G) = \omega(x)$ . Posons  $a_{r+1} = \omega(x)$  ; alors

$$a_1 | a_2 | \dots | a_r | a_{r+1}$$

et

$$\begin{aligned} G &= H \times \langle x \rangle \\ &\simeq \frac{\mathbf{Z}}{a_1 \mathbf{Z}} \times \dots \times \frac{\mathbf{Z}}{a_r \mathbf{Z}} \times \langle x \rangle \\ &\simeq \frac{\mathbf{Z}}{a_1 \mathbf{Z}} \times \dots \times \frac{\mathbf{Z}}{a_r \mathbf{Z}} \times \frac{\mathbf{Z}}{\omega(x) \mathbf{Z}} \\ &= \frac{\mathbf{Z}}{a_1 \mathbf{Z}} \times \dots \times \frac{\mathbf{Z}}{a_r \mathbf{Z}} \times \frac{\mathbf{Z}}{a_{r+1} \mathbf{Z}}. \end{aligned}$$

□

Les  $a_i$  sont uniques ; on les appelle les **facteurs invariants** de  $G$ .



## Références

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