1

Structure de groupe. Groupes finis

Cette leçon ne fait pas partie de la liste officielle des leçons, mais le sera peut être un jour.

Les notions et méthodes utilisées dans ce chapitre sont suffisamment importantes pour en justifier sa rédaction.

1.1 Quelques rappels sur les groupes

Sauf précision contraire, les groupes sont notés multiplicativement et on note 1 (ou 1_G si nécessaire) l'élément neutre.

Les notions de base : définition d'un groupe, d'un sous-groupe, d'un morphisme de groupes, de noyau et d'image avec leurs propriétés élémentaires sont supposées acquises.

Si $(G,\cdot)$ est un groupe ayant un nombre fini d'éléments son cardinal est aussi appelé l'ordre de G.

Si p,q sont deux entiers relatifs, on note $p\wedge q$ le pgcd de p et q et $p\vee q$ le ppcm de p et q.

Les anneaux quotients $\mathbb{Z}_n=\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sont supposés construits sans grande culture sur les groupes et anneaux quotients.

La fonction indicatrice d'Euler est définie par $\varphi(n)=\operatorname{card}\left(\mathbb{Z}_n^\times\right)$, où $\mathbb{Z}_n^\times$ désigne le groupe multiplicatif des éléments inversibles de $\mathbb{Z}_n$.

On vérifie que :

$$\mathbb{Z}_n^\times=\left\{\overline{k}\in\mathbb{Z}_n \mid k\wedge n=1\right\}$$

En effet, dire que $\overline{k}$ est inversible dans $\mathbb{Z}_n$ équivaut à dire qu'il existe $\overline{u}\in\mathbb{Z}_n$ tel que $\overline{k}\overline{u}=\overline{1}$ encore équivalent à dire qu'il existe deux entiers relatifs u et v tels que $ku+nv=1$, ce qui est équivalent à dire que k et n sont premiers entre eux (théorème de Bézout).

Si E est un ensemble non vide, $\mathcal{S}(E)$ est le groupe des permutations de E et $\mathcal{S}(E)$ le sous-groupe formé des permutations paires. Pour $E=\{1,\cdots,n\}$, on les note $\mathcal{S}_n$ et $\mathcal{A}_n$.

Si $\mathbb{K}$ est un corps commutatif, $\mathcal{M}_n(\mathbb{K})$ est l'algèbre des matrices carrées d'ordre n à coefficients dans $\mathbb{K}$ et $GL_n(\mathbb{K})$ le groupe des matrices inversibles.

Pour ce paragraphe, on se donne un groupe multiplicatif $(G,\cdot)$.

L'associativité du produit permet de définir les puissances entières, positives ou négatives, de $g\in G$ par :

$$\begin{cases} g^0=1 \\ \forall n\in\mathbb{N},\ g^{n+1}=g^n g \\ \forall n\in\mathbb{N}^*,\ g^{-n}=\left(g^n\right)^{-1} \end{cases}$$

On peut remarquer que pour $n\in\mathbb{N}^*$, on a aussi $g^{-n}=\left(g^{-1}\right)^n$, ce qui résulte de :

$$\left(g^{-1}\right)^n g^n=g^{-1}\cdots g^{-1}g\cdots g=1$$

Dans le cas où $(G,+)$ est un groupe additif, g^n est noté ng pour $n \in \mathbb{Z}$.

Théorème 1.1 *Pour g dans G et n, m dans $\mathbb{Z}$, on a :*

$$g^n g^m = g^{n+m}$$

et pour $h \in G$ qui commute avec g, on a :

$$(gh)^n = g^n h^n = h^n g^n$$

Démonstration. On montre tout d'abord le résultat pour n, m dans $\mathbb{N}$ par récurrence sur $m \geq 0$ à n fixé. Le résultat est évident pour $m = 0$ et le supposant acquis pour $m \geq 0$, on a :

$$g^n g^{m+1} = g^n g^m g = g^{n+m} g = g^{n+m+1}.$$

On en déduit que pour n', m' dans $\mathbb{N}$, on a :

$$g^{-n'} g^{-m'} = \left(g^{n'}\right)^{-1} \left(g^{m'}\right)^{-1} = \left(g^{m'} g^{n'}\right)^{-1} = \left(g^{m'+n'}\right)^{-1} = \left(g^{n'+m'}\right)^{-1} = g^{-n'-m'}$$

c'est-à-dire que le résultat est valable pour $n \leq 0$ et $m \leq 0$.

Pour n, m' dans $\mathbb{N}$ tels que $n \geq m'$ on a :

$$g^{n-m'} g^{m'} = g^n \Rightarrow g^n \left(g^{m'}\right)^{-1} = g^n g^{-m'} = g^{n-m'}$$

et pour $n \leq m'$, on a :

$$g^{n-m'} = \left(g^{m'-n}\right)^{-1} = \left(g^{m'} g^{-n}\right)^{-1} = g^n g^{-m'}$$

donc le résultat est valable pour $n \geq 0$ et $m \leq 0$.

On voit de manière analogue qu'il est valable pour $n \leq 0$ et $m \geq 0$.

En définitive, c'est valable pour tous n, m dans $\mathbb{Z}$.

En supposant que g et h commutent, on montre par récurrence sur $n \geq 0$ que $(gh)^n = g^n h^n$ et $gh^{n+1} = h^{n+1} g$. C'est clair pour $n = 0$ et supposant le résultat acquis pour $n \geq 0$, on a :

$$\begin{aligned}(gh)^{n+1} &= (gh)^n gh = g^n h^n gh = g^n h^n hg \\ &= g^n h^{n+1} g = g^n g h^{n+1} = g^{n+1} h^{n+1}.\end{aligned}$$

Et avec $gh = hg$, on déduit que $(gh)^n = (hg)^n = h^n g^n$.

Ensuite, pour $n' \geq 0$, on a :

$$(gh)^{-n'} = \left((gh)^{n'}\right)^{-1} = \left(g^{n'} h^{n'}\right)^{-1} = \left(h^{n'} g^{n'}\right)^{-1} = g^{-n'} h^{-n'} = h^{-n'} g^{-n'}$$

et le résultat est valable pour $n \leq 0$. ∎

Remarque 1.1 *La relation $(gh)^n = g^n h^n$ est fausse si g et h ne commutent pas, des exemples simples étant donnés dans $GL_n(\mathbb{R})$ avec $n \geq 2$ ou dans le groupe symétrique $\mathcal{S}_n$ avec $n \geq 3$.*
Par exemple, pour $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ dans $GL_n(\mathbb{R})$, on a $(AB)^2 = \begin{pmatrix} 10 & 24 \\ 24 & 58 \end{pmatrix}$ et $A^2 B^2 = \begin{pmatrix} 7 & 24 \\ 15 & 52 \end{pmatrix}$.
Dans le groupe symétrique $\mathcal{S}_3$, on a $(1,2,3) = (1,2)(2,3)$, $(1,2,3)^2 = (1,3,2)$ et $(1,2)^2 (2,3)^2 = Id$.

Définition 1.1 *Le centre (ou commutateur) $Z(G)$ d'un groupe G est la partie de G formée des éléments de G qui commutent à tous les autres éléments de G, soit :*

$$Z(G) = \{h \in G \mid \forall g \in G,\ gh = hg\}$$

Un groupe G est commutatif si, et seulement si, $Z(G) = G$.

Pour tout $g \in G$, l'application $\Phi_g : h \mapsto ghg^{-1}$ est un automorphisme de G (on dit que Φ_g est un automorphisme intérieur de G) et l'application $\Phi : g \mapsto \Phi_g$ est un morphisme de groupes de G dans $\mathrm{Aut}(G)$.

Le noyau de Φ est formé des $g \in G$ tels que $\Phi_g = Id_G$, c'est-à-dire des $g \in G$ tels que $ghg^{-1} = h$ pour tout $h \in G$, ce qui équivaut à $gh = hg$ pour tout $h \in G$. Le noyau est donc le centre de G et ce centre est un sous-groupe de G. De plus ce sous-groupe est commutatif.

Remarque 1.2 *Si on prend pour définition d'automorphismes intérieurs les applications $\Psi_g : h \mapsto g^{-1}hg$ on a $\Psi_{gg'} = \Psi_{g'} \circ \Psi_g \neq \Psi_g \circ \Psi_{g'}$ en général et l'application $\Psi : g \mapsto \Psi_g$ n'est pas un morphisme de groupes.*

Par exemple pour le groupe multiplicatif $G = GL_2(\mathbb{R})$, soient $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$.

On a $A^{-1} = A$, $B^{-1} = \begin{pmatrix} 0 & \frac{1}{2} \\ 1 & 0 \end{pmatrix}$ et pour toute matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$, on a :

$$\Psi_A(M) = A^{-1}MA = AMA = \begin{pmatrix} d & c \\ b & a \end{pmatrix}$$

et :

$$\Psi_B(M) = B^{-1}MB = \begin{pmatrix} d & \frac{c}{2} \\ 2b & a \end{pmatrix}$$

ce qui donne :

$$\Psi_A \circ \Psi_B(M) = \begin{pmatrix} a & 2b \\ \frac{c}{2} & d \end{pmatrix} \neq \Psi_B \circ \Psi_A(M) = \begin{pmatrix} a & \frac{b}{2} \\ 2c & d \end{pmatrix}$$

en général.

Exercice 1.1 *Déterminer le centre de $GL_n(\mathbb{K})$, où $\mathbb{K}$ est un corps commutatif infini.*

Solution 1.1 *On note $(E_{i,j})_{1 \leq i,j \leq n}$ la base canonique de $\mathcal{M}_n(\mathbb{K})$.*
Soit A dans le centre de $GL_n(\mathbb{K})$. Pour tout $B \in \mathcal{M}_n(\mathbb{K})$, le polynôme $\det(B - \lambda I_n)$ a au plus n racines dans $\mathbb{K}$ et il existe un scalaire $\lambda \in \mathbb{K}$ tel que $B - \lambda I_n$ soit inversible. On a alors $A(B - \lambda I_n) = (B - \lambda I_n)A$, c'est-à-dire $AB - \lambda A = BA - \lambda A$ et $AB = BA$. Donc A est dans le centre de l'anneau $\mathcal{M}_n(\mathbb{K})$.
On a alors $AE_{ij} = E_{ij}A$, pour tous i, j et :

$$AE_{ij}e_j = Ae_i = \sum_{k=1}^{n} a_{ki}e_k = E_{ij}Ae_j = E_{ij}\left(\sum_{k=1}^{n} a_{kj}e_k\right) = a_{jj}e_i.$$

Donc $a_{ki} = 0$ pour $k \in \{1, \cdots, n\} - \{i\}$ et $a_{ii} = a_{jj}$. C'est-à-dire que $A = \lambda I_n$ avec $\lambda \neq 0$.
On a donc $Z(GL_n(\mathbb{K})) = \mathbb{K}^*$.
On peut aussi remarquer que si A est dans le centre de $\mathcal{M}_n(\mathbb{K})$, alors A commute à tout projecteur p_x sur la droite $\mathbb{K}x$. On en déduit alors que toutes les droites sont stables par A et A est une homothétie.

Exercice 1.2 *Les groupes $GL_n(\mathbb{R})$ et $GL_n(\mathbb{C})$ peuvent-ils être isomorphes ?*

Solution 1.2 *Si $\varphi : GL_n(\mathbb{R}) \to GL_n(\mathbb{C})$ est un isomorphisme de groupes multiplicatifs, alors il induit un isomorphisme du centre de $GL_n(\mathbb{R})$ sur celui de $GL_n(\mathbb{C})$. En effet, dire que A est dans le centre de $GL_n(\mathbb{R})$ équivaut à dire que $AM = MA$ pour tout $M \in GL_n(\mathbb{R})$, ce qui équivaut à :*

$$\forall M \in GL_n(\mathbb{R}),\ \varphi(A)\varphi(M) = \varphi(M)\varphi(A),$$

encore équivalent à :

$$\forall M' \in GL_n(\mathbb{C}),\ \varphi(A)M' = M'\varphi(A)$$

et donc à $\varphi(A)$ est dans le centre de $GL_n(\mathbb{C})$. On aurait alors un isomorphisme de groupes multiplicatifs de $\mathbb{R}^*$ sur $\mathbb{C}^*$, ce qui est impossible puisque i est d'ordre 4 dans $\mathbb{C}^*$ et il n'y a pas d'élément d'ordre 4 dans $\mathbb{R}^*$ (voir le paragraphe 1.4 pour la notion d'ordre d'un élément dans un groupe).

1.2 Sous-groupe engendré par une partie d'un groupe. Groupes monogènes

On se donne un groupe multiplicatif $(G, \cdot)$.

Théorème 1.2 *L'intersection d'une famille quelconque $(H_i)_{i\in I}$ de sous-groupes de G est un sous-groupe de G.*

Démonstration. Soit $H = \bigcap_{i\in I} H_i$. Comme l'élément neutre 1 est dans tous les H_i, il est aussi dans H et $H \neq \emptyset$. Si g_1, g_2 sont dans H, ils sont alors dans tous les H_i, donc $g_1 g_2^{-1} \in H_i$ pour tout $i \in I$, ce qui signifie que $g_1 g_2^{-1} \in H$. On a donc montré que H un sous-groupe de G. ■

Corollaire 1.1 *Si X est une partie de $(G, \cdot)$, l'intersection de tous les sous-groupes de G qui contiennent X est un sous-groupe de G.*

Démonstration. L'ensemble des sous-groupes de G qui contiennent X est non vide puisque G en fait partie et le théorème précédent nous dit que l'intersection de tous ces sous-groupes est un sous-groupe de G. ■

Définition 1.2 *Si X est une partie de $(G, \cdot)$, le sous-groupe de G engendré par X est l'intersection de tous les sous-groupes de G qui contiennent X.*

On note $\langle X \rangle$ le sous-groupe de G engendré par X et ce sous-groupe $\langle X \rangle$ est le plus petit (pour l'ordre de l'inclusion) des sous-groupes de G qui contiennent X.

Dans le cas où X est l'ensemble vide, on a $\langle X \rangle = \{1\}$.

Si X est une partie non vide de G formée d'un nombre fini d'éléments, $x_1, \cdots, x_n$, on note $\langle X \rangle = \langle x_1, \cdots, x_n \rangle$ le groupe engendré par X.

Définition 1.3 *Si X est une partie de $(G, \cdot)$, on dit que X engendre G (ou que X est une partie génératrice de G), si $G = \langle X \rangle$.*

Définition 1.4 *On dit que G est de type fini s'il admet une partie génératrice finie.*

Définition 1.5 *On dit que G est monogène s'il existe $g_0 \in G$ tel que $G = \langle g_0 \rangle$. Si de plus, G est fini, on dit alors qu'il est cyclique (ce terme sera justifié après avoir défini la notion d'ordre d'un élément d'un groupe au paragraphe 1.4).*

Théorème 1.3 *Soient X, Y deux parties de G.*

1. *On a $X \subset \langle X \rangle$ et l'égalité est réalisée si, et seulement si X est un sous-groupe de G.*
2. *Si $X \subset Y$, on a alors $\langle X \rangle \subset \langle Y \rangle$.*
3. *En notant, pour X non vide, X^{-1} l'ensemble formé des symétriques des éléments de X, soit $X^{-1} = \{x^{-1} \mid x \in X\}$, les éléments de $\langle X \rangle$ sont de la forme $x_1 \cdot \cdots \cdot x_r$ où $r \in \mathbb{N}^*$ et les x_k sont dans $X \cup X^{-1}$ pour tout k compris entre 1 et r.*

Démonstration. Les points **1.** et **2.** se déduisent immédiatement des définitions.
Pour le point **3.** on montre tout d'abord que l'ensemble :

$$H = \left\{x_1 \cdot \cdots \cdot x_r \mid r \in \mathbb{N}^* \text{ et } x_k \in X \cup X^{-1} \text{ pour } 1 \leq k \leq r\right\}$$

est un sous-groupe de G.

Pour $x_1 \in X$, on a $1 = x_1 \cdot x_1^{-1} \in H$ et pour $x = x_1 \cdot \cdots \cdot x_r$, $y = y_1 \cdot \cdots \cdot y_s$ dans H, on a :

$$x \cdot y^{-1} = x_1 \cdot \cdots \cdot x_r \cdot y_s^{-1} \cdot \cdots \cdot y_1^{-1} \in H$$

Donc H est bien un sous-groupe de G.

Comme H est un sous-groupe de G qui contient X, on a $\langle X \rangle \subset H$. Réciproquement, tout élément $h = x_1 \cdot \cdots \cdot x_r$ de H est un produit d'éléments de $X \cup X^{-1} \subset \langle X \rangle$, donc dans $\langle X \rangle$ et on a bien $\langle X \rangle = H$. ∎

Remarque 1.3 *Le point **3.** du théorème précédent nous dit aussi que $\langle X \rangle = \langle X^{-1} \rangle = \langle X \cup X^{-1} \rangle$.*

Remarque 1.4 *On a aussi :*

$$\langle X \rangle = \left\{ \prod_{k=1}^{r} x_k^{\varepsilon_k} \mid r \in \mathbb{N}^*,\ x_k \in X \text{ et } \varepsilon_k \in \{-1, 1\} \text{ pour } 1 \leq k \leq r \right\}$$

En particulier, pour tout $g \in G$, le sous-groupe de G engendré par g est :

$$\langle g \rangle = \left\{ \prod_{k=1}^{r} g^{\varepsilon_k} \mid r \in \mathbb{N}^*,\ \varepsilon_k = \pm 1 \text{ pour } 1 \leq k \leq r \right\} = \{g^n \mid n \in \mathbb{Z}\}$$

Plus généralement, on a le résultat suivant, dans le cas commutatif.

Exercice 1.3 *Montrer que pour tout n-uplet $(g_1, \cdots, g_p)$ d'éléments de G qui commutent deux à deux (avec $p \geq 1$), on a :*

$$\langle g_1, \cdots, g_p \rangle = \left\{ \prod_{k=1}^{p} g_k^{\alpha_k} \mid (\alpha_1, \cdots, \alpha_p) \in \mathbb{Z}^p \right\}$$

et ce groupe $\langle g_1, \cdots, g_p \rangle$ est commutatif.

Solution 1.3 *En notant* $X = \{g_1, \cdots, g_p\}$, *on a* $X^{-1} = \left\{g_1^{-1}, \cdots, g_p^{-1}\right\}$ *et comme les* g_k *commutent, on déduit que :*

$$\langle g_1, \cdots, g_p\rangle = \left\{\prod_{k=1}^{m} h_k \mid m \in \mathbb{N}^* \text{ et } h_k \in X \cup X^{-1} \text{ pour } 1 \leq k \leq m\right\}$$
$$= \left\{\prod_{k=1}^{p} g_k^{\alpha_k} \mid (\alpha_1, \cdots, \alpha_p) \in \mathbb{Z}^p\right\}$$

($g_k g_j = g_j g_k$ entraîne $g_j^{-1} g_k = g_j^{-1} g_k g_j g_j^{-1} = g_j^{-1} g_j g_k g_j^{-1} = g_k g_j^{-1}$ et les éléments de $X \cup X^{-1}$ commutent).
Comme les g_k commutent, ce groupe est commutatif.

