Chapitre 2 : Groupes et Quotients

V Ordre

A - Relation définie par un sous-groupe

Soit G un groupe .

Définition V.1
Soit $x \in G$, et H un sous-groupe de G. La classe à gauche *de x modulo H est l'ensemble $xH = \{xh \,|\, h \in H\}$.*

On peut voir que pour tout $x \in G$ et tout $H < G$, on a $x \in xH$. On constate également que $eH = H$.
Remarque : On peut également définir la classe à droite Hx, mais dans ce cours nous ne nous servirons que des classes à gauche

Proposition V.2
Soit $x, y \in G$ et $H < G$. On a $xH = yH$ si et seulement si $x^{-1}y \in H$

Démonstration : Si $y \in xH$, alors $x^{-1}y \in H$ donc il existe $h \in H$ tel que $x^{-1}y = h$ c'est à dire $y = xh$. □

On dit que x et y sont congrus modulo H, lorsque $xH = yH$. On notera $x \underset{H}{\sim} y$ cette relation.

Proposition V.3
Si $G = \mathbb{Z}$ et $H = n\mathbb{Z}$, la relation $\underset{H}{\sim}$ est la congruence habituelle modulo n. C'est à dire que $x \underset{H}{\sim} y$ si et seulement si x et y ont même reste par la division euclidienne par n.

Démonstration : Soit $x, y \in \mathbb{Z}$. On a $x \underset{H}{\sim} y \Leftrightarrow x - y \in n\mathbb{Z}$. Or $x - y \in n\mathbb{Z}$ signifie que $x - y$ est divisible par n et donc que son reste est égal à 0. Et finalement, $x - y \equiv 0 \bmod (n) \Leftrightarrow x \equiv y \bmod (n)$
□

Proposition V.4
Soit G un groupe et H un sous-groupe. La relation $\underset{H}{\sim}$ est une relation d'équivalence sur G.

Démonstration : Une relation d'équivalence est une relation Réflexive, Symétrique et Transitive.

— Soit $x \in G$. On a $xH = xH$. (Réflexive)

— Soit $x, y \in G$. Si $xH = yH$ alors $yH = xH$. (Symétrique)

— Soit $x, y, z \in G$. Si Si $xH = yH$ et $yH = zH$, alors $xH = zH$. (Transitive)

□

Exemple 17 : Dans le groupe $G = \mathbb{C}^*$ on peut prendre $H = \mathbb{U}$ le cercle unité et $x = 4$. Alors la classe à gauche $4\mathbb{U}$ est l'ensemble des nombres complexes $y \in \mathbb{C}$ tels que $\frac{4}{y} \in \mathbb{U}$. On en déduit que $4\mathbb{U}$ est l'ensemble des nombres complexes de module 4

Exemple 18 : Dans $G = (\mathbb{Z}, +)$ on peut prendre l'élément $5 \in \mathbb{Z}$ et le sous-groupe $H = 3\mathbb{Z}$. Alors la classe à gauche est l'ensemble

$$\overline{5} = 5 + 3\mathbb{Z} = \{n \in \mathbb{Z} | \exists h \in 3\mathbb{Z}, n = 5 + h\} = \{3m + 2 | m \in \mathbb{Z}\}$$

qui est l'ensemble des nombres congrus à 2 modulo 3.

Exemple 19 : Dans le cas $G = \mathbb{Z}$ et $H = n\mathbb{Z}$, la classe d'un élément est l'ensemble des éléments ayant le même reste par la division euclidienne par n. Pour tout $k \in \mathbb{Z}$, on notera plutôt ${}^n\overline{k}$ la classe de k modulo n. (cela évite la notation $k + n\mathbb{Z}$ qui est un peu lourde). Lorsqu'il n'y a pas d'ambiguité sur le nombre n, on peut simplement écrire $\overline{k}$.

On voit tout de suite qu'il y a autant de classes d'équivalence modulo n que de restes possibles, c'est à dire n classes distinctes.

