Groupes quotients :

Rappel sur la notion de Relation d'équivalence :

Soit E un ensemble. Une relation R sur E est la donnée d'un sous ensemble $\Gamma_R \subseteq E \times E$.

On dit que $x \in E$ et $y \in E$ sont en relation et on note $x \sim y$ si $(x,y) \in \Gamma_R$

R est dite relation d'équivalence si elle est :

- réflexive : $\forall x \in E,\ x \sim x$.
- symétrique : si $x \sim_R y$ alors $y \sim_R x$
- transitive : si $x \sim y$ et $y \sim z$ alors $x \sim z$.

Exemple : Soit $E = \mathbb{Z}$, la relation définie par $x \sim y \Leftrightarrow x \equiv y \ [2]$ est une relation d'équivalence.

Si $x \in E$, on note $\bar{x} = \{ y \in E \mid x \sim y \}$. On dit que $\bar{x}$ est la classe d'équivalence de x.

⚠ si $y \in \bar{x}$, alors $\bar{x} = \bar{y}$.

Proposition : Les classes d'équivalence de R forment une partition de E. En d'autres termes, il existe un sous ensemble $I \subseteq E$ tels que

$$E = \bigsqcup_{x \in I} \bar{x}$$

(↑ union disjointe)

Preuve :

Montrons que pour $x, y \in E$, soit on a $\bar{x} \cap \bar{y} = \emptyset$ ou $\bar{x} = \bar{y}$. En effet, si $z \in \bar{x} \cap \bar{y}$, alors $z \sim x$ et $z \sim y$ donc $x \sim y$ et $\bar{x} = \bar{y}$. De plus, pour tout $x \in E$, $x \in \bar{x}$ donc E est bien la réunion de toutes les classes d'équivalence. ∎

Soit $(G, \cdot)$ un groupe, et $H \subseteq G$ un sous groupe. On considère la relation R_H sur G :

$$x \sim_H y \iff x^{-1}y \in H \qquad (x, y \in E)$$

Alors R_H est une relation d'équivalence.

Lemme : La classe d'équivalence de $x \in G$ est l'ensemble

$$xH = \{ xh \mid h \in H \}$$

Preuve : Soit $y \in G$ tels que $x \sim y$. Alors il existe $h \in H$ tels que $x^{-1}y = h$. Donc $y = xH$

Réciproquement si $y \in xH$, $y = xH$ avec $h \in H$ donc $x^{-1}y = h \in H$. et $x \sim y$. ∎

Définition : L'ensemble xH s'appelle la classe à gauche de x modulo H. L'ensemble des classes à gauche des éléments de G modulo H se note G/H et s'appelle l'ensemble quotient à gauche de G modulo H. On a ainsi

$$G/H = \{xH ; x \in G\}.$$

On en déduit le théorème de Lagrange qui est à la base de la théorie des groupes finis.

Supposons que G est un groupe fini. Dans ce cas, il en est de même des ensembles H et G/H. Notons $|G|$, $|H|$ et $|G/H|$ leurs cardinaux respectifs.

Théorème (Lagrange)

Supposons G fini. Alors on a l'égalité $|G| = |H| \times |G/H|$.

En particulier, l'ordre de H divise celui de G.

Preuve :

Pour tout $x \in G$, on a une bijection

$$\begin{aligned} \phi_x : H &\xrightarrow{\sim} xH \\ h &\longmapsto xh \end{aligned}$$

ainsi toutes les classes d'équivalence ont le même cardinal.

Comme G est la réunion disjointe de ses classes d'équivalence, et que leur nombre est $|G/H|$, on en déduit le résultat.

Groupe quotient d'un groupe abélien :

Soit $(G,+)$ un groupe abélien. On note par 0 son élément neutre. Soit $H \subseteq G$ un sous-groupe de G.

On munit l'ensemble quotient

$$G/H = \{ x+H \mid x \in G \}$$

d'une structure de groupe de la façon suivante :

- Soient $u, v \in G/H$. alors il existe $x, y \in G$ tels que $u = x+H$ et $v = y+H$. On définit :

$$u \oplus v := x+y+H.$$

autrement dit, $u \oplus v$ est la classe de $x+y$ modulo H.