Pour une loi de groupe notée additivement, on a, dans le cas où G est commutatif :

$$\langle g_1, \cdots, g_p\rangle = \left\{\sum_{k=1}^{p} \alpha_k g_k \mid (\alpha_1, \cdots, \alpha_p) \in \mathbb{Z}^p\right\}$$

Par exemple pour le groupe additif $G = \mathbb{Z}$, on a :

$$\langle g_1, \cdots, g_p\rangle = \sum_{k=1}^{p} g_k\mathbb{Z} = \delta\mathbb{Z}$$

où $\delta \in \mathbb{N}$ est pgcd de $g_1, \cdots, g_p$.

Exercice 1.4 *Soit* $X = \{r_1, \cdots, r_n\}$ *une partie finie de* $\mathbb{Q}$ *et* $G = \langle X\rangle$ *le sous groupe de* $(\mathbb{Q}, +)$ *engendré par* X. *Montrer que* G *est monogène infini.*

Solution 1.4 *En désignant par* μ *le* ppcm *des dénominateurs de* $r_1, \cdots, r_n$, *il existe des entiers relatifs* $a_1, \cdots, a_n$ *tels que* $r_k = \dfrac{a_k}{\mu}$ *pour tout* k *compris entre* 1 *et* n *et en désignant par* δ *le* pgcd *de* $a_1, \cdots, a_n$, *on a :*

$$G = \left\{\sum_{k=1}^{n} \alpha_k \frac{a_k}{\mu} \mid (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n\right\}$$
$$= \left\{\frac{\delta}{\mu}\sum_{k=1}^{n} \alpha_k b_k \mid (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n\right\}$$

où $b_1, \cdots, b_n$ sont des entiers relatifs premiers entre eux dans leur ensemble. On a donc $G = \dfrac{\delta}{\mu}\mathbb{Z}$, *ce qui signifie que G est monogène engendré par* $\dfrac{\delta}{\mu}$.

1.3 Sous-groupes distingués. Groupes quotients

On se donne un groupe multiplicatif $(G, \cdot)$.
Si H est une partie non vide G, on note, pour tout $g \in G$:

$$gH = \{gh \mid h \in H\} \text{ et } Hg = \{hg \mid h \in H\}.$$

Dans le cas où G est commutatif, on a $gH = Hg$.

Théorème 1.4 *Pour tout sous-groupe H de G, la relation $\mathcal{R}_g$ (ou de manière plus précise $(\mathcal{R}_H)_g$) définie sur G par :*

$$g_1 \mathcal{R}_g g_2 \Leftrightarrow g_1^{-1} g_2 \in H$$

est une relation d'équivalence.

Démonstration. Pour tout $g \in G$, on a $g^{-1}g = 1 \in H$, donc $\mathcal{R}_g$ est réflexive.

Si g_1, g_2 dans G sont tels que $g_1^{-1}g_2 \in H$, on a alors $\left(g_1^{-1}g_2\right)^{-1} = g_2^{-1}g_1 \in H$, ce qui signifie que $g_2 \mathcal{R}_g g_1$. Cette relation est donc symétrique.

Si g_1, g_2, g_3 dans G sont tels que $g_1^{-1}g_2 \in H$ et $g_2^{-1}g_3 \in H$, on a alors $g_1^{-1}g_3 = \left(g_1^{-1}g_2\right)\left(g_2^{-1}g_3\right) \in H$, ce qui signifie que $g_1 \mathcal{R}_g g_3$. Cette relation est donc transitive. ∎

Avec les notations du théorème précédent, on note, pour tout $g \in G$, $\overline{g}$ la classe d'équivalence de g modulo $\mathcal{R}_g$ et on dit que $\overline{g}$ est la classe à gauche modulo H de g.

On a donc, pour tout $g \in G$:

$$h \in \overline{g} \Leftrightarrow g \mathcal{R}_g h \Leftrightarrow g^{-1}h \in H \Leftrightarrow \exists k \in H \mid h = gk \Leftrightarrow h \in gH$$

c'est-à-dire que $\overline{g} = gH$.

En particulier, $\overline{1} = H$ et $\overline{g} = H$ si, et seulement si, $g \in H$.

L'ensemble de toutes ces classes d'équivalence est noté G/H et on l'appelle l'ensemble des classes à gauche modulo H.

On a donc :

$$G/H = \{\overline{g} \mid g \in G\} = \{gH \mid g \in G\}.$$

Remarque 1.5 *On peut définir, de manière analogue l'ensemble :*

$$H\backslash G = \{Hg \mid g \in G\}$$

des classes à droites modulo H à partir de la relation d'équivalence :

$$g_1 \mathcal{R}_d g_2 \Leftrightarrow g_1 g_2^{-1} \in H$$

La relation d'équivalence $\mathcal{R}_g$ nous fourni une partition de G.

Théorème 1.5 *Si H est un sous-groupe de G, alors l'ensemble des classes à gauche [resp. à droite] modulo H deux à deux distinctes forme une partition de G.*

Démonstration. Notons :

$$G/H = \{\overline{g_i} = g_i H \mid i \in I\}$$

l'ensemble des classes à gauche modulo H deux à deux distinctes.

Pour tout $g \in g$, il existe un unique indice $i \in I$ tel que $\overline{g} = \overline{g_i}$, donc $G = \bigcup_{i \in I} \overline{g_i}$. Dire que g est dans $\overline{g_j} \cap \overline{g_k}$ signifie que g est équivalent à gauche modulo H à g_j et g_k et donc par transitivité g_j et g_k sont équivalents, ce qui revient à dire que $\overline{g_j} = \overline{g_k}$. Les classes à gauche modulo H forment donc bien une partition de G.

On peut aussi tout simplement dire que dès qu'on a une relation d'équivalence, sur G les classes d'équivalence partitionnent G. ∎

Définition 1.6 *Si H est un sous-groupe de G, le cardinal de l'ensemble G/H est noté $[G : H]$ et on l'appelle l'indice de H dans G.*

Exercice 1.5 *Montrer que, pour tout sous-groupe H de G, on a :*

$$\operatorname{card}(G/H) = \operatorname{card}(G\backslash H).$$

Solution 1.5 *En remarquant que l'application $g \mapsto g^{-1}$ réalise un isomorphisme de G, on en déduit que l'application :*

$$\begin{array}{rccc} \varphi : & G/H & \to & G\backslash H \\ & gH & \mapsto & Hg^{-1} \end{array}$$

est bijective. On vérifie d'abord qu'elle est bien définie : si $gH = g'H$, on a alors $(gH)^{-1} = Hg^{-1} = (g'H)^{-1} = H(g')^{-1}$. Puis qu'elle est injective : $Hg^{-1} = H(g')^{-1}$ entraîne $(Hg^{-1})^{-1} = gH = \left(H(g')^{-1}\right)^{-1} = g'H$. Comme est surjective, c'est une bijection.

L'application :

$$\begin{array}{rccc} \pi : & G & \to & G/H \\ & g & \mapsto & \overline{g} = gH \end{array}$$

est surjective. On dit que c'est la surjection canonique de G sur G/H.

Dans le cas des groupes finis, la partition en classes à gauche modulo H nous donne le résultat de démonstration élémentaire suivant qui a de nombreuses applications.

Théorème 1.6 (Lagrange) *Soient G un groupe fini d'ordre $n \geq 2$ et H un sous-groupe de G. Pour tout $g \in G$ on a $\operatorname{card}(gH) = \operatorname{card}(H)$ et :*

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

donc l'ordre de H divise celui de G.

Démonstration. Pour g fixé dans le groupe G, la « translation à gauche » $h \mapsto gh$ est une bijection de G sur G et sa restriction à H réalise une bijection de H sur gH. Il en résulte que gH et H ont même cardinal.

L'ensemble des classes à gauche suivant H réalise une partition de G et ces classes sont en nombre fini de même cardinal égal à celui de H, il en résulte que :

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

et $\operatorname{card}(H)$ divise $\operatorname{card}(G)$. ∎

Pour $n = 1$, on a $H = G = \{Id\}$ et $[G : H] = 1$.

Le théorème de Lagrange peut aussi se traduire par :

$$[G : H] = \operatorname{card}(G/H) = \frac{\operatorname{card}(G)}{\operatorname{card}(H)}.$$

Ce résultat peut être utilisé pour montrer que $\operatorname{card}(\mathcal{S}(E)) = n!$ où $\mathcal{S}(E)$ est le groupe des permutations d'un ensemble E à n éléments.

Exercice 1.6 *Soit $E = \{x_1, \cdots, x_n\}$ un ensemble à $n \geq 2$ éléments et H le sous-ensemble de $\mathcal{S}(E)$ formé des permutations de E qui laissent stable x_n.*

1. *Montrer que H est un sous-groupe de $\mathcal{S}(E)$ isomorphe à $\mathcal{S}(F)$, où $F = \{x_1, \cdots, x_{n-1}\}$.*
2. *En désignant, pour tout entier k compris entre 1 et $n-1$, par τ_k la permutation $\tau_k = (x_k, x_n)$, montrer que $\mathcal{S}(E)/H = \{\tau_1 H, \cdots, \tau_{n-1} H, H\}$.*
3. *En déduire que $\operatorname{card}(\mathcal{S}(E)) = n \operatorname{card}(\mathcal{S}(F))$ et conclure.*

Solution 1.6

1. *$Id \in H$ et pour σ_1, σ_2 dans H, on a $\sigma_1\sigma_2^{-1}(x_n) = \sigma_1(x_n) = x_n$, donc $\sigma_1\sigma_2^{-1} \in H$ et H est un sous-groupe de $\mathcal{S}(E)$. L'application qui associe à $\sigma \in H$ sa restriction à F réalise un isomorphisme de H sur $\mathcal{S}(F)$.*
2. *On note $\tau_n = Id$. Soient $\sigma \in \mathcal{S}(E)$ et $k \in \{1, \cdots, n\}$ tel que $\sigma(x_n) = x_k$. Avec $\tau_k^{-1}\sigma(x_n) = \tau_k^{-1}(x_k) = x_n$, on déduit que $\tau_k^{-1}\sigma \in H$, c'est-à-dire que $\sigma \backsim_H \tau_k$ et $\sigma H = \tau_k H$. On a donc $\mathcal{S}(E)/H = \{\tau_1 H, \cdots, \tau_n H\}$.*
3. *On en déduit que :*

$$\operatorname{card}(\mathcal{S}(E)) = \operatorname{card}(\mathcal{S}(E)/H)\operatorname{card}(H) = \operatorname{card}(\mathcal{S}(E)/H)\operatorname{card}(\mathcal{S}(F))$$

Pour $1 \leq k \neq j \leq n$ et σ, σ' dans H, on a $\tau_k\sigma(x_n) = \tau_k(x_n) = x_k \neq x_j = \tau_j\sigma'(x_n)$, donc $\tau_k\sigma \neq \tau_j\sigma'$ et $\tau_k H \neq \tau_j H$. Il en résulte que $\operatorname{card}(\mathcal{S}(E)/H) = n$ et $\operatorname{card}(\mathcal{S}(E)) = n\operatorname{card}(\mathcal{S}(F))$. On conclut alors par récurrence sur $n \geq 1$. Pour $n = 1$, on a $\operatorname{card}(\mathcal{S}(E)) = 1$ et supposant le résultat acquis au rang $n - 1 \geq 1$, on déduit de ce qui précède que $\operatorname{card}(\mathcal{S}(E)) = n(n-1)! = n!$

Exercice 1.7 *Soient H un sous-groupe de G et K un sous-groupe de H. Montrer que si l'indice de K dans G est fini, alors l'indice de H dans G et celui de K dans H sont aussi finis et on a :*

$$[G : K] = [G : H][H : K]$$

Solution 1.7 *On note respectivement $(g_i H)_{i\in I}$ et $(h_j K)_{j\in J}$ les classes à gauches modulo H dans G et modulo K dans H deux à deux distinctes.*
Nous allons alors montrer que la famille des classes à gauches modulo K dans G deux à deux distinctes est $(g_i h_j K)_{(i,j)\in I\times J}$. Dans le cas où $[G : K]$ est fini, il n'y a qu'un nombre fini de telles classes, ce qui impose que I et J sont finis et on a :

$$[G : K] = \operatorname{card}(I \times J) = \operatorname{card}(I)\operatorname{card}(J) = [G : H][H : K]$$

Montrons le résultat annoncé.
Si $g \in G$, il existe un unique indice $i \in I$ tel que $gH = g_i H$ et il existe $h \in H$ tel que $g = g_i h$. De même il existe un unique indice $j \in J$ tel que $hK = h_j K$ et h s'écrit $h = h_j k$ avec $k \in K$, ce qui donne $g = g_i h_j k \in g_i h_j K$, soit $g \sim_K g_i h_j$ et $gK = g_i h_j K$. Les classes à gauche dans G modulo K sont donc les $g_i h_j K$ pour $(i, j) \in I \times J$. Il reste à montrer que ces classes sont deux à deux distinctes.
Si (i, j) et (i', j') dans $I \times J$ sont tels que $g_i h_j K = g_{i'} h_{j'} K$, il existe $k \in K$ tel que $g_i h_j = g_{i'} h_{j'} k$ et $g_i = g_{i'}\left(h_{j'} k h_j^{-1}\right)$ avec $h_{j'} k h_j^{-1} \in H$, donc $g_i \sim_H g_{i'}$, soit $g_i H = g_{i'} H$ et $i = i'$. Il en résulte que $h_j = h_{j'} k$ avec $k \in K$ et $h_j K = h_{j'} K$, qui équivaut à $j = j'$.

Définition 1.7 *On dit qu'une relation d'équivalence $\mathcal{R}$ sur G est compatible avec la loi de G si, pour tous g, g', h dans G, on a :*

$$(g\mathcal{R}g') \Rightarrow (gh\mathcal{R}g'h \text{ et } hg\mathcal{R}hg')$$

Théorème 1.7 *Si H est un sous-groupe de G, alors la relation d'équivalence $\mathcal{R}_g$ associée à H est compatible avec la loi de G si, et seulement si, $gH = Hg$ pour tout $g \in G$.*

Démonstration. Supposons $\mathcal{R}_g$ compatible avec la loi de G.

Pour tout $k \in gH$, on a $g^{-1}k\mathcal{R}_g 1$ et avec la compatibilité à gauche et à droite, on déduit que $g\left(g^{-1}k\right)\mathcal{R}_g g$ et $g\left(g^{-1}k\right)g^{-1}\mathcal{R}_g g g^{-1}$, soit $kg^{-1}\mathcal{R}_g 1$, ce qui revient à dire que $k \in Hg$. On a donc $gH \subset Hg$.

De manière analogue, on voit que $Hg \subset gH$ et donc $gH = Hg$ (si $k \in Hg$, alors $kg^{-1}\mathcal{R}_g 1$, donc $\left(kg^{-1}\right)g\mathcal{R}_g g$ et $g^{-1}\left(kg^{-1}\right)g\mathcal{R}_g g^{-1}g$, soit $g^{-1}k\mathcal{R}_g 1$ et $k \in gH$).

Réciproquement, supposons que $gH = Hg$ pour tout $g \in G$. Si $g\mathcal{R}_g g'$ et $h \in G$, on a alors $(gh)^{-1}g'h = h^{-1}g^{-1}g'h$ avec $g^{-1}g' \in H$, donc $g^{-1}g'h \in Hh = hH$ et $(gh)^{-1}g'h = h^{-1}hk = k \in H$, c'est-à-dire que $gh\mathcal{R}_g g'h$. Puis avec $(hg)^{-1}hg' = g^{-1}h^{-1}hg' = g^{-1}g' \in H$, on déduit que $hg\mathcal{R}_g hg'$. Donc $\mathcal{R}_g$ est compatible avec la loi de G. ∎

Définition 1.8 *On dit qu'un sous-groupe H de G est distingué (ou normal) si on a $gH = Hg$ pour tout $g \in G$.*

On note $H \lhd G$ pour signifier que H est un sous-groupe distingué de G.

Exemple 1.1 *$\{1\}$ et G sont toujours distingués dans G.*

Exemple 1.2 *Si le groupe G est commutatif, alors tous ses sous-groupes sont distingués.*

Remarque 1.6 *Un sous-groupe H de G est distingué si, et seulement si, on a $gHg^{-1} = H$ (ou $H = g^{-1}Hg$) ce qui équivaut à dire que $ghg^{-1} \in H$ (ou $g^{-1}hg \in H$) pour tout $(h, g) \in H \times G$, qui est encore équivalent à dire que H est stable par tout automorphisme intérieur $h \mapsto ghg^{-1}$.*

Exercice 1.8 *Montrer que l'intersection de deux sous-groupes distingués de G est un sous-groupe distingué.*

Solution 1.8 *Si H, K sont distingués dans G, pour tous $g \in G$ et $h \in H \cap K$, on a $ghg^{-1} \in H \cap K$.*

Exercice 1.9 *Soit H un sous-groupe de G. Montrer que :*

$$(H \lhd G) \Leftrightarrow (\forall g \in G,\ gH \subset Hg) \Leftrightarrow \left(\forall g \in G,\ gHg^{-1} \subset H\right)$$

Solution 1.9 *Il est clair que :*

$$(H \lhd G) \Rightarrow (\forall g \in G,\ gH \subset Hg) \Rightarrow \left(\forall g \in G,\ gHg^{-1} \subset H\right)$$

Si $gHg^{-1} \subset H$ pour tout $g \in H$, on a alors $gH \subset Hg$ et $g^{-1}Hg \subset H$ (l'hypothèse pour g^{-1}) et $Hg \subset gH$, ce qui donne $gH = Hg$.

Le résultat qui suit est souvent utilisé pour montrer qu'un sous-groupe est distingué.

Théorème 1.8 *Si G, G' sont deux groupes et φ un morphisme de groupes de G dans G', alors $\ker(\varphi)$ est un sous-groupe distingué de G.*

Démonstration. Pour $(g, h) \in G \times \ker(\varphi)$, on a :

$$\varphi\left(g^{-1}hg\right) = \varphi\left(g^{-1}\right)\varphi(h)\varphi(g) = \varphi(g)^{-1} \cdot 1_{G'} \cdot \varphi(g) = 1_{G'}$$

c'est-à-dire que $g^{-1}hg \in \ker(\varphi)$. Le sous-groupe $\ker(\varphi)$ de G est donc distingué. ∎

Exemple 1.3 *Si $\mathbb{K}$ est un corps commutatif, alors l'ensemble :*

$$SL_n(\mathbb{K}) = \{A \in \mathcal{M}_n(\mathbb{K}) \mid \det(A) = 1\}$$

est un sous-groupe distingué de $GL_n(\mathbb{K})$ comme noyau du morphisme de groupes :

$$\det : A \in GL_n(\mathbb{K}) \mapsto \det(A) \in \mathbb{K}^*.$$

Exemple 1.4 *$\mathcal{O}_n^+(\mathbb{R})$ (groupe des déplacements de $\mathbb{R}^n$ euclidien) est un sous-groupe distingué du groupe $\mathcal{O}_n(\mathbb{R})$ des isométries de $\mathbb{R}^n$.*

Exemple 1.5 *Le groupe alterné $\mathcal{A}_n$ est distingué dans le groupe symétrique $\mathcal{S}_n$ comme noyau de la signature.*

Exercice 1.10 *Montrer que le centre d'un groupe G est distingué.*

Solution 1.10 *Le centre $Z(G)$ est le noyau du morphisme de groupes $g \mapsto \Phi_g : h \mapsto ghg^{-1}$ de G dans $\mathrm{Aut}(G)$, c'est donc un sous-groupe distingué de G.*

Exercice 1.11 *Soient G, G' deux groupes et φ un morphisme de groupes de G dans G'.*

1. *Montrer que si H est un sous-groupe distingué de G et φ est surjectif, alors $\varphi(H)$ est un sous-groupe distingué de G'.*
2. *Montrer que si H' est un sous-groupe distingué de G', alors $\varphi^{-1}(H')$ est un sous-groupe distingué de G.*

Solution 1.11 *On sait déjà que $\varphi(H)$ est un sous-groupe de G' (que φ soit surjectif ou non) et que $\varphi^{-1}(H')$ est un sous-groupe de G.*

1. *Si φ est surjectif, tout $g' \in G'$ s'écrit $g' = \varphi(g)$ avec $g \in G$ et pour tout $h' = \varphi(h) \in \varphi(H)$ (avec $h \in H$), on a :*

$$\begin{aligned} g'h'(g')^{-1} &= \varphi(g)\varphi(h)(\varphi(g))^{-1} = \varphi(g)\varphi(h)\varphi\left(g^{-1}\right) \\ &= \varphi\left(ghg^{-1}\right) \in \varphi(H) \end{aligned}$$

   ce qui signifie que $\varphi(H)$ est distingué dans G'.
2. *Pour $g \in G$ et $h \in \varphi^{-1}(H')$, on a :*

$$\varphi\left(ghg^{-1}\right) = \varphi(g)\varphi(h)(\varphi(g))^{-1} \in \varphi(g)H'(\varphi(g))^{-1} = H'$$

   et $ghg^{-1} \in \varphi^{-1}(H')$. Donc $\varphi^{-1}(H')$ est distingué dans G.

Exercice 1.12 *Soient $(G, \cdot)$ un groupe fini d'ordre $n \geq 2$ et H un sous-groupe de G d'indice 2. Montrer que H distingué.*

Solution 1.12 *Si H est d'indice 2, on a alors $G/H = \{H, g_1H\}$ avec $g_1 \notin H$ et la partition $G = H \cup g_1H$. Il s'agit alors de montrer que pour tous $g \in G$ et $h \in H$, on a forcément $ghg^{-1} \in H$. Si $g \in H$ c'est clair, sinon $g = g_1k$ avec $k \in H$ et $ghg^{-1} = g_1khk^{-1}g_1^{-1} = g_1\ell g_1^{-1}$ avec $\ell \in H$ et $g_1\ell g_1^{-1} \in g_1H$ donne $g_1\ell g_1^{-1} = g_1m$ avec $m \in H$, ce qui entraîne $g_1 = \ell m^{-1} \in H$ qui est faux, on a donc $ghg^{-1} = g_1\ell g_1^{-1} \in H$ et H est distingué dans G.*

Théorème 1.9 *Un sous-groupe H de G est distingué si, et seulement si, il existe une unique structure de groupe sur l'ensemble quotient G/H des classes à gauche modulo H telle que la surjection canonique $\pi : G \to G/H$ soit un morphisme de groupes.*

Démonstration. Si G/H est muni d'une structure de groupe telle que π soit un morphisme de groupes, on a alors nécessairement pour tous g, g' dans G :

$$\overline{g}\overline{g'} = \pi(g)\,\pi(g') = \pi(gg') = \overline{gg'}$$

Pour (g, h) dans $G \times H$, on a alors $\overline{g^{-1}hg} = \overline{g^{-1}}\overline{h}\overline{g} = \overline{g^{-1}}\overline{g} = \overline{g^{-1}g} = \overline{1} = H$, ce qui signifie que $g^{-1}hg \in H$ (on rappelle que $\overline{g} = gH = \overline{1} = H$ si, et seulement si, $g \in H$).

Supposons H distingué. L'analyse que l'on vient de faire nous montre que la seule loi possible sur G/H est définie par $\overline{g}\overline{g'} = \overline{gg'}$. Pour montrer qu'une telle définition est permise, il s'agit de montrer qu'elle ne dépend pas des choix des représentants de $\overline{g}$ et $\overline{g'}$, ce qui résulte du fait que $\mathcal{R}_g$ est compatible avec la loi de G. En effet, si $g\mathcal{R}_g g_1$ et $g'\mathcal{R}_g g_1'$, on a alors $gg'\mathcal{R}_g g_1 g'$ et $g_1 g'\mathcal{R}_g g_1 g_1'$, donc $gg'\mathcal{R}_g g_1 g_1'$ et $\overline{gg'} = \overline{g_1 g_1'}$.

Il reste à vérifier que G/H muni de cette loi de composition interne est bien un groupe.

Avec :

$$\begin{aligned}\overline{g_1}\,(\overline{g_2}\ \overline{g_3}) &= \overline{g_1 g_2 g_3} = \overline{g_1\,(g_2 g_3)} = \overline{(g_1 g_2)\,g_3} \\ &= \overline{g_1 g_2 g_3} = (\overline{g_1}\ \overline{g_2})\,\overline{g_3}\end{aligned}$$

on déduit que cette loi est associative.

Avec $\overline{g}\overline{1} = \overline{g \cdot 1} = \overline{g}$, on déduit que $\overline{1}$ est le neutre.

Avec $\overline{g}\overline{g^{-1}} = \overline{g \cdot g^{-1}} = \overline{1}$, on déduit que tout élément de G/H est inversible avec $(\overline{g})^{-1} = \overline{g^{-1}}$.

Par définition de cette loi de composition interne, l'application π est surjective. ∎

Remarque 1.7 *Pour H distingué dans G, le noyau de la surjection canonique est :*

$$\ker(\pi) = \left\{g \in G \mid \overline{g} = \overline{1}\right\} = \overline{1} = H$$

Comme on a vu que le noyau d'un morphisme de groupes est distingué, on déduit qu'un sous-groupe distingué de G est le noyau d'un morphisme de groupes.

Remarque 1.8 *Dans le cas où G est commutatif, pour tout sous-groupe H de G, G/H est un groupe puisque tous les sous-groupes de G sont distingués. On le note alors $\dfrac{G}{H}$ (il est aussi égal à $G\backslash H$).*

Exemple 1.6 *Si G est le groupe additif $\mathbb{Z}$, on sait alors que ces sous-groupes sont les $n\mathbb{Z}$ où n est un entier naturel et comme $(\mathbb{Z}, +)$ est commutatif, l'ensemble quotient $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est naturellement muni d'une structure de groupe.*

D'autre part, le théorème de division euclidienne nous permet d'écrire tout entier relatif k sous la forme $k = qn + r$ avec $0 \leq r \leq n-1$, ce qui entraîne $k - r \in n\mathbb{Z}$ et $\overline{k} = \overline{r}$. Et comme $\overline{r} \neq \overline{s}$ pour $0 \leq r \neq s \leq n-1$ (on a $0 < |r - s| < n$ et $r - s$ ne peut être multiple de n), on en déduit que :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}$$

a n éléments. Ce groupe est cyclique d'ordre n engendré par $\overline{1}$.

Exemple 1.7 *Dans le groupe additif* $(\mathbb{R},+)$, *on considère le sous groupe* $2\pi\mathbb{Z}$. *Le groupe quotient* $\mathbb{R}/2\pi\mathbb{Z}$ *est l'ensemble des classes d'équivalence relatif à la relation :*

$$(x\sim y)\Leftrightarrow(\exists k\in\mathbb{Z}\mid x-y=2k\pi)$$

et on vérifie facilement que l'application :

$$\begin{array}{ccc}\mathbb{R}/2\pi\mathbb{Z} & \to & \Gamma=\{z\in\mathbb{C}\mid |z|=1\}\\ \overline{x} & \mapsto & e^{ix}\end{array}$$

est un isomorphisme de groupes.

Exemple 1.8 *Dans le groupe multiplicatif* $(\mathbb{C}^*,\cdot)$, *on considère le sous groupe* $\mathbb{R}^{+,*}$. *Le groupe quotient* $\mathbb{C}^*/\mathbb{R}^{+,*}$ *est l'ensemble des classes d'équivalence relatif à la relation :*

$$(z\sim z')\Leftrightarrow\left(\exists\lambda\in\mathbb{R}^{+,*}\mid\frac{z'}{z}=\lambda\right)$$

et on vérifie facilement que l'application :

$$\begin{array}{ccc}\mathbb{C}^*/\mathbb{R}^{+,*} & \to & \Gamma=\{z\in\mathbb{C}\mid |z|=1\}\\ \overline{z}=\overline{\rho e^{i\theta}} & \mapsto & \dfrac{z}{|z|}=e^{i\theta}\end{array}$$

est un isomorphisme de groupes.

Théorème 1.10 *Si* G,G' *sont deux groupes et* $\varphi:G\to G'$ *un morphisme de groupes, il existe alors un unique isomorphisme de groupes* $\overline{\varphi}:G/\ker(\varphi)\to\mathrm{Im}(\varphi)$ *tel que* $\varphi=i\circ\overline{\varphi}\circ\pi$, *où* $i:\mathrm{Im}(\varphi)\to G'$ *est l'injection canonique (définie par* $i(h')=h'$ *pour tout* $h'\in\mathrm{Im}(\varphi)$*) et* $\pi:G\to G/\ker(\varphi)$ *la surjection canonique (définie par* $\pi(g)=\overline{g}=g\ker(\varphi)$ *pour tout* $g\in G$*).*

Démonstration. Comme $\ker(\varphi)$ est distingué dans G, $G/\ker(\varphi)$ est un groupe.

Si un tel isomorphisme $\overline{\varphi}$ existe, on a alors, pour tout $g\in G$:

$$\varphi(g)=i\circ\overline{\varphi}\circ\pi(g)=i\circ\overline{\varphi}(\overline{g})=\overline{\varphi}(\overline{g})$$

ce qui prouve l'unicité de $\overline{\varphi}$.

Vu l'analyse du problème, on montre d'abord que l'on peut définir $\overline{\varphi}$ par $\overline{\varphi}(\overline{g})=\varphi(g)$ pour tout $\overline{g}\in G/\ker(\varphi)$. Pour justifier cette définition, on doit vérifier qu'elle ne dépend pas des choix du choix d'un représentant de $\overline{g}$. Si $\overline{g}=\overline{h}$, on a alors $g^{-1}h\in\ker(\varphi)$, donc $(\varphi(g))^{-1}\varphi(h)=\varphi(g^{-1}h)=1$ et $\varphi(g)=\varphi(h)$. L'application $\overline{\varphi}$ est donc bien définie et par construction, on a $\varphi=i\circ\overline{\varphi}\circ\pi$.

Avec :

$$\overline{\varphi}\left(\overline{g}\overline{h}\right)=\overline{\varphi}\left(\overline{gh}\right)=\varphi(gh)=\varphi(g)\varphi(h)=\overline{\varphi}(\overline{g})\overline{\varphi}\left(\overline{h}\right)$$

on voit que c'est un morphisme de groupes.

L'égalité $\overline{\varphi}(\overline{g})=1$ équivaut à $\varphi(g)=1$, soit à $g\in\ker(\varphi)$ ou encore à $\overline{g}=\overline{1}$. Ce morphisme est donc surjectif et à valeurs dans $\mathrm{Im}(\varphi)=\mathrm{Im}(\overline{\varphi})$, il est surjectif. ∎

Le théorème précédent s'exprime aussi en disant qu'on a le diagramme commutatif :

$$\begin{array}{ccc}G & \overset{\varphi}{\to} & G'\\ \pi\downarrow & & \uparrow i\\ G/\ker(\varphi) & \overset{\overline{\varphi}}{\underset{\sim}{\to}} & \mathrm{Im}(\varphi)\end{array}$$

Corollaire 1.2 *Soient G, G' deux groupes et $\varphi : G \to G'$ un morphisme de groupes. Si G est fini, on a alors :*

$$\operatorname{card}(G) = \operatorname{card}(\ker(\varphi)) \operatorname{card}(\operatorname{Im}(\varphi))$$

Démonstration. Comme $G/\ker(\varphi)$ et $\operatorname{Im}(\varphi)$ sont isomorphes, dans le cas où G est fini, on a :

$$\operatorname{card}(\operatorname{Im}(\varphi)) = \operatorname{card}(G/\ker(\varphi)) = \frac{\operatorname{card}(G)}{\operatorname{card}(\ker(\varphi))}.$$

■

Exercice 1.13 *Soient G, H deux groupes, $\varphi : G \to H$ un morphisme de groupes, G' un sous-groupe distingué de G et H' un sous-groupe distingué de H tel que $\varphi(G') \subset H'$. Montrer qu'il existe un unique morphisme de groupes $\overline{\varphi} : G/G' \to H/H'$ tel que $\pi_H \circ \varphi = \overline{\varphi} \circ \pi_G$, où $\pi_G : G \to G/G'$ et $\pi_H : H \to H/H'$ sont les surjections canoniques.*

Solution 1.13 *En supposant que $\overline{\varphi}$ existe, on a nécessairement $\pi_H \circ \varphi(g) = \overline{\varphi} \circ \pi_G(g)$ pour tout $g \in G$, ce qui assure l'unicité de $\overline{\varphi}$.*
On définit donc $\overline{\varphi}$ par :

$$\forall \overline{g} \in G/G',\ \overline{\varphi}(\overline{g}) = \widetilde{\varphi(g)}$$

en notant $\overline{g} = gG'$ la classe de $g \in G$ modulo G' et $\widetilde{h}$ la classe de $h \in H$ modulo H'. Pour justifier cette définition, on doit vérifier qu'elle ne dépend pas des choix du choix d'un représentant de $\overline{g}$. Si $\overline{g_1} = \overline{g_2}$, on a alors $g_2 g_1^{-1} \in G'$, donc $\varphi(g_2)(\varphi(g_1))^{-1} = \varphi\left(g_2 g_1^{-1}\right) \in \varphi(G') \subset H'$ et $\widetilde{\varphi(g_1)} = \widetilde{\varphi(g_2)}$. L'application $\overline{\varphi}$ est donc bien définie et par construction, on a $\pi_H \circ \varphi = \overline{\varphi} \circ \pi_G$. Avec :

$$\begin{aligned}\overline{\varphi}(\overline{g_1}\ \overline{g_2}) &= \overline{\varphi}(\overline{g_1 g_2}) = \widetilde{\varphi(g_1 g_2)} = \widetilde{\varphi(g_1)\varphi(g_2)} \\ &= \widetilde{\varphi(g_1)}\widetilde{\varphi(g_2)} = \overline{\varphi}(\overline{g_1})\,\overline{\varphi}(\overline{g_2})\end{aligned}$$

on voit que c'est un morphisme de groupes.

Exercice 1.14 *Soit E un espace euclidien de dimension $n \geq 2$. Montrer que $\mathcal{O}^+(E)$ est un sous-groupe distingué de $\mathcal{O}(E)$ d'indice 2.*

Solution 1.14 *$\mathcal{O}^+(E)$ est un sous-groupe distingué de $\mathcal{O}(E)$ comme noyau du morphisme de groupes $\det : \mathcal{O}(E) \to \{-1, 1\}$. Comme cette application est surjective ($Id \in \mathcal{O}^+(E)$ et en désignant par $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base orthonormée de E, l'application u définie par $u(e_1) = -e_1$ et $u(e_i) = e_i$ pour i compris entre 2 et n est dans $\mathcal{O}^-(E)$), $\mathcal{O}(E)/\mathcal{O}^+(E)$ est isomorphe à $\{-1, 1\}$ et $[\mathcal{O}(E) : \mathcal{O}^+(E)] = 2$.*

Remarque 1.9 *Pour H sous-groupe de G, la compatibilité de $\mathcal{R}_g$ avec la loi de G est une condition nécessaire et suffisante pour définir naturellement une structure de groupe sur l'ensemble quotient G/H par :*

$$\overline{g}\ \overline{g'} = \overline{gg'}$$

Précisément, on a le résultat suivant, où $G/\mathcal{R}$ est l'ensemble des classes d'équivalence modulo une relation d'équivalence $\mathcal{R}$ et $\pi : g \mapsto \overline{g} = \{h \in G \mid g\mathcal{R}h\}$ est la surjection canonique de G sur $G/\mathcal{R}$.

Théorème 1.11 *Soit $\mathcal{R}$ une relation d'équivalence sur G. Cette relation est compatible avec la loi de G si, et seulement si, il existe une unique structure de groupe sur l'ensemble quotient $G/\mathcal{R}$ telle que la surjection canonique $\pi : G \to G/\mathcal{R}$ soit un morphisme de groupes.*

Démonstration. Si $G/\mathcal{R}$ est muni d'une structure de groupe telle que π soit un morphisme de groupe, on a alors nécessairement pour tous g, g' dans G :

$$\overline{g}\overline{g'} = \pi(g)\,\pi(g') = \pi(gg') = \overline{gg'}$$

On en déduit que pour g, g', h, h' dans G tels que $g\mathcal{R}h$ et $g'\mathcal{R}h'$, on a :

$$\overline{gg'} = \overline{g}\ \overline{g'} = \overline{h}\ \overline{h'} = \overline{hh'}$$

ce qui signifie que $gg'\mathcal{R}hh'$. La relation $\mathcal{R}$ est donc compatible avec la loi de G.