Il faut vérifier que cette opération est bien définie, c.à.d que $u \oplus v$ ne dépend pas des représentants choisis x et y de u et v. Considérons pour cela des représentants x' et y' de u et v. Donc $x - x' \in H$ et $y - y' \in H$. Comme G est abélien,

$$(x'+y') - (x+y) = (x'-x) + (y'-y) \in H$$

ainsi $x'+y'+H = x+y+H$.

- L'élément neutre de $\oplus$ est $H = 0+H$.
- Pour tout $x \in G$, l'opposé de $x+H$ est $-x+H$.

Remarque : On a un morphisme de groupes :

$$\pi : G \longrightarrow G/H$$
$$x \longmapsto x+H$$

Le groupe additif

Soit $n \in \mathbb{N}^*$. On prend $(G,+) = (\mathbb{Z},+)$ et $H = n\mathbb{Z}$.

On obtient le groupe quotient : $G/H = \mathbb{Z}/n\mathbb{Z}$.

Notons que $x, y \in \mathbb{Z}$, $x \sim_H y \iff x - y \in n\mathbb{Z}$

$\iff x \equiv y \mod n$

Pour tout $x \in \mathbb{Z}$, la classe de x modulo $n\mathbb{Z}$ est

$$x + n\mathbb{Z} = \{x + nk \mid k \in \mathbb{Z}\}$$

on note souvent $\bar{x} = x + n\mathbb{Z}$. Ainsi on a :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

Sous-groupe engendré par un élément, ordre d'un élément

Soit $(G,\cdot)$ un groupe. Pour tout $x \in G$, soit $\langle x \rangle$ le plus petit sous-groupe de G contenant x. Alors on a :

$$\langle x \rangle = \{x^k = \underbrace{x \cdots x}_{k\text{-fois}} \mid k \in \mathbb{Z}\}$$

Définition : On appelle l'ordre de x l'ordre de $\langle x \rangle$ (qui est égal à ∞ si le sous-groupe est infini). Il est parfois noté $\mathrm{ord}(x)$ ou $|x|$.

Théorème : Supposons que G est fini. Soit x un élément de G d'ordre m.

1) On a $m \geq 1$ et m divise $|G|$.

2) On a $x^m = e$ et m est le plus petit entier $k \geq 1$ tels que $x^k = 1$.

3) Les éléments $e, x, \ldots, x^{m-1}$ sont distincts deux à deux

En particulier, on a :

$$\langle x \rangle = \{e, x, \ldots, x^{m-1}\}$$

Preuve :

1) résulte du théorème de Lagrange.

2) Considérons l'ensemble $A \subseteq \mathbb{N}$ défini par

$$A = \{k \in \mathbb{N} \mid 1 \leq k \leq m \text{ et } x^k = e\}$$

Il est non-vide. En effet, si A était vide, alors les éléments

$$x, x^2, \ldots, x^m, x^{m+1}$$

seraient distincts deux à deux et l'ordre de x serait strictement plus grand que m.

Soit u le plus petit élément de A. Il faut montrer que $u = m$.

Posons $B = \{e, x, \ldots, x^{u-1}\}$

Par minimalité de u, on a $\#B = u$.

Vérifions que $\langle x \rangle \subseteq B$. Soit $k \in \mathbb{Z}$, la division euclidienne de k

par u s'écrit :

$$k = uq + r \quad \text{avec} \quad 0 \leq r < u.$$

Comme $x^u = 1$, on a

$$x^k = (x^u)^q x^r = x^r \in B$$

D'où $\langle x \rangle \in B$. Comme $B \subseteq \langle x \rangle$, on a $\langle x \rangle = B$ et $u = m$.

3) cela résulte de la preuve de 2)

■

Théorème : Soit G un groupe fini d'ordre n. Alors pour tout $x \in G$ on a $x^n = 1$.

Preuve : Par le théorème précédent, on a $n = k \cdot m$; $k \in \mathbb{Z}$ si m est l'ordre de x, et on a $x^n = (x^m)^k = 1^k = 1$.

■