Réciproquement, supposons que $\mathcal{R}$ soit compatible avec la loi de G. L'analyse que l'on vient de faire nous montre que la seul loi possible sur $G/\mathcal{R}$ est définie par $\overline{g}\overline{g'} = \overline{gg'}$. Pour montrer qu'une telle définition est permise, il s'agit de montrer qu'elle ne dépend pas des choix des représentants de $\overline{g}$ et $\overline{g'}$. Si $\overline{g} = \overline{h}$ et $\overline{g'} = \overline{h'}$, on a alors $g\mathcal{R}h$ et $g'\mathcal{R}h'$, ce qui entraîne $gg'\mathcal{R}hh'$, soit $\overline{gg'} = \overline{hh'}$. ■

Exercice 1.15 *Soit $\mathcal{R}$ une relation d'équivalence sur G compatible avec la loi de G. Montrer que :*

1. *pour tous g, h dans G, on a $g\overline{h} = \overline{gh}$ et $\overline{h}g = \overline{hg}$;*
2. *$H = \overline{1}$ est un sous-groupe distingué de G ;*
3. *pour tout $g \in G$, $\overline{g} = gH = Hg$ et $G/\mathcal{R} = G/H$.*

Solution 1.15

1. *On a :*

   $$\left(k \in g\overline{h}\right) \Leftrightarrow (\exists h' \in G \mid h'\mathcal{R}h \text{ et } k = gh') \Rightarrow (k = gh'\mathcal{R}gh) \Rightarrow \left(k \in \overline{gh}\right)$$

   donc $g\overline{h} \subset \overline{gh}$. Et réciproquement :

   $$\left(k \in \overline{gh}\right) \Leftrightarrow (k\mathcal{R}gh) \Rightarrow \left(g^{-1}k\mathcal{R}h\right) \Rightarrow \left(g^{-1}k \in \overline{h}\right) \Rightarrow \left(k \in g\overline{h}\right)$$

   soit $\overline{gh} \subset g\overline{h}$ et $g\overline{h} = \overline{gh}$.
   On procède de manière analogue pour l'égalité $\overline{h}g = \overline{hg}$
2. *On a $1 \in H = \overline{1}$, si g, h sont dans H, on a $g\mathcal{R}1$ et $h\mathcal{R}1$, donc $gh\mathcal{R}1$ et pour $g \in H$, $1\mathcal{R}g$ et $g^{-1}\mathcal{R}g^{-1}$ entraîne $g^{-1}\mathcal{R}1$, soit $g^{-1} \in H$. Donc H est bien un sous-groupe de G.*
   Pour $g \in G$, on a $gH = g\overline{1} = \overline{g}$ et $Hg = \overline{1}g = \overline{g} = gH$, ce qui signifie que H est distingué dans G.
3. *On a aussi montré en **2.** que $G/\mathcal{R} = G/H$.*

L'exercice précédent nous dit en fait que les relations d'équivalence sur un groupe compatibles avec sa loi sont celles suivant un groupe distingué (à gauche ou à droite).

1.4 Ordre d'un élément dans un groupe

On se donne un groupe multiplicatif $(G, \cdot)$.

Définition 1.9 *L'ordre d'un élément g de G est l'élément $\theta(g) \in \mathbb{N}^* \cup \{+\infty\}$ défini par :*

$$\theta(g) = \operatorname{card}(\langle g \rangle).$$

Si $\theta(g)$ est dans $\mathbb{N}^*$, on dit alors que g est d'ordre fini, sinon on dit qu'il est d'ordre infini.

Remarque 1.10 *Seul l'élément neutre 1_G est d'ordre 1 dans G. En effet, si $g = 1$, alors $\langle g\rangle = \{1\}$ et si $g \neq 1$, alors $g^0 \neq g^1$ et $\langle g\rangle$ a au moins deux éléments.*

Remarque 1.11 *Pour tout $g \in G$, on a $\theta(g) = \theta(g^{-1})$ puisque :*

$$\begin{aligned}\left\langle g^{-1}\right\rangle &= \left\{\left(g^{-1}\right)^n \mid n \in \mathbb{Z}\right\} = \left\{g^{-n} \mid n \in \mathbb{Z}\right\}\\ &= \left\{g^n \mid n \in \mathbb{Z}\right\} = \langle g\rangle\end{aligned}$$

Remarque 1.12 *Dans le cas, où le groupe G est fini d'ordre $n \geq 1$, le théorème de Lagrange nous dit que l'ordre de tout élément de G divise l'ordre de G et en conséquence, on a $g^n = 1$ pour tout $g \in G$.*

Exercice 1.16 *Déterminer l'ordre d'un élément du groupe multiplicatif $\mathbb{C}^*$.*

Solution 1.16 *Tout nombre complexe non nul s'écrit $z = \rho e^{i\alpha}$ où $\rho \in \mathbb{R}^{+,*}$ et $\alpha \in [0, 2\pi[$ (avec un tel choix de α cette écriture est unique et on dit que α est la détermination principale de l'argument).*
Si $\rho \neq 1$, on a $\left|z^k\right| = \rho^k \neq 1$ pour tout entier relatif non nul k, donc $z^k \neq z^j$ pour $k \neq j$ dans $\mathbb{Z}$ et $\langle z\rangle$ est infini.
Si $\rho = 1$, on a alors, pour k entier relatif non nul, $z^k = e^{ik\alpha} = 1$ si, et seulement si, il existe un entier relatif q tel que $k\alpha = 2q\pi$, ce qui signifie que $\dfrac{\alpha}{2\pi}$ est rationnel. On en déduit donc que :

- *pour $\dfrac{\alpha}{2\pi}$ irrationnel, $z^k \neq 1$ pour tout entier relatif non nul k et $\langle z\rangle$ est infini ;*
- *pour $\dfrac{\alpha}{2\pi} = \dfrac{p}{q}$ rationnel avec $(p, q) \in \mathbb{Z}\times\mathbb{N}^*$ et $p\wedge q = 1$, en effectuant la division euclidienne d'un entier relatif k par q, on a $k = mq + r$ avec $0 \leq r \leq q - 1$ et :*

$$z^k = e^{ik\alpha} = \left(e^{iq\alpha}\right)^m e^{ir\alpha} = \left(e^{2ip\pi}\right)^m e^{ir\alpha} = e^{ir\alpha}$$

et $\langle z\rangle = \{e^{ir\alpha} \mid 0 \leq r \leq q - 1\}$ a au plus q éléments.
Pour $0 \leq r \neq s \leq q - 1$ l'égalité $e^{ir\alpha} = e^{is\alpha}$ équivaut à $e^{i(s-r)\alpha} = 1$, ce qui revient à dire $(s - r)\alpha = 2m\pi$ avec $m \in \mathbb{Z}$, qui tenant compte de $\alpha = 2\pi\dfrac{p}{q}$, donne $(s - r)\dfrac{p}{q} = m$, soit q divise $p(s - r)$ sachant que q est premier avec p, donc q divise $r - s$ (théorème de Gauss) et nécessairement $r = s$ puisque $|r - s| \leq q - 1$. On a donc exactement q éléments dans $\langle z\rangle$ et z est d'ordre q.
En fait $\langle z\rangle$ est le groupe Γ_q des racines q-èmes de l'unité.
En définitive :

$$\theta\left(\rho e^{i\alpha}\right) = \begin{cases} +\infty \text{ si } \rho \neq 1 \text{ ou } \rho = 1 \text{ et } \dfrac{\alpha}{2\pi} \text{ irrationnel}\\ q \text{ si } \dfrac{\alpha}{2\pi} = \dfrac{p}{q} \in \mathbb{Q} \text{ avec } p \wedge q = 1\end{cases}$$

Théorème 1.12 *Si $\varphi : G \to G'$ est un isomorphisme de groupes, on a alors $\theta(\varphi(g)) = \theta(g)$ pour tout $g \in G$.*

Démonstration. Pour $g \in G$, on a :

$$\langle\varphi(g)\rangle = \{(\varphi(g))^n \mid n \in \mathbb{Z}\} = \{\varphi(g^n) \mid n \in \mathbb{Z}\} = \varphi(\langle g\rangle)$$

avec φ bijective, donc $\operatorname{card}(\langle\varphi(g)\rangle) = \operatorname{card}(\langle g\rangle)$. ∎

Exercice 1.17 *Montrer que pour g, h dans G, on a $\theta(gh) = \theta(hg)$.*

Solution 1.17 *L'application $\varphi : k \mapsto g^{-1}kg$ est isomorphisme de G sur lui même, donc $\theta(gh) = \theta(\varphi(gh)) = \theta(hg)$.*

Exercice 1.18 *Déterminer l'ordre d'une matrice de rotation [resp. de réflexion] dans $GL_2(\mathbb{R})$. En déduire qu'on peut trouver deux éléments d'ordre fini dans $GL_2(\mathbb{R})$ dont le produit est d'ordre infini.*

Solution 1.18 *L'application :*

$$R_\alpha = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \in \mathcal{O}_2^+(\mathbb{R}) \mapsto e^{i\alpha}$$

est un isomorphisme de groupes de $\mathcal{O}_2^+(\mathbb{R})$ sur le groupe Γ des nombres complexes de module égale à 1. En utilisant l'exercice 1.16, on en déduit que :

$$\theta(R_\alpha) = \begin{cases} +\infty \text{ si } \dfrac{\alpha}{2\pi} \text{ est irrationnel} \\ q \text{ si } \dfrac{\alpha}{2\pi} = \dfrac{p}{q} \in \mathbb{Q} \text{ avec } p \wedge q = 1 \end{cases}$$

Si $S_\alpha = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{pmatrix}$ est une matrice de réflexion, on a $S_\alpha^2 = R_{\alpha-\alpha} = I_n$ et $S_\alpha \neq I_n$, donc S_α est d'ordre 2.
La composée de deux matrices de réflexions $S_\alpha \circ S_{\alpha'} = R_{\alpha-\alpha'}$ est d'ordre infini si $\dfrac{\alpha - \alpha'}{2\pi} \notin \mathbb{Q}$.

Pour $g \in G$, le sous-groupe de G engendré par g peut être vu comme l'image du morphisme de groupes :

$$\begin{array}{rccc} \varphi_g : & \mathbb{Z} & \to & G \\ & k & \mapsto & g^k \end{array}$$

(pour j, k dans $\mathbb{Z}$, on a $\varphi_g(j+k) = g^{j+k} = g^j g^k = \varphi_g(j)\varphi_g(k)$ et φ_g est bien un morphisme de groupes).

Connaissant les sous-groupes additifs de $\mathbb{Z}$, on a le résultat suivant.

Théorème 1.13 *Pour $g \in G$, on a $\theta(g) = +\infty$ si, et seulement si, φ_g est un isomorphisme et pour g d'ordre fini, on a $\ker(\varphi_g) = \theta(g)\mathbb{Z}$.*

Démonstration. Le noyau de φ_g étant un sous-groupe de $\mathbb{Z}$, il existe un unique entier $n \geq 0$ tel que $\ker(\varphi_g) = n\mathbb{Z}$.

On aura $n = 0$ si, et seulement si, φ_g est injective, ce qui revient à dire que $\varphi_g(k) = a^k \neq 1$ pour tout $k \in \mathbb{Z}^*$ ou encore que $\varphi_g(k) = g^k \neq \varphi_g(j) = g^j$ pour tous $j \neq k$ dans $\mathbb{Z}$ et le sous-groupe $\langle g \rangle = \mathrm{Im}(\varphi_g)$ est infini.

Si $n \geq 1$, en effectuant, pour $k \in \mathbb{Z}$, la division euclidienne de k par n, on a $k = qn + r$ avec $0 \leq r \leq n-1$ et $g^k = (g^n)^q g^r = g^r$, ce qui nous donne :

$$\langle g \rangle = \mathrm{Im}(\varphi_g) = \{g^r \mid 0 \leq r \leq n-1\}$$

De plus pour $1 \leq r \leq n-1$, on a $g^r \neq 1$ puisque $n = \inf(\ker(\varphi_g) \cap \mathbb{N}^*)$, ce qui entraîne $g^r \neq g^s$ pour $0 \leq r \neq s \leq n-1$ (pour $s \geq r$, l'égalité $g^r = g^s$ équivaut à $g^{s-r} = 1$ avec $s - r$ compris entre 0 et $n-1$, ce qui équivaut à $r = s$). Le groupe $\langle g \rangle$ a donc exactement n éléments. ∎

Le théorème précédent nous permet de donner d'autres définitions de l'ordre d'un élément d'un groupe.

Corollaire 1.3 *Dire que $g \in G$ est d'ordre fini $n \geq 1$ équivaut à dire que $g^n = 1$ et $g^k \neq 1$ pour tout k est compris entre 1 et $n-1$ ($\theta(g)$ est le plus petit entier naturel non nul tel que $g^n = 1$).*

Démonstration. Si g est d'ordre $n \geq 1$, on a vu avec la démonstration du théorème précédent que $g^n = 1$ et $g^k \neq 1$ pour tout k est compris entre 1 et $n-1$.

Réciproquement s'il existe un entier $n \geq 1$ tel que $g^n = 1$ et $g^k \neq 1$ pour k est compris entre 1 et $n-1$, le morphisme de groupes φ_g est non injectif, donc g est d'ordre fini et $\ker(\varphi_g) = \theta(g)\,\mathbb{Z}$ avec $\theta(g) = \inf(\ker(\varphi_g) \cap \mathbb{N}^*) = n$. ∎

Corollaire 1.4 *Dire que $g \in G$ est d'ordre fini $n \geq 1$ équivaut à dire que, pour $k \in \mathbb{Z}$, on a $g^k = 1$ si, et seulement si, k est multiple de n.*

Démonstration. Si g est d'ordre n, on a alors $g^n = 1$ et pour $k = qn + r \in \mathbb{Z}$ avec $q \in \mathbb{Z}$ et $0 \leq r \leq n-1$ (division euclidienne), on a $g^k = g^r = 1$ si, et seulement si $r = 0$.

Réciproquement supposons que $g^k = 1$ si, et seulement si, k est multiple de n. On a alors $g^n = 1$ et $g^k \neq 1$ si k est compris entre 1 et $n-1$, ce qui signifie que g est d'ordre n. ∎

En résumé, on retiendra que :

- $(\theta(g) = +\infty) \Leftrightarrow (\varphi_g \text{ injective}) \Leftrightarrow (\ker(\varphi_g) = \{0\}) \Leftrightarrow$
  $\left(\forall k \in \mathbb{Z}^*,\ g^k \neq 1\right) \Leftrightarrow (\langle g \rangle \text{ est infini isomorphe à } \mathbb{Z})$;
- $(\theta(g) = n \in \mathbb{N}^*) \Leftrightarrow (\ker(\varphi_g) = n\mathbb{Z}) \Leftrightarrow (\langle g \rangle = \{g^r \mid 0 \leq r \leq n-1\})$
  $\Leftrightarrow \left(k \in \mathbb{Z} \text{ et } g^k = 1 \text{ équivaut à } k \equiv 0 \mod(n)\right) \Leftrightarrow$
  (n est le plus petit entier naturel non nul tel que $g^n = 1$).

Pour g d'ordre fini, le groupe $\langle g \rangle$ est dit cyclique, ce qui est justifié par $g^{qn+r} = g^r$ pour $q \in \mathbb{Z}$ et $0 \leq r \leq n-1$.

Théorème 1.14 *Si G est un groupe cyclique d'ordre n, il est alors isomorphe au groupe $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.*

Démonstration. Si $G = \langle g \rangle$ est cyclique d'ordre n, alors l'application $\varphi_g : k \mapsto g^k$ est un morphisme de groupes surjectif de $(\mathbb{Z}, +)$ sur G de noyau $\ker(\varphi_g) = n\mathbb{Z}$ et le théorème d'isomorphisme nous dit $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est isomorphe à G. ∎

Exemple 1.9 *Le groupe multiplicatif Γ_n des racines n-èmes de l'unité, qui est cyclique d'ordre n, est isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ par l'application $\overline{k} \mapsto e^{\frac{2ik\pi}{n}}$.*

Dans le cas où le groupe G est additif, l'ordre de $g \in G$ est défini comme le plus petit entier $n \geq 1$ tel que $ng = 0$, quand cet ordre est fini. L'égalité $mg = 0$ équivaut alors à dire que m est multiple de n. Le groupe engendré par g est alors :

$$\langle g \rangle = \{kg \mid k \in \mathbb{Z}\} = \{rg \mid 0 \leq r \leq n-1\}.$$

Exercice 1.19 *Montrer que, pour tout entier $n \geq 1$, il existe un unique sous-groupe de $(\mathbb{C}^*, \cdot)$ d'ordre n.*

Solution 1.19 *Si G est sous groupe d'ordre $n \geq 1$ de $(\mathbb{C}^*, \cdot)$, on a alors $z^n = 1$ pour tout $z \in G$, donc G est contenu dans le groupe Γ_n des racines n-èmes de l'unité et $G = \Gamma_n$ puisque ces ensembles sont de même cardinal.*

Exercice 1.20 *Déterminer les sous-groupes finis du groupe multiplicatif $\mathbb{R}^*$.*

Solution 1.20 *Si $G \subset \mathbb{R}^*$ est un groupe d'ordre $n \geq 1$, on a alors $x^n = 1$ pour $x \in G$ et G est contenu dans l'ensemble :*

$$\Delta_n = \{x \in \mathbb{R} \mid x^n = 1\} = \begin{cases} \{-1, 1\} & \text{si } n \text{ est pair} \\ \{1\} & \text{si } n \text{ est impair} \end{cases}$$

On a donc nécessairement $n = 1$ et $G = \{1\}$ ou $n = 2$ et $G = \{-1, 1\}$.

Dans le cas général, on peut montrer que les sous-groupes finis d'un corps commutatif sont cycliques.

Exercice 1.21 *Montrer que tout sous-groupe d'ordre $n \geq 1$ du groupe $O_2^+(\mathbb{R})$ des matrices de rotations du plan vectoriel euclidien $\mathbb{R}^2$ est cyclique engendré par $R\left(\frac{2\pi}{n}\right)$ (rotation d'angle $\frac{2\pi}{n}$).*

Solution 1.21 *Le groupe $O_2^+(\mathbb{R})$ est isomorphe au groupe multiplicatif Γ des nombres complexes de module égal à 1, un isomorphisme étant défini par l'application :*

$$R(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \mapsto e^{i\theta}.$$

Un sous-groupe fini de $O_2^+(\mathbb{R})$ est donc identifié à un sous-groupe fini de Γ, donc de $\mathbb{C}^*$, et en conséquence il est cyclique engendré par $R\left(\frac{2\pi}{n}\right)$.

Exercice 1.22 *Montrer que, pour tout entier $n \geq 1$, il existe un unique sous-groupe de $(\mathbb{Q}/\mathbb{Z}, +)$ d'ordre n.*

Solution 1.22 *Supposons que G soit un sous-groupe de $(\mathbb{Q}/\mathbb{Z}, +)$ d'ordre n. Tout $\overline{r} \in G$ a un ordre qui divise n, donc $n\overline{r} = \overline{0}$, c'est-à-dire qu'il existe $q \in \mathbb{Z}$ tel que $nr = q$ et $r = \frac{q}{n}$. On a donc $\overline{r} = \overline{\frac{q}{n}} = q\overline{\frac{1}{n}} \in \left\langle \overline{\frac{1}{n}} \right\rangle$ et $G \subset \left\langle \overline{\frac{1}{n}} \right\rangle$. Comme $\overline{\frac{1}{n}}$ est d'ordre n dans $\mathbb{Q}/\mathbb{Z}$ (on a $k\overline{\frac{1}{n}} = \overline{\frac{k}{n}} = \overline{0}$ si, et seulement si, $\frac{k}{n} \in \mathbb{Z}$, ce qui équivaut à dire que k est multiple de n), on a nécessairement $G = \left\langle \overline{\frac{1}{n}} \right\rangle$. D'où l'unicité d'un groupe d'ordre n et ce groupe existe (c'est $\left\langle \overline{\frac{1}{n}} \right\rangle$).*

Exercice 1.23 *Soient $(G, \cdot)$ un groupe fini d'ordre $n \geq 2$ et H un sous-groupe distingué de G. Comparer l'ordre de $\overline{g}$ dans G/H avec l'ordre de g dans G.*

Solution 1.23 *Soit $g \in G$ d'ordre p et q l'ordre de $\overline{g}$ dans le groupe quotient G/H (H est distingué dans G). Avec $\overline{g}^p = \overline{g^p} = \overline{1}$, on déduit que $q = \theta(\overline{g})$ divise $p = \theta(g)$.*
Pour $G = \{1, -1, i, -i\} \subset \mathbb{C}^*$, $H = \{1, -1\}$, $g = i$ est d'ordre 4 et $\overline{g} = gH = \{i, -i\}$ est d'ordre 2 ($\overline{g} \neq \overline{1} = H$ et $\overline{g}^2 = \overline{i^2} = \overline{-1} = H = \overline{1}$).

Exercice 1.24 *Montrer qu'un groupe G est fini si et seulement si l'ensemble de ses sous-groupes est fini. En conséquence, un groupe infini a une infinité de sous-groupes.*

Solution 1.24 *Si G est un groupe fini alors l'ensemble $\mathcal{P}(G)$ des parties de G est fini (de cardinal $2^{\mathrm{card}(G)}$) et il en est de même de l'ensemble des sous-groupes de G.*
Réciproquement soit $(G,\cdot)$ un groupe tel que l'ensemble de ses sous-groupes soit fini. On peut écrire $G=\bigcup_{g\in G}\langle g\rangle$ et cette réunion est finie, soit $G=\bigcup_{k=1}^{r}\langle g_k\rangle$. Si l'un de ces sous-groupes $\langle g_k\rangle$ est infini, alors les $\langle g_k^n\rangle$ où n décrit $\mathbb{N}$ forment une famille infinie de sous-groupes de G : en effet l'égalité $\langle g_k^n\rangle=\langle g_k^m\rangle$ entraîne $g_k^n=g_k^{jm}$, soit $g_k^{n-jm}=1$ et $n-jm=0$ (g_k est d'ordre infini), c'est-à-dire que m divise n. Comme n et m jouent des rôles symétriques, on a aussi n qui divise m et en définitive $n=m$ (on peut aussi dire plus rapidement que $\langle g_k\rangle$ est isomorphe à $\mathbb{Z}$ et de ce fait a une infinité de sous groupes). On a donc une contradiction si l'un des $\langle g_k\rangle$ est infini. Donc tous les $\langle g_k\rangle$ sont finis et aussi G.

Exercice 1.25 *Donner des exemples de groupes infinis dans lequel tous les éléments sont d'ordre fini.*

Solution 1.25 *Le groupe quotient $(\mathbb{Q}/\mathbb{Z},+)$ est infini et tous ses éléments sont d'ordre fini (pour tout nombre rationnel $\frac{p}{q}$, on a $q\overline{\frac{p}{q}}=\overline{0}$).*
En désignant, pour tout entier $n\geq 1$, par Γ_n le groupe des racines n-èmes de l'unité dans $\mathbb{C}^*$, la réunion $\Gamma=\bigcup_{n=1}^{+\infty}\Gamma_n$ est un sous-groupe de $\mathbb{C}^*$ ($1\in\Gamma$, pour $z\in\Gamma$, il existe $n\geq 1$ tel que $z\in\Gamma_n$, donc $z^{-1}\in\Gamma_n\subset\Gamma$ et pour z,z' dans Γ, il existe n,m tels que $z\in\Gamma_n$ et $z'\in\Gamma_m$, donc $zz'\in\Gamma_{n\cdot m}\subset\Gamma$). Ce groupe Γ est infini avec tous ses éléments d'ordre fini.
Le groupe additif $G=\dfrac{\mathbb{Z}}{p\mathbb{Z}}[X]$ avec p premier est infini et tous ses éléments sont d'ordre 1 ou p.
Si E est un ensemble infini, alors $(\mathcal{P}(E),\Delta)$ où Δ est l'opérateur de différence symétrique est infini et tous les éléments sont d'ordre 1 ou 2 puisque $A\Delta A=\emptyset$.

Exercice 1.26 *Donner des exemples de groupes dans lequel on peut trouver deux éléments d'ordre fini dont le produit est d'ordre infini.*

Solution 1.26 *Dans le groupe linéaire $GL(\mathbb{R}^2)$, le produit de deux réflexions vectorielles $\sigma_{\mathcal{D}}$ et $\sigma_{\mathcal{D}'}$ d'axes $\mathcal{D}$ et $\mathcal{D}'$ faisant un angle α est une rotation d'angle 2α. Chaque réflexion est d'ordre 2 et la composée $\sigma_{\mathcal{D}}\circ\sigma_{\mathcal{D}'}$ est d'ordre infini si $\dfrac{2\pi}{2\alpha}\notin\mathbb{Q}$.*
Dans le groupe affine $GA(\mathbb{R}^2)$, le produit de deux symétries centrales σ_O et $\sigma_{O'}$ (d'ordres 2) de centres distincts O et O' est la translation de vecteur $2\overrightarrow{OO'}$ qui est d'ordre infini.
Dans le groupe des matrices réelles inversibles d'ordre 2, les matrices $A=\begin{pmatrix}1&0\\1&-1\end{pmatrix}$ et $B=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ sont d'ordre 2 alors que $AB=\begin{pmatrix}1&0\\1&1\end{pmatrix}$ est d'ordre infini (pour tout $n\in\mathbb{N}$, on a $(AB)^n=\begin{pmatrix}1&0\\n&1\end{pmatrix}$).

Exercice 1.27 *Soit $(G,\cdot)$ un groupe tel que tout élément de G soit d'ordre au plus égal à 2.*

1. *Montrer que G est commutatif.*
2. *On suppose de plus que G est fini. Montrer qu'il existe un entier $n\geq 0$ tel que $\mathrm{card}(G)=2^n$.*

Solution 1.27 *Dire que tous les éléments de G sont d'ordre au plus égal à 2, revient à dire que l'on a $g^2 = 1$, ou encore $g = g^{-1}$, pour tout $g \in G$.*

1. *Pour g_1, g_2 dans G, on a $g_1 g_2 = (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1} = g_2 g_1$.*
2. *On peut montrer ce résultat de diverses manières.*

   (a) *On peut raisonner par récurrence sur l'ordre de G.*
   Si G est réduit à $\{1\}$, on a alors $\operatorname{card}(G) = 1 = 2^0$.
   Si G est d'ordre $n \geq 2$, pour tout $g \in G \setminus \{1\}$, on a $\langle g \rangle = \{1, g\}$ et le groupe quotient $\dfrac{G}{\langle g \rangle}$ (c'est un groupe car G est commutatif) est de cardinal $\dfrac{n}{2} < n$ avec tous ses éléments d'ordre au plus égal à 2. En supposant le résultat acquis pour les groupes d'ordre strictement inférieur à n, on a $\operatorname{card}\left(\dfrac{G}{\langle g \rangle}\right) = 2^p$ *et* $\operatorname{card}(G) = 2^{p+1}$.

   (b) *On peut procéder de façon plus astucieuse comme suit. En notant la loi de G sous forme additive, on a $2 \cdot g = 0$ pour tout $g \in G$ et on peut munir G d'une structure de $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$-espace vectoriel en définissant la loi externe par $\overline{0} g = 0$ et $\overline{1} g = g$ pour tout $g \in G$, la loi interne étant l'addition de G (qui est bien commutative). Si G est fini, il est nécessairement de dimension fini sur $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ et notant p sa dimension, on a* $\operatorname{card}(G) = \operatorname{card}\left(\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^p\right) = 2^p$.

   (c) *Comme G est fini, on peut aussi utiliser un système générateur minimal de G, c'est-à-dire que :*
   $$G = \langle g_1, \cdots, g_p \rangle = \left\{ \prod_{k=1}^{p} g_k^{\alpha_k} \mid (\alpha_1, \cdots, \alpha_p) \in \mathbb{Z}^p \right\}$$
   (G est commutatif). Si $p = 1$, on a $G = \langle g_1 \rangle = \{1\}$ ou $\{1, g_1\}$ et c'est terminé. On suppose donc que $p \geq 2$. Comme tous les éléments de G sont d'ordre 1 ou 2, en effectuant des divisions euclidiennes par 2 tout élément de G s'écrit $g = \prod_{k=1}^{p} g_k^{\alpha_k}$ avec $(\alpha_1, \cdots, \alpha_p) \in \{0,1\}^p$ et l'application :
   $$\begin{array}{rccc} \varphi & (\{0,1\})^p & \to & G \\ & (\alpha_1, \cdots, \alpha_p) & \mapsto & \displaystyle\prod_{k=1}^{p} g_k^{\alpha_k} \end{array}$$
   est une bijection de $((\{0,1\})^p, \cdot)$ sur G. On vient de voir que φ est surjective et pour α, β dans $(\{0,1\})^p$, l'égalité $\varphi(\alpha) = \varphi(\beta)$ équivaut à $\prod_{k=1}^{p} g_k^{\beta_k - \alpha_k} = 1$. Si $\alpha \neq \beta$, il existe alors un indice k compris entre 1 et p tel que $\beta_k \neq \alpha_k$ et $\beta_k - \alpha_k = \pm 1$, ce qui entraîne que $g_k = \prod_{\substack{j=1 \\ j \neq k}}^{p} g_k^{\gamma_j}$ est dans le groupe engendré par les g_j avec $j \neq k$ et G est égal à ce groupe, ce qui contredit le caractère minimal de p. On a donc $\alpha = \beta$ et φ est injective, donc bijective. En conséquence $\operatorname{card}(G) = \operatorname{card}(\{0,1\})^p = 2^p$.

   (d) *On peut aussi utiliser le théorème de Cauchy (voir plus loin). Notons $n = 2^p m$ le cardinal de G avec m impair. Si $m = 1$, c'est terminé, sinon, il admet un diviseur premier $q \geq 3$ et le théorème de Cauchy nous dit qu'il existe dans $G \setminus \{1\}$ un élément d'ordre q, ce qui contredit le fait que tous ses éléments sont d'ordre 2.*

(e) Une autre solution consiste à dire que le ppcm *des ordres des éléments de G est égal à 2, et comme ce* ppcm *a les mêmes facteurs premiers que n (voir plus loin), on a nécessairement $n = 2^p$.*

Exercice 1.28 *En utilisant l'exercice précédent, montrer le cas particulier suivant du théorème de Cauchy : si G est un groupe fini d'ordre $2p$ avec p premier, il existe alors un élément d'ordre p dans G.*

Solution 1.28 *Si G est d'ordre $2p \geq 4$ avec p premier, le théorème de Lagrange nous dit que les éléments de $G \setminus \{1\}$ sont d'ordre 2, p ou $2p$. S'il n'y a aucun élément d'ordre p, il n'y en a pas d'ordre $2p$ (si $g \in G \setminus \{1\}$ est d'ordre $2p$, on a alors $g^2 \neq 1$, $g^p \neq 1$ et $(g^2)^p = g^{2p} = 1$, donc g^2 est d'ordre p), donc tous les éléments de $G \setminus \{1\}$ sont d'ordre 2 et G est commutatif d'ordre $2^n = 2p$, donc $p = 2^{n-1}$, $n = 2$ et $p = 2$ puisque p est premier, soit une contradiction avec l'hypothèse qu'il n'y a pas d'élément d'ordre p $(= 2)$. Il existe donc dans G des éléments d'ordre p.*

Exercice 1.29 *Soient $\mathbb{K}$ est un corps de caractéristique différente de 2 et n un entier naturel non nul.*

1. *Montrer que si G est un sous-groupe multiplicatif fini de $GL_n(\mathbb{K})$ tel que tout élément de G soit d'ordre au plus égal à 2, alors G est commutatif de cardinal inférieur ou égal à 2^n.*
2. *En déduire que pour $(n, m) \in (\mathbb{N}^*)^2$ les groupes multiplicatifs $GL_n(\mathbb{K})$ et $GL_m(\mathbb{K})$ sont isomorphes si, et seulement si, $n = m$.*

Solution 1.29

1. *Si tous les éléments du sous-groupe G de $GL_n(\mathbb{K})$ sont d'ordre inférieur ou égal à 2, on sait alors que G est commutatif d'ordre 2^p et il s'agit de montrer que $p \leq n$.*
   Du fait que tous les éléments de G sont diagonalisables (ils sont annulés par le polynôme $X^2 - 1$ qui est scindé à racine simples puisque $\mathbb{K}$ est de caractéristique différente de 2, ce qui entraîne $-1 \neq 1$) et G est commutatif, on déduit les éléments de G sont simultanément diagonalisables, c'est-à-dire qu'il existe une matrice inversible P telle que pour tout M de G la matrice $P^{-1}MP$ est diagonale. De plus avec $M^2 = I_n$, on déduit que les valeurs propres de M sont dans $\{-1, 1\}$ et la matrice $P^{-1}MP$ est de la forme :

$$D = \begin{pmatrix} \varepsilon_1(M) & 0 & \cdots & 0 \\ 0 & \varepsilon_2(M) & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \varepsilon_n(M) \end{pmatrix}$$

   où $\varepsilon_k(M) \in \{-1, 1\}$, pour tout k compris entre 1 et n. On en déduit alors que l'application :

$$M \longmapsto (\varepsilon_1(M), \varepsilon_2(M), \cdots, \varepsilon_n(M))$$

   réalise un isomorphisme de groupes de G sur un sous groupe de $\{-1, 1\}^n$. Le groupe multiplicatif $\{-1, 1\}^n$ étant d'ordre 2^n et l'ordre d'un sous groupe divisant l'ordre du groupe, on déduit que G est fini d'ordre 2^p avec $p \leq n$.
2. *Supposons qu'il existe un isomorphisme de groupes Φ de $GL_n(\mathbb{K})$ sur $GL_m(\mathbb{K})$.*
   On désigne par G le sous groupe de $GL_n(\mathbb{K})$ formé des matrices diagonales de la forme :

$$D = \begin{pmatrix} \varepsilon_1 & 0 & \cdots & 0 \\ 0 & \varepsilon_2 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \varepsilon_n \end{pmatrix}$$

où $\varepsilon_k \in \{-1,1\}$, pour tout k compris entre 1 et n. Ce groupe est d'ordre 2^n avec tous ses éléments d'ordre inférieur ou égal à 2. Par l'isomorphisme Φ il est transformé en un sous groupe H de $GL_m(\mathbb{K})$ ayant les mêmes propriétés. D'après la question précédente, on a alors $n \leq m$. En raisonnant avec l'isomorphisme Φ^{-1} on déduit qu'on a aussi $m \leq n$. Ce qui donne en définitive $m = n$.
La réciproque est évidente.

Théorème 1.15 *Soient g, h dans G d'ordre fini et $k \in \mathbb{Z}^*$.*

1. *On a $\theta\left(g^k\right) = \dfrac{\theta(g)}{\theta(g) \wedge k}$ (en particulier $\theta(g^{-1}) = \theta(g)$).*
2. *Si k divise $\theta(g)$, on a alors $\theta\left(g^k\right) = \dfrac{\theta(g)}{|k|}$.*
3. *Si k est premier avec $\theta(g)$, on a alors $\theta\left(g^k\right) = \theta(g)$.*
4. *Si $gh = hg$, alors hg est d'ordre fini divisant $\theta(g) \vee \theta(h)$.*
   Dans le cas où $\langle g\rangle \cap \langle h\rangle = \{1\}$, on a $\theta(gh) = \theta(g) \vee \theta(h)$. Si $\theta(g)$ et $\theta(h)$ sont premiers entre eux, on a alors $\langle g\rangle \cap \langle h\rangle = \{1\}$ et $\theta(gh) = \theta(g) \vee \theta(h) = \theta(g)\,\theta(h)$.

Démonstration.

1. Soit $\delta = \theta(g) \wedge k$ et n', k' premiers entre eux tels que $\theta(g) = \delta n'$, $k = \delta k'$.
   Pour tout entier relatif j, on a :

$$\begin{aligned}\left(g^k\right)^j = g^{kj} = 1 &\Leftrightarrow \exists q \in \mathbb{Z} \mid kj = q\theta(g) \Leftrightarrow \exists q \in \mathbb{Z} \mid k'j = qn' \\ &\Leftrightarrow n' \text{ divise } j \text{ (Gauss)}\end{aligned}$$

   et en conséquence $\theta\left(g^k\right) = n' = \dfrac{\theta(g)}{\theta(g) \wedge k}$.

2. Si k divise $\theta(g)$, on a alors $\theta(g) \wedge k = |k|$ et $\theta\left(g^k\right) = \dfrac{\theta(g)}{|k|}$.
3. Si k est premier avec $\theta(g)$, on a alors $\theta(g) \wedge k = 1$ et $\theta\left(g^k\right) = \theta(g)$.
4. Soit $\mu = \theta(g) \vee \theta(h)$. Dans le cas où g et h commutent, on a $(gh)^\mu = g^\mu h^\mu = 1$ avec $\mu \geq 1$, donc gh est d'ordre fini et cet ordre divise μ. En désignant par $n = \theta(gh)$ l'ordre de gh, on a $g^n h^n = (gh)^n = 1$ et $g^n = h^{-n} \in \langle g\rangle \cap \langle h\rangle$.
   Si $\langle g\rangle \cap \langle h\rangle = \{1\}$, on a alors $g^n = h^n = 1$ et n est multiple de $\theta(g)$ et $\theta(h)$, donc de $\theta(g) \vee \theta(h)$ et $n = \theta(g) \vee \theta(h)$.
   Si $\theta(g) \wedge \theta(h) = 1$, on a alors $\theta(g) \vee \theta(h) = \theta(g)\,\theta(h)$. De plus avec $\langle g\rangle \cap \langle h\rangle \subset \langle g\rangle$ et $\langle g\rangle \cap \langle h\rangle \subset \langle h\rangle$, on déduit que $\operatorname{card}(\langle g\rangle \cap \langle h\rangle)$ divise $\theta(g) = \operatorname{card}(\langle g\rangle)$ et $\theta(h) = \operatorname{card}(\langle h\rangle)$, donc $\operatorname{card}(\langle g\rangle \cap \langle h\rangle) = 1$ et $\langle g\rangle \cap \langle h\rangle = \{1\}$, ce qui implique que $\theta(gh) = \theta(g) \vee \theta(h) = \theta(g)\,\theta(h)$.

■

On retiendra de ce théorème que si g, h sont deux éléments de G qui commutent avec des ordres premiers entre eux, alors le produit gh est d'ordre $\theta(g)\,\theta(h)$.

Remarque 1.13 *Si $\theta(g)$ et $\theta(h)$ ne sont pas premiers entre eux, avec g, h commutant et d'ordre fini, l'ordre de gh n'est pas nécessairement le* ppcm *de $\theta(g)$ et $\theta(h)$. En prenant par exemple g d'ordre $n \geq 2$ dans G et $h = g^{-1}$ qui est également d'ordre n, on $gh = hg = 1$ d'ordre $1 \neq \operatorname{ppcm}(n, n) = n$.*

Remarque 1.14 *Si g et h ne commutent pas le résultat est faux. Par exemple dans le groupe symétrique $\mathcal{S}_3$ d'ordre 6, $g = (1,2)$ est d'ordre 2, $h = (1,2,3)$ est d'ordre 3 et gh ne peut être d'ordre 6, sans quoi $\mathcal{S}_3$ serait cyclique, ce qui n'est pas (il n'est pas commutatif). En fait $gh = (2,3)$ est d'ordre 2.*

Remarque 1.15 *Pour g et h ne commutant pas, le produit gh peut être d'ordre infini, même si g et h sont d'ordre fini. Considérer, par exemple, le produit de deux matrices de réflexion dans $GL_2(\mathbb{R})$.*

1.5 Quelques applications du théorème de Lagrange

Théorème 1.16 *Un groupe de cardinal premier est cyclique (donc commutatif et isomorphe à $\frac{\mathbb{Z}}{p\mathbb{Z}}$, ce qui signifie qu'à isomorphisme près, il y a un seul groupe d'ordre p premier).*

Démonstration. Soit $(G,\cdot)$ un groupe de cardinal premier $p \geq 2$. Si $g \in G \setminus \{1\}$, il est d'ordre différent de 1 qui divise p, donc cet ordre est p et G est cyclique engendré par g.

L'application $[k] = k + p\mathbb{Z} \in \frac{\mathbb{Z}}{p\mathbb{Z}} \mapsto g^k$ réalise alors un isomorphisme du groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}, +\right)$ sur $(G,\cdot)$. ■

Théorème 1.17 *Un groupe commutatif d'ordre pq, où p et q sont deux nombres premiers distincts, est cyclique (donc commutatif et isomorphe à $\frac{\mathbb{Z}}{pq\mathbb{Z}}$ ou à $\frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{q\mathbb{Z}}$ – théorème chinois – ce qui signifie qu'à isomorphisme près, il y a un seul groupe d'ordre pq, avec p, q premiers distincts)*

Démonstration. Soit G commutatif d'ordre pq avec $2 \leq p < q$ premiers.

S'il existe dans G un élément g d'ordre p et un élément h d'ordre q, alors gh est d'ordre pq (théorème 1.15 pour G commutatif) et G est cyclique.

Sinon les éléments de $G \setminus \{1\}$ sont tous d'ordre p ou tous d'ordre q. Supposons les tous d'ordre p. Si $g \in G$ est d'ordre p, alors le groupe quotient $G/\langle g\rangle$ est d'ordre q premier, donc cyclique, il est donc engendré par $\overline{g_0}$ d'ordre q dans $G/\langle g\rangle$, ce qui entraîne que $\theta(g_0) = p$ divise q, ce qui est impossible pour $p \neq q$ premiers.

Le théorème de Cauchy (voir plus loin) nous donne une démonstration plus rapide. Ce théorème nous dit qu'il existe dans G un groupe d'ordre p et un d'ordre q, ces groupes sont cycliques et on a ainsi un élément d'ordre p et un élément d'ordre q. ■

Pour G non commutatif le résultat précédent est faux comme le montre l'exemple du groupe $\mathcal{S}_3$ qui est d'ordre 6 non commutatif (et donc non cyclique).

Pour $p = q$ premier, c'est également faux comme le montre l'exemple de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$ qui est d'ordre p^2 non cyclique puisque tous ses éléments distincts du neutre sont d'ordre p.

En utilisant les actions de groupe, on montrera qu'un groupe d'ordre p^2 avec p premier est commutatif isomorphe à $\frac{\mathbb{Z}}{p^2\mathbb{Z}}$ (cyclique) ou $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$ (non cyclique).

Exercice 1.30 *Soit $p \geq 2$ un nombre premier. Donner un exemple de groupe d'ordre p^3 non commutatif.*

Solution 1.30 *Le sous-groupe de* $GL_3(\mathbb{Z}_p)$ *formé des matrices de la forme* $\begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix}$ *est d'ordre* p^3 *et non commutatif :*

$$\begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha' & \beta' \\ 0 & 1 & \gamma' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha+\alpha' & \beta+\beta'+\alpha\gamma' \\ 0 & 1 & \gamma+\gamma' \\ 0 & 0 & 1 \end{pmatrix}$$

et il suffit de prendre $\alpha\gamma' \neq \alpha'\gamma$, *par exemple* $\alpha = 0$, $\alpha' = \gamma = 1$.
On peut aussi considérer le groupe des isométries du plan qui conservent les sommets d'un carré qui est d'ordre 2^3 *et non commutatif.*

Exercice 1.31 *Soient* $(G, \cdot)$ *un groupe et* H, K *deux sous-groupes distincts de* G *d'ordre un même nombre premier* $p \geq 2$. *Montrer que* $H \cap K = \{1\}$.

Solution 1.31 $H \cap K$ *est un sous groupe de* H, *il est donc d'ordre* 1 *ou* p. *S'il est d'ordre* p, *il est égal à* H *et* $H = H \cap K \subset K$ *entraîne* $H = K$, *puisque ces deux ensembles ont le même nombre d'éléments. On a donc, pour* $H \neq K$, $p = 1$ *et* $H \cap K = \{1\}$.

Lemme 1.1 *Si* g, h *sont deux éléments d'ordre fini d'un groupe* $(G, \cdot)$ *tels que* $gh = hg$, *il existe alors un élément d'ordre* $\theta(g) \vee \theta(h)$ *dans* G.

Démonstration. Si $\theta(g)$ et $\theta(h)$ sont premiers entre eux avec $gh = hg$, on sait alors que gh est d'ordre $\theta(g)\theta(h) = \theta(g) \vee \theta(h)$ (théorème 1.15). L'idée est de se ramener à ce cas de figure.

On écrit les décompositions en facteurs premiers de $\theta(g)$ et $\theta(h)$ sous la forme :

$$\theta(g) = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{r} p_i^{\alpha_i},\ \theta(h) = \prod_{i=1}^{k} p_i^{\beta_i} \prod_{i=k+1}^{r} p_i^{\beta_i}$$

où les facteurs premiers p_i ont été regroupés de sorte que $\alpha_i > \beta_i$ pour $1 \leq i \leq k$ et $\alpha_i \leq \beta_i$ pour $k+1 \leq i \leq r$, les exposants α_i, β_i étant positifs ou nuls (si l'une des conditions $\alpha_i > \beta_i$ ou $\alpha_i \leq \beta_i$ n'est jamais vérifiée, alors le produit correspondant vaut 1). Avec ces écritures, on a :

$$\theta(g) \vee \theta(h) = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{r} p_i^{\beta_i} = m_1 m_2$$

où $m_1 = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $m_2 = \prod_{i=k+1}^{r} p_i^{\beta_i}$ sont premiers entre eux et $\theta(g) = m_1 n_1$, $\theta(h) = m_2 n_2$. Les éléments $g' = g^{n_1}$ et $h' = h^{n_2}$ sont alors d'ordres respectifs m_1 et m_2 avec $g'h' = h'g'$, donc $g'h'$ est d'ordre $m_1 m_2 = \theta(g) \vee \theta(h)$.

On peut remarquer que ∎

Théorème 1.18 *Si* $(G, \cdot)$ *est un groupe commutatif,* $p \geq 2$ *un entier et* $g_1, g_2, \cdots, g_p$ *des éléments deux à deux distincts de* G *d'ordres respectifs* $m_1, m_2, \cdots, m_p$, *il existe alors dans* G *un élément d'ordre égal au* ppcm *de ces ordres.*

Démonstration. On procède par récurrence sur $p \geq 2$. Pour $p = 2$, c'est le lemme précédent.

Supposons le résultat acquis pour $p \geq 2$ et soient $g_1, g_2, \cdots, g_{p+1}$ deux à deux distincts dans G d'ordres respectifs $m_1, m_2, \cdots, m_{p+1}$. L'hypothèse de récurrence nous dit qu'il existe $g_0 \in G$ d'ordre $m_0 = m_1 \vee m_2 \vee \cdots \vee m_p$ et le cas $p = 2$ qu'il existe g_0' d'ordre :

$$\begin{aligned} m_0 \vee m_{p+1} &= (m_1 \vee m_2 \vee \cdots \vee m_p) \vee m_0 \\ &= m_1 \vee m_2 \vee \cdots \vee m_{p+1} \end{aligned}$$

(associativité du ppcm). ∎

Théorème 1.19 *Si $(G, \cdot)$ est un groupe commutatif fini, on a alors :*

$$\max_{g \in G} \theta(g) = \operatorname{ppcm} \{\theta(g) \mid g \in G\}$$

Démonstration. Comme G est commutatif fini, il existe $g_0 \in G$ tel que :

$$\theta(g_0) = \operatorname{ppcm} \{\theta(g) \mid g \in G\}$$

En désignant par g_1 un élément de G tel que $\theta(g_1) = \max_{g \in G} \theta(g)$, on a $\theta(g_0) \leq \theta(g_1)$ ($\theta(g_1)$ est le plus grand) et $\theta(g_1)$ divise $\theta(g_0)$ ($\theta(g_0)$ est multiple de tous les ordres) donc $\theta(g_1) \leq \theta(g_0)$ et $\theta(g_0) = \theta(g_1)$. ∎

Pour un groupe fini G, $\max_{g \in G} \theta(g)$ est l'exposant du groupe.

Corollaire 1.5 *Tout sous groupe fini du groupe multiplicatif $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ d'un corps commutatif $\mathbb{K}$ est cyclique.*

Démonstration. Soit $(G, \cdot)$ un sous groupe d'ordre n de $\mathbb{K}^*$. Il existe dans le groupe fini commutatif G un élément g_0 d'ordre $m \leq n$ égal au ppcm des ordres des éléments de G. L'ordre de tout élément de G divisant m, on déduit que tout $g \in G$ est racine du polynôme $P(X) = X^m - 1$, ce qui donne n racines distinctes de P dans $\mathbb{K}$, mais sur un corps commutatif un polynôme de degré m a au plus m racines[1], on a donc $n \leq m$ et $m = n$. Le groupe G d'ordre n ayant un élément d'ordre n est cyclique. ∎

Exemple 1.10 *Si $\mathbb{K}$ est un corps fini, il est alors commutatif (démonstration non évidente) et en conséquence $\mathbb{K}^*$ est cyclique. En particulier, pour $p \geq 2$ premier le groupe $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ est cyclique d'ordre $p - 1$.*

Théorème 1.20 *Si $(G, \cdot)$ un groupe commutatif fini d'ordre $n \geq 2$, alors n et son exposant $m = \max_{g \in G} \theta(g)$ ont les mêmes facteurs premiers.*

Démonstration. Soit $G = \{g_1, \cdots, g_n\}$ un groupe commutatif fini d'ordre $n \geq 2$.

Comme il existe $i \in \{1, \cdots, n\}$ tel que $m = \theta(g_i)$, cet entier m divise l'ordre n de G et les facteurs premiers de m sont aussi des facteurs premiers de n.

En utilisant l'application φ du groupe produit $H = \prod_{k=1}^{n} \langle g_k \rangle$ dans G définie par :

$$\forall h = (h_1, \cdots, h_n) \in H,\ \varphi(h) = \prod_{i=1}^{n} h_i$$

[1] Ce résultat est faux sur un corps non commutatif, voir par exemple le corps des quaternions.

on vérifie d'abord que n divise le produit des ordres $\prod_{k=1}^{n}\theta(g_k)$.

L'application φ est surjective et comme G est commutatif, c'est un morphisme de groupes. Ce morphisme φ induit alors un isomorphisme du groupe quotient $H/\ker(\varphi)$ sur G, ce qui entraîne que $\text{card}(H) = \text{card}(\ker(\psi))\,\text{card}(G)$ et $n = \text{card}(G)$ divise $\text{card}(H) = \prod_{k=1}^{n}\theta(g_k)$.

Sachant que m est aussi le ppcm des ordres des éléments de G, il est multiple de chaque $\theta(g_k)$ et m^n est multiple de $\prod_{k=1}^{n}\theta(g_k)$ donc de n. Donc les facteurs premiers de n sont aussi des facteurs premiers de m. En définitive m et n ont les mêmes facteurs premiers. ■

Remarque 1.16 *Si $(G,\cdot)$ est un groupe commutatif fini d'ordre $n \geq 2$ tel que tous les éléments de $G\setminus\{1\}$ soient d'ordre un nombre premier $p \geq 2$, alors $n = p^r$ avec $r \geq 1$. En effet, dans ce cas* $\text{ppcm}\{\theta(g) \mid g \in G\} = p$ *et c'est le seul facteur premier de n (voir aussi l'exercice 1.27).*

Corollaire 1.6 *Si $n \geq 2$ est un entier premier avec $\varphi(n)$, alors tout groupe commutatif d'ordre n est cyclique.*

Démonstration. Comme $m = \text{ppcm}\{\theta(g) \mid g \in G\} = \theta(g_0)$ et n ont les mêmes facteurs premiers, on a les décompositions en facteurs premiers $m = \prod_{k=1}^{r} p_k^{\alpha_k}$ et $n = \prod_{k=1}^{r} p_k^{\beta_k}$, où les p_k sont premiers deux à deux distincts et $1 \leq \alpha_k \leq \beta_k$ pour tout k compris entre 1 et n. Sachant que :

$$\varphi(n) = \prod_{k=1}^{r} p_k^{\beta_k - 1}(p_k - 1)$$

on déduit que si $\varphi(n)$ est premier avec n, alors tous les β_k valent 1 (sinon p_k divise $\varphi(n)$ et n) et les α_k valent aussi 1, ce qui donne $n = m$ et G est cyclique puisque g_0 est d'ordre $n = \text{card}(G)$. ■

Réciproquement, on peut montrer que la réciproque est vrai, c'est-à-dire qu'un entier $n \geq 2$ est premier avec $\varphi(n)$, si, et seulement si, tout groupe commutatif d'ordre n est cyclique (voir Francinou et Gianella, exercices de mathématiques pour l'agrégation, Masson).

Le théorème de Lagrange peut aussi être utilisé pour montrer quelques résultats classiques d'arithmétique.

Théorème 1.21 (Euler) *Soit $n \geq 2$. Pour tout entier relatif k premier avec n, on a $k^{\varphi(n)} \equiv 1 \pmod{n}$*

Démonstration. Si k est premier avec n, alors $\overline{k}$ appartient à $\mathbb{Z}_n^\times$ qui est d'ordre $\varphi(n)$ et $\overline{k}^{\varphi(n)} = \overline{1}$, c'est-à-dire que $k^{\varphi(n)} \equiv 1 \pmod{n}$. ■

Pour $p \geq 2$ premier, on a $\varphi(p) = p-1$ et on retrouve le petit théorème de Fermat : $\overline{k}^{p-1} = \overline{1}$ pour $k \wedge p = 1$ et $\overline{k}^{p} = \overline{k}$ pour tout $k \in \mathbb{Z}$.

Exercice 1.32 *Montrer que pour $n \geq 3$, $\varphi(n)$ est un entier pair.*

Solution 1.32 *Avec $\overline{(-1)}^2 = \overline{(-1)^2} = \overline{1}$, on déduit que $\overline{(-1)}$ est d'ordre 1 ou 2 dans $\mathbb{Z}_n^\times$. Pour $n \geq 3$, on a $\overline{(-1)} \neq \overline{1}$, donc $\overline{(-1)}$ est d'ordre 2 qui va diviser l'ordre du groupe $\mathbb{Z}_n^\times$, soit $\varphi(n)$. On peut aussi montrer ce résultat en écrivant que :*

$$\mathbb{Z}_n^\times = \left\{-\overline{1}, \overline{1}\right\} \cup \left\{\overline{k}, \frac{1}{\overline{k}} \mid \overline{k} \notin \left\{-\overline{1}, \overline{1}\right\}\right\}$$

Pour $n = 2$, on a $\mathbb{Z}_2 = \left\{\overline{0}, \overline{1}\right\}$ et $\mathbb{Z}_2^\times = \left\{\overline{1}\right\}$.

Théorème 1.22 (Wilson) *Un entier naturel $p \geq 2$ est premier si et seulement si $(p-1)! \equiv -1 \ (p)$*

Démonstration. Si p est premier, alors $\mathbb{Z}_p$ est un corps commutatif à p éléments et tout élément $\overline{k}$ du groupe $\mathbb{Z}_p^\times$ est racine du polynôme $X^{p-1} - \overline{1}$, on a donc $X^{p-1} - \overline{1} = \prod_{k=1}^{p-1} \left(X - \overline{k}\right)$ dans $\mathbb{Z}_p[X]$ et en évaluant ce polynôme en $\overline{0}$, il vient $-\overline{1} = \prod_{k=1}^{p-1} \left(-\overline{k}\right) = (-1)^{p-1} \overline{(p-1)!}$. Pour $p = 2$, on a $-\overline{1} = \overline{1}$ et pour p premier impair, on a $-\overline{1} = \overline{(p-1)!}$ dans $\mathbb{Z}_p$.

Réciproquement si $p \geq 2$ est tel que $\overline{(p-1)!} = -\overline{1}$ dans $\mathbb{Z}_p$, alors tout diviseur d de p compris entre 1 et $p-1$ divisant $(p-1)! = -1 + kp$ va diviser -1, ce qui donne $d = 1$ et l'entier p est premier. ∎

Exercice 1.33 *Montrer qu'un entier p supérieur ou égal à 2 est premier si, et seulement si, $(p-2)!$ est congru à 1 modulo p.*

Solution 1.33 *Pour $p \geq 2$, on a $(p-1)! = (p-1)(p-2)! \equiv -(p-2)!$ modulo p, avec la convention $0! = 1$. Le résultat se déduit alors du théorème de Wilson.*

Exercice 1.34 *Soit p un nombre premier impair.*

1. *En utilisant l'application $x \mapsto x^2$ de $\mathbb{Z}_p^\times$ dans $\mathbb{Z}_p^\times$, montrer qu'il y a exactement $\dfrac{p-1}{2}$ carrés dans $\mathbb{Z}_p^\times$.*
2. *Montrer que l'ensemble des carrés de $\mathbb{Z}_p^\times$ est l'ensemble des racines du polynôme $P(X) = X^{\frac{p-1}{2}} - \overline{1}$.*
3. *En déduire que $\overline{(-1)}$ est un carré dans $\mathbb{Z}_p$ si, et seulement si, p est congru à 1 modulo 4.*
4. *En déduire qu'il existe une infinité de nombres premiers de la forme $4n+1$.*

Solution 1.34

1. *L'application $\varphi : x \mapsto x^2$ est un morphisme de groupes de $\mathbb{Z}_p^\times$ dans $\mathbb{Z}_p^\times$ de noyau $\ker(\varphi) = \left\{\overline{(-1)}, \overline{1}\right\}$ ($x^2 = 1 \Leftrightarrow (x-1)(x+1) = 0$ et $-1 \neq 1$ dans le corps $\mathbb{Z}_p$ pour $p \geq 3$ premier). On a donc $\operatorname{card}(\operatorname{Im}(\varphi)) = \operatorname{card}\left(\mathbb{Z}_p^\times / \left\{\overline{(-1)}, \overline{1}\right\}\right) = \dfrac{p-1}{2}$, ce qui signifie qu'il y a exactement $\dfrac{p-1}{2}$ carrés dans $\mathbb{Z}_p^\times$ (comme $\overline{0}$ est un carré, il y a exactement $\dfrac{p+1}{2}$ carrés dans $\mathbb{Z}_p$).*
2. *Si $x \in \mathbb{Z}_p^\times$ est un carré, il existe $y \in \mathbb{Z}_p^\times$ tel que $x = y^2$ et $x^{\frac{p-1}{2}} = y^{p-1} = \overline{1}$. Donc les carrés de $\mathbb{Z}_p^\times$ sont racines du polynôme $P(X) = X^{\frac{p-1}{2}} - \overline{1}$. Comme il y a $\dfrac{p-1}{2}$ carrés et au plus $\dfrac{p-1}{2}$ racines du polynôme P dans $\mathbb{Z}_p^\times$, on en déduit l'ensemble $\operatorname{Im}(\varphi)$ des carrés de $\mathbb{Z}_p^\times$ est l'ensemble des racines du polynôme $P(X) = X^{\frac{p-1}{2}} - \overline{1}$.*
3. *On a :*

$$\left(\overline{(-1)} \in \operatorname{Im}(\varphi)\right) \Leftrightarrow \left(\overline{(-1)}^{\frac{p-1}{2}} = \overline{1}\right) \Leftrightarrow \left(\frac{p-1}{2} \equiv 0 \pmod 2\right)$$
$$\Leftrightarrow (p \equiv 1 \pmod 4)$$

4. *Supposons qu'il y a un nombre fini d'entiers premiers de la forme* $4n+1$. *On désigne par* m *le plus grand de ces entiers et par* $p \geq 3$ *un diviseur premier de* $N = (m!)^2 + 1$, *on a alors* $p > m$ *et* $\overline{(m!)^2} = \overline{(-1)}$, *donc* $\overline{(-1)}$ *est un carré dans* $\mathbb{Z}_p$ *et est premier de la forme* $4n+1$, *ce qui contredit* $p > m$.

Exercice 1.35 *On appelle nombre de Fermat tout entier de la forme :*

$$F_n = 2^{2^n} + 1$$

où n *est un entier naturel.*
On désigne par p *un diviseur premier d'un nombre de Fermat* F_n *et on suppose que* $p \neq F_n$.

1. *Montrer que pour* $n \neq m$ *dans* $\mathbb{N}$, F_n *et* F_m *sont premiers entre eux.*
2. *Montrer que* $\overline{2}$ *est d'ordre* 2^{n+1} *dans le groupe multiplicatif* $\mathbb{Z}_p^*$.
3. *Montrer que* p *congru à* 1 *modulo* 2^{n+1}.
4. *Soient* $r \geq 1$ *et* $a \geq 2$ *deux entiers. Montrer que si* $a^r + 1$ *est premier, alors* a *est pair et il existe un entier* $n \geq 0$ *tel que* $r = 2^n$.
5. *Montrer que* $p = 2^{n+1}q + 1$, *où* q *est un entier qui admet un diviseur premier impair.*
   Pour $F_5 = 4\ 294\,967\,297$, *s'il n'est pas premier ses diviseurs premiers sont de la forme* $p = 2^6 q + 1 = 64q + 1$ *où les valeurs possibles de* q *sont* $3, 5, 6, 7, 9, 10, \cdots$ *En essayant successivement ces valeurs, on aboutit à :*

$$\frac{F_5}{641} = \frac{4\ 294\,967\,297}{641} = 6700\,417$$

   et F_5 *n'est pas premier (ce qui fût montré par Euler).*

Solution 1.35 *Si* p *premier divise* F_n, p *est impair comme* F_n *et* $p \geq 3$.

1. *On a* $\overline{F_n} = \overline{0}$ *dans* $\mathbb{Z}_p$, *soit* $\overline{2^{2^n}} = -1$ *et* $\overline{F_m} = \left(\overline{2^{2^n}}\right)^{2^{m-n}} + \overline{1} = \overline{2} \neq \overline{0}$ *dans* $\mathbb{Z}_p$ *puisque* $p \neq 2$, *ce qui signifie que* p *ne divise pas* F_m. *Donc* F_n *et* F_m *sont premiers entre eux.*
2. *Comme* $p \geq 3$ *divise* F_n, *on a* $\overline{F_n} = \overline{0}$ *dans* $\mathbb{Z}_p$, *soit* $\overline{2}^{2^n} = -\overline{1} \neq \overline{1}$ *dans* $\mathbb{Z}_p^\times$ *et* $\overline{2}^{2^{n+1}} = \left(\overline{2}^{2^n}\right)^2 = \left(-\overline{1}\right)^2 = \overline{1}$. *Donc l'ordre de* $\overline{2}$ *est exactement* 2^{n+1}.
3. 2^{n+1} *est donc un diviseur de* $p - 1 = \operatorname{card}\left(\mathbb{Z}_p^\times\right)$, *ce qui peut se traduire par* $p-1$ *congru à* 0 *modulo* 2^{n+1} *ou encore* p *congru à* 1 *modulo* 2^{n+1}.
4. *Supposons que* a *soit impair, on a donc* $a \geq 3$ *et* $a^r + 1$ *est un nombre pair supérieur ou égal à* 4, *il ne peut être premier. L'entier* a *est donc nécessairement pair si* $a^r + 1$ *est premier.*
   En utilisant la décomposition en facteurs premiers, on a $r = 2^n(2q+1)$ *où* n *et* q *sont deux entiers naturels et :*

$$\begin{aligned} a^r + 1 &= \left(a^{2^n}\right)^{2q+1} + 1 = b^{2q+1} + 1 \\ &= (b+1)\sum_{k=0}^{2q} (-1)^k b^{2q-k} = (b+1)\,S \end{aligned}$$

   avec $b + 1 = a^{2^n} + 1 \geq 3$ *puisque* $a \geq 2$, *ce qui impose* $S = 1$ *puisque* $a^r + 1$ *est premier. En écrivant que :*

$$S = \frac{a^r + 1}{b+1} = \frac{b^{2q+1} + 1}{b+1} = \frac{b^{2q}b + 1}{b+1} = 1$$

   on déduit que $q = 0$ *et* $r = 2^n$.

5. *Dire que p est congru à 1 modulo 2^{n+1} signifie qu'il existe un entier $q \geq 1$ tel que $p = 2^{n+1}q + 1$. Si q n'admet aucun diviseur premier impair, il est de la forme $q = 2^m$ avec $m \geq 0$ et $p = 2^{n+1+m} + 1$ est premier, ce qui impose que $n + 1 + m = 2^r$, c'est-à-dire que $p = 2^{2^r} + 1$ est un nombre de Fermat et $p = F_n$ puisque deux nombres de Fermat distincts sont premiers entre eux, en contradiction avec $p \neq F_n$. Donc q admet un diviseur premier impair.*

Exercice 1.36 *Pour $n \geq 1$, on désigne par Γ_n le groupe multiplication des racines complexes de l'unité.*

1. *Montrer que pour $n \geq 1$ et $m \geq 1$, on a $\Gamma_n \cap \Gamma_m = \Gamma_{n \wedge m}$.*
2. *Montrer que $(X^n - 1) \wedge (X^m - 1) = X^{n \wedge m} - 1$ dans $\mathbb{C}[X]$. Expliquer pourquoi ce résultat est encore vrai dans $\mathbb{R}[X]$.*

Solution 1.36

1. *Notons $\delta = n \wedge m$ et $H = \Gamma_n \cap \Gamma_m$. Avec $H \subset \Gamma_n$ et $H \subset \Gamma_m$, on déduit que* $\operatorname{card}(H)$ *divise n et m, il divise donc δ. Puis avec $\Gamma_\delta \subset \Gamma_n$ et $\Gamma_\delta \subset \Gamma_m$, on déduit que $\Gamma_\delta \subset H = \Gamma_n \cap \Gamma_m$ et $\delta = \operatorname{card}(\Gamma_\delta)$ divise* $\operatorname{card}(H)$. *On a donc* $\operatorname{card}(H) = \operatorname{card}(\Gamma_\delta)$ *et $H = \Gamma_\delta$.*
2. *Pour tout $r \geq 1$, on a $X^r - 1 = \prod_{\lambda \in \Gamma_r} (X - \lambda)$. Donc $X^n - 1 = \prod_{\lambda \in \Gamma_n} (X - \lambda)$, $X^m - 1 = \prod_{\lambda \in \Gamma_m} (X - \lambda)$ et comme toutes ces racines sont simples :*

$$(X^n - 1) \wedge (X^m - 1) = \prod_{\lambda \in \Gamma_n \cap \Gamma_m} (X - \lambda) = \prod_{\lambda \in \Gamma_{n \wedge m}} (X - \lambda) = X^{n \wedge m} - 1$$

Comme le pgcd *dans $\mathbb{K}[X]$ se calcule en effectuant des divisions euclidiennes successives et que restes et quotients sont uniquement déterminés, on en déduit que le* pgcd *de deux polynômes de $\mathbb{R}[X]$ est le même dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.*

1.6 Actions de groupes

Définition 1.10 *Si $(G, \cdot)$ est un groupe et E un ensemble non vide, on dit que G opère à gauche sur E si on a une application :*

$$\begin{array}{rcl} G \times E & \to & E \\ (g, x) & \mapsto & g \cdot x \end{array}$$

telle que :

$$\begin{cases} \forall x \in E,\ 1 \cdot x = x \\ \forall (g, g', x) \in G^2 \times E,\ g \cdot (g' \cdot x) = (gg') \cdot x \end{cases}$$

Une telle application est aussi appelée action à gauche de G sur E.
Pour tout $g \in G$, l'application :

$$\begin{array}{rccc} \varphi(g) : & E & \to & E \\ & x & \mapsto & g \cdot x \end{array}$$

est alors une bijection de E sur E, c'est-à-dire que $\varphi(g) \in \mathcal{S}(E)$, où on a noté $\mathcal{S}(E)$ le groupe des permutations de E. En effet, avec $1 \cdot x = x$ pour tout $x \in E$, on déduit que

$\varphi(1) = Id_E$ et avec $g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = 1 \cdot x = x$ et $g^{-1} \cdot (g \cdot x) = x$ on déduit que $\varphi(g) \circ \varphi(g^{-1}) = \varphi(g^{-1}) \circ \varphi(g) = Id_E$, ce qui signifie que $\varphi(g)$ est bijective d'inverse $\varphi(g^{-1})$.

De plus avec $g \cdot (g' \cdot x) = (gg') \cdot x$, pour tous g, g', x, on déduit que $\varphi(gg') = \varphi(g) \circ \varphi(g')$, c'est-à-dire que l'application φ est un morphisme de groupes de $(G, \cdot)$ dans $(\mathcal{S}(E), \circ)$.

Réciproquement un tel morphisme φ définit une action à gauche de G sur E avec :

$$g \cdot x = \varphi(g)(x)$$

Exemple 1.11 *Un groupe G agit sur lui même par automorphismes intérieurs :*

$$(g, h) \in G \times G \mapsto g \cdot h = ghg^{-1}$$

Exemple 1.12 *Un groupe G agit sur tout sous-groupe distingué H par conjugaison :*

$$(g, h) \in G \times H \mapsto g \cdot h = ghg^{-1} \in H$$

Exemple 1.13 *Le groupe $\mathcal{S}(E)$ agit naturellement sur E par :*

$$(\sigma, x) \in \mathcal{S}(E) \times E \mapsto \sigma \cdot x = \sigma(x) \in E$$

Définition 1.11 *Soit G un groupe opérant sur un ensemble non vide E. Pour tout $x \in E$, le sous-ensemble de E :*

$$G \cdot x = \{g \cdot x \mid g \in G\}$$

est appelé orbite de x sous l'action de G.

On vérifie facilement que la relation $x \sim y$ si, et seulement si, il existe $g \in G$ tel que $y = g \cdot x$ est une relation d'équivalence sur E ($x = 1 \cdot x$ donne la réflexivité, $y = g \cdot x$ équivalent à $x = g^{-1} \cdot y$ donne la symétrie et $y = g \cdot x$, $z = h \cdot y$ qui entraîne $z = (hg) \cdot x$ donne la transitivité) et la classe de $x \in E$ pour cette relation est l'orbite de x. Il en résulte que les orbites forment une partition de E.

Définition 1.12 *Soit G un groupe opérant sur un ensemble non vide E. Pour tout $x \in X$, le sous-ensemble de G :*

$$G_x = \{g \in G \mid g \cdot x = x\}$$

est le stabilisateur de x sous l'action de G.

On vérifie facilement que ces stabilisateurs G_x sont des sous-groupes de G (en général non distingués).

Théorème 1.23 (équation des classes) *Soit $(G, \cdot)$ est un groupe opérant sur un ensemble E.*

1. *Pour tout $x \in E$ l'application :*

$$\begin{array}{rccc} \varphi_x : & G/G_x & \to & G \cdot x \\ & \overline{g} = gG_x & \mapsto & g \cdot x \end{array}$$

est bien définie et bijective. Dans le cas où G fini, on a :

$$\operatorname{card}(G \cdot x) = \frac{\operatorname{card}(G)}{\operatorname{card}(G_x)}$$

(donc $\operatorname{card}(G \cdot x)$ *divise* $\operatorname{card}(G)$*).*

2. *Dans le cas où G et E sont finis, en notant $G \cdot x_1, \cdots, G \cdot x_r$ toutes les orbites deux à deux distinctes, on a :*

$$\operatorname{card}(E) = \sum_{i=1}^{r} \operatorname{card}(G \cdot x_i) = \sum_{i=1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})}$$

Démonstration.

1. En remarquant que pour g, h dans G et $x \in E$, l'égalité $g \cdot x = h \cdot x$ équivaut à $(h^{-1}g) \cdot x = x$, soit à $h^{-1}g \in G_x$ ou encore à $\overline{g} = \overline{h}$ dans G/G_x, on déduit que l'application φ_x est bien définie et injective. Cette application étant clairement surjective, elle définie une bijection de G/G_x sur $G \cdot x$. Dans le cas où G fini, on a :

$$\operatorname{card}(G \cdot x) = \operatorname{card}(G/G_x) = \frac{\operatorname{card}(G)}{\operatorname{card}(G_x)}$$

2. Si E est fini, on a alors un nombre fini d'orbites $G \cdot x_1, \cdots, G \cdot x_r$ qui forment une partition de E et :

$$\operatorname{card}(E) = \sum_{i=1}^{r} \operatorname{card}(G \cdot x_i).$$

   En utilisant la bijection de G/G_x sur $G \cdot x_i$, on déduit que si G est aussi fini, on a alors :

$$\operatorname{card}(E) = \sum_{i=1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})}.$$

■

Si $(G, \cdot)$ est un groupe opérant sur un ensemble E, on note alors :

$$E^G = \{x \in E \mid G \cdot x = \{x\}\}$$

C'est l'ensemble des éléments de E dont l'orbite est réduite à un point.
En séparant dans la formule des classes les orbites réduites à un point des autres, elle s'écrit :

$$\operatorname{card}(E) = \operatorname{card}\left(E^G\right) + \sum_{\substack{i=1 \\ \operatorname{card}(G \cdot x_i) \geq 2}}^{r} \operatorname{card}(G \cdot x_i)$$

(la somme étant nulle si toutes les orbites sont réduites à un point).

Définition 1.13 *Si $p \geq 2$ est un nombre premier, on appelle p-groupe tout groupe de cardinal p^α où α est un entier naturel non nul.*

Corollaire 1.7 *Si $p \geq 2$ est un nombre premier et $(G, \cdot)$ est un p-groupe opérant sur un ensemble fini E, alors :*

$$\operatorname{card}\left(E^G\right) \equiv \operatorname{card}(E) \pmod{p}.$$

Démonstration. Dans le cas d'un p-groupe de cardinal p^α avec $\alpha \geq 1$, pour toute orbite $G \cdot x_i$ non réduite à un point (s'il en existe), on a :

$$\operatorname{card}(G \cdot x_i) = \operatorname{card}\left(\frac{G}{G_{x_i}}\right) = \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})} \geq 2$$

donc $\operatorname{card}(G_{x_i}) = p^{\beta_i}$ avec $0 \leq \beta_i < \alpha$ et $\operatorname{card}(G \cdot x_i) = p^{\alpha-\beta_i}$ avec $1 \leq \alpha - \beta_i \leq \alpha$. Il en résulte que :

$$\operatorname{card}(E) = \operatorname{card}\left(E^G\right) + \sum_{\substack{i=1 \\ \operatorname{card}(G\cdot x_i)\geq 2}}^{r} \operatorname{card}(G \cdot x_i) \equiv \operatorname{card}\left(E^G\right) \pmod{p}$$

■

Corollaire 1.8 *Soit G un groupe fini que l'on fait opérer sur lui même par conjugaison ($g \cdot h = ghg^{-1}$, pour $(g,h) \in G \times G$). En notant $G \cdot h_1, \cdots, G \cdot h_r$ toutes les orbites deux à deux distinctes, on a :*

$$\begin{aligned} \operatorname{card}(G) &= \operatorname{card}(Z(G)) + \sum_{\substack{i=1 \\ \operatorname{card}(G\cdot h_i)\geq 2}}^{r} \operatorname{card}(G \cdot h_i) \\ &= \operatorname{card}(Z(G)) + \sum_{\substack{i=1 \\ \operatorname{card}(G\cdot h_i)\geq 2}}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{h_i})}. \end{aligned}$$

Démonstration. Une orbite $G \cdot h$ est réduite à $\{h\}$ si et seulement si $ghg^{-1} = h$ pour tout $g \in G$, ce qui revient à dire que $gh = hg$, ou encore que $h \in Z(G)$. On a donc $Z(G) = G^G$ et le résultat annoncé. ■

Corollaire 1.9 *Pour tout nombre premier p, le centre d'un p-groupe n'est pas réduit à $\{1\}$.*

Démonstration. Soit G un p-groupe à p^α éléments.

On a, avec les notations des corollaires qui précèdent :

$$\operatorname{card}(Z(G)) = \operatorname{card}\left(G^G\right) \equiv \operatorname{card}(G) \pmod{p}$$

et comme $\operatorname{card}(Z(G)) \geq 1$, il en résulte que $\operatorname{card}(Z(G)) \geq p$ et $Z(G)$ est non trivial. ■

Corollaire 1.10 *Tout groupe d'ordre p^2 avec p premier est commutatif.*

Démonstration. Soit G d'ordre p^2. On sait que $Z(G)$ est non trivial, il est donc de cardinal p ou p^2 et il s'agit de montrer qu'il est de cardinal p^2.

Si $Z(G)$ est de cardinal p, il est alors cyclique, soit $Z(G) = \langle g \rangle$.

Un élément h de $G \setminus Z(G)$ ne pouvant être d'ordre p^2 (sinon $G = \langle h \rangle$ et G serait commutatif ce qui contredit l'hypothèse $G \neq Z(G)$), il est d'ordre p et $Z(G) \cap \langle h \rangle = \{1\}$ (exercice 1.31)

En utilisant l'application :

$$\begin{array}{rccc} \varphi : & \{0,1,\cdots,p-1\}^2 & \to & G \\ & (i,j) & \mapsto & g^i h^j \end{array}$$

nous déduisons que tout élément de G s'écrit de manière unique $g^i h^j$. Pour ce faire il suffit de montrer que φ est injective. Si $g^i h^j = g^{i'} h^{j'}$, alors $g^{i-i'} = h^{j'-j} \in Z(G) \cap \langle h \rangle = \{1\}$ et $g^{i-i'} = h^{j'-j} = 1$ ce qui entraîne que p divise $i - i'$ et $j - j'$ et comme $|i - i'| < p$, $|j - j'| < p$, on a nécessairement $i = i'$, $j = j'$. Avec les cardinaux il en résulte que φ est une bijection.

Si k, k' sont dans G, il s'écrivent $k = g^i h^j$ et $k' = g^{i'} h^{j'}$ et comme g commute à tout G, on en déduit que k et k' commutent. Le groupe G serait alors commutatif ce qui est contraire à l'hypothèse $G \neq Z(G)$.

En définitive $Z(G)$ ne peut être de cardinal p, il est donc de cardinal p^2 et G est commutatif. ■

Si G d'ordre p^2 a un élément d'ordre p^2, il est alors cyclique isomorphe à $\dfrac{\mathbb{Z}}{p^2\mathbb{Z}}$. Dans le cas où tous ses éléments sont d'ordre p, il est isomorphe à $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$.

Exercice 1.37 *Soit $(G,\cdot)$ est un groupe fini opérant sur un ensemble fini E. Pour tout $g \in G$, on note :*

$$\mathrm{Fix}(g) = \{x \in E \mid g \cdot x = x\}$$

Montrer que le nombre d'orbites est :

$$r = \frac{1}{\mathrm{card}(G)} \sum_{g \in G} \mathrm{card}(\mathrm{Fix}(g))$$

(formule de Burnside).

Solution 1.37 *L'idée est de calculer le cardinal de l'ensemble :*

$$F = \{(g,x) \in G \times E \mid g \cdot x = x\}$$

de deux manières en utilisant les partitions :

$$F = \bigcup_{g \in G} \{(g,x) \mid x \in \mathrm{Fix}(g)\} = \bigcup_{x \in E} \{(g,x) \mid g \in G_x\}$$

ce qui donne :

$$\mathrm{card}(F) = \sum_{g \in G} \mathrm{card}(\mathrm{Fix}(g))$$

et en notant $G \cdot x_1, \cdots, G \cdot x_r$ les orbites distinctes :

$$\begin{aligned}
\mathrm{card}(F) &= \sum_{x \in E} \mathrm{card}(G_x) = \sum_{x \in E} \frac{\mathrm{card}(G)}{\mathrm{card}(G \cdot x)} \\
&= \sum_{i=1}^{r} \sum_{x \in G \cdot x_i} \frac{\mathrm{card}(G)}{\mathrm{card}(G \cdot x)} = \sum_{i=1}^{r} \mathrm{card}(G) \left(\sum_{x \in G \cdot x_i} \frac{1}{\mathrm{card}(G \cdot x)} \right) \\
&= \sum_{i=1}^{r} \mathrm{card}(G) \left(\sum_{x \in G \cdot x_i} \frac{1}{\mathrm{card}(G \cdot x_i)} \right) = \sum_{i=1}^{r} \mathrm{card}(G) = r\,\mathrm{card}(G)
\end{aligned}$$

du fait que $G \cdot x = G \cdot x_i$ pour $x \in G \cdot x_i$ (la relation $x \sim y$ si $y = g \cdot x$ est d'équivalence et les classes d'équivalence sont les orbites). Ce qui donne le résultat annoncé.

1.7 Le théorème de Cauchy

Si H est un sous-groupe de G, le théorème de Lagrange nous dit que l'ordre de H est un diviseur de n. On s'intéresse ici à la réciproque.

Le théorème qui suit nous dit que les sous-groupes d'un groupe cyclique sont cycliques et que pour tout diviseur d de n, il existe un sous-groupe de G d'ordre d. Ce résultat n'est pas vrai pour un groupe fini quelconque comme nous le verrons avec l'étude du groupe symétrique ($\mathcal{A}_4$ qui est d'ordre 12 n'a pas de sous groupes d'ordre 6).

Théorème 1.24 *Soit $G = \langle a \rangle$ groupe cyclique d'ordre $n \geq 2$. Pour tout diviseur d de n, il existe un unique sous groupe d'ordre d de G, c'est le groupe cyclique $H = \left\langle a^{\frac{n}{d}} \right\rangle$.*

Démonstration. Pour tout diviseur d de n, $H = \left\langle a^{\frac{n}{d}} \right\rangle$ est un sous-groupe cyclique de G et le théorème 1.15 nous dit qu'il est d'ordre $\theta\left(a^{\frac{n}{d}}\right) = \dfrac{n}{n \wedge \frac{n}{d}} = d$.

Réciproquement soit H un sous-groupe de G d'ordre d, un diviseur de n.

Si $d = 1$, on a alors $H = \{1\} = \langle a^n \rangle$.

Si $d \geq 2$, H n'est pas réduit à $\{1\}$, donc il existe un entier k compris entre 1 et $n-1$ tel que $a^k \in H$ et on peut poser :

$$p = \min\left\{k \in \{1, \cdots, n-1\} \mid a^k \in H\right\}.$$

En écrivant, pour tout $h = a^k \in H$, $k = pq + r$ avec $0 \leq r \leq p-1$ (division euclidienne par p), on a $a^r = a^k \left(a^{pq}\right)^{-1} \in H$ et nécessairement $r = 0$. On a donc $H \subset \langle a^p \rangle \subset H$, soit $H = \langle a^p \rangle$. Avec $a^n = 1 \in H$, on déduit que n est multiple de p et l'ordre de H est $d = \dfrac{n}{n \wedge p} = \dfrac{n}{p}$, c'est-à-dire que $H = \left\langle a^{\frac{n}{d}} \right\rangle$. Un tel sous-groupe d'ordre d est donc unique. ∎

Réciproquement, on peut montrer qu'un groupe fini ayant la propriété du théorème précédent est nécessairement cyclique (voir Delcourt, exercice 1.1.12.).

Exemple 1.14 *Les sous groupes de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sont les $\left\langle \dfrac{n}{d}\overline{1} \right\rangle = \left\langle \dfrac{\overline{n}}{d} \right\rangle$ où d est un diviseur de n. Un tel sous-groupe est isomorphe à $\dfrac{\mathbb{Z}}{d\mathbb{Z}}$ et il y en a autant que de diviseurs de n.*

Exemple 1.15 *Les sous groupes de $\Gamma_n = \{z \in C \mid z^n = 1\} = \left\langle e^{\frac{2i\pi}{n}} \right\rangle$ sont les $\left\langle \left(e^{\frac{2i\pi}{n}}\right)^{\frac{n}{d}} \right\rangle = \left\langle e^{\frac{2i\pi}{d}} \right\rangle = \Gamma_d$ où d est un diviseur de n et il y en a autant que de diviseurs de n.*

Le théorème précédent nous permet de montrer le théorème de Cauchy dans le cas commutatif.

Théorème 1.25 (Cauchy) *Soit G un groupe commutatif fini d'ordre $n \geq 2$. Pour tout diviseur premier p de n il existe dans G un élément d'ordre p.*

Démonstration. On procède par récurrence sur l'ordre $n \geq 2$ de G.

Pour $n = 2$, c'est clair puisque $G = \{1, g\}$ est le seul sous-groupe d'ordre 2.

Supposons le acquis pour les groupes commutatifs d'ordre $m < n$, où $n \geq 3$. On se donne un groupe commutatif G d'ordre n, un diviseur premier p de n et un élément $g \in G \setminus \{1\}$.

Si $G = \langle g \rangle$, alors G est cyclique et g est d'ordre n. Pour tout diviseur premier p de n, l'élément $h = g^{\frac{n}{p}}$ est d'ordre p dans G.

Si $G \neq \langle g \rangle$ et p divise $m = \operatorname{card}(\langle g \rangle) < n$, alors l'hypothèse de récurrence nous assure de l'existence d'un élément h dans $\langle g \rangle$ qui est d'ordre p.

Supposons enfin que $G \neq \langle g \rangle$ et p ne divise pas $m = \operatorname{card}(\langle g \rangle)$. Comme p est premier ne divisant pas m, il est premier avec m et le groupe quotient $G/\langle g \rangle$ est commutatif d'ordre $r = \dfrac{n}{m} < n$ divisible par p (p divise $n = rm$ et p est premier avec m, le théorème de Gauss nous dit alors que p divise r). L'hypothèse de récurrence nous assure alors de l'existence d'un élément $\overline{h}$ d'ordre p dans $G/\langle g \rangle$. Comme l'ordre s de h est multiple de $\theta\left(\overline{h}\right) = p$ (exercice 1.23), $k = h^{\frac{s}{p}}$ est d'ordre p dans G. ∎

Remarque 1.17 *Pour G commutatif non cyclique et d diviseur quelconque de n, il n'existe pas nécessairement d'élément d'ordre d dans G. Par exemple, $G = \left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^3$ est d'ordre 8 avec tous ses éléments distincts du neutre d'ordre 2 et il n'existe pas d'élément d'ordre 4.*
Ou plus simplement, pour G non cyclique et $d = n$, il n'existe pas d'élément d'ordre n.

Remarque 1.18 *En utilisant la décomposition d'un groupe commutatif fini en produit de groupes cycliques, on peut montrer que si G est un groupe commutatif d'ordre $n \geq 2$, alors pour tout diviseur d de n, il existe un sous-groupe de G d'ordre d. En fait si $n = \prod_{k=1}^{r} p_k^{\alpha_k}$ est la décomposition de n en facteurs premiers, le sous-groupe $H_k = \left\{g \in G \mid \theta(g) = p^k \text{ où } k \geq 1\right\}$ est l'unique sous-groupe de G d'ordre $p_k^{\alpha_k}$ (voir Combes, p. 67).*

Exercice 1.38 *Donner une deuxième démonstration du théorème de Cauchy dans le cas commutatif, en utilisant les théorème 1.18 et 1.20.*

Solution 1.38 *Si p est un diviseur premier de n, c'est également un diviseur premier de $\theta(g_0) = \operatorname{ppcm}\{\theta(g) \mid g \in G\}$, soit $\theta(g_0) = pq$ et g_0^q est d'ordre p dans G.*

Le théorème de Cauchy dans le cas général peut se déduire du cas commutatif en utilisant le corollaire 1.8.

Théorème 1.26 (Cauchy) *Si G est un groupe fini d'ordre $n \geq 2$, alors pour tout diviseur premier p de n, il existe dans G un élément d'ordre p.*

Démonstration. On procède par récurrence sur l'ordre n du groupe G.
Pour $n = 2$, $G = \{1, g\}$ est cyclique avec g d'ordre 2.
Supposons le résultat acquis pour les groupes d'ordre strictement inférieur à n et soit G un groupe d'ordre $n \geq 3$. On note p un diviseur premier de n.
Si G admet un sous-groupe H d'ordre $n' < n$ divisible par p, alors H admet un élément d'ordre p par hypothèse de récurrence et cet élément est d'ordre p dans G.
Dans le cas contraire, en écrivant $n = p^\alpha m$ avec $\alpha \geq 1$ et m non divisible par p, si H est un sous-groupe strict de G, son ordre qui divise $p^\alpha m$ et est premier avec p va diviser m et $[G : H] = \dfrac{\operatorname{card}(G)}{\operatorname{card}(H)} = p^\alpha m'$ avec $m' < m$. En faisant agir G sur lui même par conjugaison et en notant $G \cdot h_1, \cdots, G \cdot h_r$ toutes les orbites non réduites à un élément deux à deux distinctes, on déduit que :

$$\operatorname{card}(Z(G)) = \operatorname{card}(G) - \sum_{i=q+1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{h_i})}$$

est divisible par p. Donc $Z(G)$ est un groupe commutatif de cardinal divisible par p, il admet donc un élément d'ordre p qui est d'ordre p dans G. ∎

Exercice 1.39 *On se propose ici de montrer le théorème de Cauchy pour tout groupe fini en utilisant les actions de groupe.*
Soit G un groupe fini de cardinal n et p un diviseur premier de n. On note :

$$E = \{(g_1, \cdots, g_p) \in G^p \mid g_1 \cdots g_p = 1\}$$

1. *Calculer le cardinal de E.*

2. *On désigne par* $H = \langle\sigma\rangle$ *le sous-groupe de* $\mathcal{S}_p$ *engendré par le* p*-cycle* $\sigma = (1, 2, \cdots, p)$. *Montrer que l'application :*

$$\left(\sigma^k, (g_1, \cdots, g_p)\right) \mapsto \left(g_{\sigma^k(1)}, \cdots, g_{\sigma^k(p)}\right)$$

définit une action de H *sur* E.

3. *On note* E^H *l'ensemble des éléments* $x \in E$ *tels que* $H \cdot x = \{x\}$. *Montrer que* $E^H \neq \emptyset$ *et* $\operatorname{card}\left(E^H\right)$ *est divisible par* p.

4. *Déduire de ce qui précède qu'il existe dans* G *un élément d'ordre* p.

Solution 1.39

1. *L'application* $(g_1, \cdots, g_{p-1}) \mapsto \left(g_1, \cdots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1}\right)$ *réalise une bijection de* G^{p-1} *sur* E *(de l'égalité* $g_1 \cdots g_p = 1$, *on déduit que la connaissance des* g_i *pour* $1 \leq i \leq p-1$ *détermine* g_p *de manière unique). On a donc :*

$$\operatorname{card}(E) = n^{p-1}.$$

2. *Pour* $g = (g_1, \cdots, g_p) \in E$, *on a :*

$$g_2 \cdots g_p g_1 = g_1^{-1} g_1 = 1$$

donc $\left(g_{\sigma(1)}, \cdots, g_{\sigma(p)}\right) = (g_2, \cdots, g_p, g_1) \in E$. *Il en résulte que pour tout entier* k *compris entre* 0 *et* $p-1$, $\left(g_{\sigma^k(1)}, \cdots, g_{\sigma^k(p)}\right) \in E$. *L'application :*

$$\left(\sigma^k, (g_1, \cdots, g_p)\right) \mapsto \sigma^k \cdot (g_1, \cdots, g_p) = \left(g_{\sigma^k(1)}, \cdots, g_{\sigma^k(p)}\right)$$

est donc bien une application de $H \times E$ *dans* E. *Cette application définit bien une action puisque :*

$$Id \cdot (g_1, \cdots, g_p) = (g_1, \cdots, g_p)$$

et

$$\begin{aligned}\sigma^j \cdot \left(\sigma^k \cdot (g_1, \cdots, g_p)\right) &= \sigma^j \cdot \left(g_{\sigma^k(1)}, \cdots, g_{\sigma^k(p)}\right) = \left(g_{\sigma^{j+k}(1)}, \cdots, g_{\sigma^{k+j}(p)}\right) \\ &= \sigma^{j+k} \cdot (g_1, \cdots, g_p) = \left(\sigma^j \circ \sigma^k\right) \cdot (g_1, \cdots, g_p)\end{aligned}$$

3. *En remarquant que* $x = (1, \cdots, 1)$ *est dans* E^H, *on déduit que* E^H *est non vide. Comme* H *est de cardinal* p *(un* p*-cycle est d'ordre* p *dans* $\mathcal{S}_p$*), on a :*

$$\operatorname{card}\left(E^H\right) \equiv \operatorname{card}(E) \pmod{p}$$

(corollaire 1.7) avec $\operatorname{card}(E) = n^{p-1}$ *divisible par* p *comme* n, *ce qui entraîne que* $\operatorname{card}\left(E^H\right)$ *est également divisible par* p.

4. *De* $\operatorname{card}\left(E^H\right) \geq 1$ *et* $\operatorname{card}\left(E^H\right)$ *divisible par* p, *on déduit que* $\operatorname{card}\left(E^H\right) \geq p \geq 2$ *et en remarquant que* $x = (g_1, \cdots, g_p) \in E^H$ *équivaut à dire que* $g_1 = \cdots = g_p = g$ *avec* $g \in G$ *tel que* $g^p = 1$, *on déduit qu'il existe* $g \neq 1$ *tel que* $g^p = 1$, *ce qui signifie que* g *est d'ordre* p.