On rappelle la propriété suivante des relations d'équivalences.

Proposition V.5
Les classes d'équivalences forment une partition de l'ensemble G

Ceci est vrai pour toute relation d'équivalence. Autrement dit, tout élément de G appartient à une unique classe d'équivalence. Deux classes d'équivalence sont donc soit égales, soit disjointes.

Remarque : Attention, une classe à gauche n'est pas un sous-groupe de G en général. La seule classe à gauche qui soit un sous-groupe est celle de l'élément neutre

Remarque : On peut définir une autre relation d'équivalence à partir de H, avec les classes à droite. Cette relation n'est pas la même a priori.

Définition V.6
On note G/H l'ensemble quotient *du groupe G par la relation d'équivalence* $\underset{H}{\sim}$. *C'est à dire que* $G/H = \{xH | x \in G\}$ *est l'ensemble des classes à gauche.*

Exemple 20 :

— On prends $G = \mathbb{Z}$ et $H = 2\mathbb{Z}$. Dans ce cas, l'ensemble quotient est $\mathbb{Z}/2\mathbb{Z}$ qui est un ensemble à deux éléments, les nombres pairs et les nombres impairs. Cela corresponds aux deux restes possibles par la division euclidienne par 2, c'est à dire 0 et 1.
— De façon générale $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.
— On prends $G = \mathbb{C}^*$ et $H = \mathbb{U}$, on obtient que G/H est l'ensemble des cercles centrés en 0. On voit que cet ensemble est en bijection avec $\mathbb{R}_+^*$ l'ensemble des réels positifs (via l'application qui donne le rayon du cercle).

Définition V.7
Le cardinal de l'ensemble G/H est appelé indice *de H dans G et est noté $[G : H]$.*

Exemple 21 : Le sous-groupe $n\mathbb{Z}$ est d'indice n dans $\mathbb{Z}$.

B - Théorème de Lagrange

Définition V.8
Si G est un groupe fini, on note son cardinal $|G|$. Ce cardinal est parfois appelé ordre du groupe.

Le théorème suivant est un théorème de structure très important. Il donne des informations sur les sous-groupes et les quotients.

Théorème V.9 (de Lagrange)
Soit G un groupe fini et H un sous-groupe de G. Alors :

$$|G| = |H| \times [G : H]$$

Démonstration : Soit $x \in G$, l'application

$$\begin{aligned} \Phi_x : H &\longrightarrow xH \\ h &\longmapsto xh \end{aligned}$$

est une bijection. En effet
• Φ_h est injective car $xh = xh' \Rightarrow h = h'$ par régularité des éléments d'un groupe.
• Φ_h est surjective par définition de l'ensemble xH.
On en déduit que pour tout $x \in G$, on a $\mathrm{Card}(H) = \mathrm{Card}(xH)$. Chaque classe a donc exactement $|H|$ éléments et par définition il y a $[G : H]$ classes.
L'ensemble des classes forme une partition, on en déduit que $|G| = |H| \times [G : H]$. □

Corollaire V.10
Si G est un groupe fini et H est un sous-groupe de G , alors l'ordre de H divise l'ordre de G.

C'est ce corollaire que nous allons utiliser le plus souvent car il donne une contrainte forte sur les sous-groupes qui peuvent exister dans un groupe G.

Exemple 22 : Un groupe d'ordre 16 ne peut pas possèder un sous-groupe d'ordre 3.

C - Ordre des éléments

Définition V.11

Soit G un groupe et $x \in G$. L'ordre de x est le plus petit entier k non-nul tel que $x^k = e$. On note alors $\mathrm{ord}(x) = m$. *Si un tel entier n'existe pas, on dit que x est d'ordre infini.*

Exemple 23 : Dans $\mathbb{C}^*$ muni de la multiplication usuelle, on a

- $\mathrm{ord}(1) = 1$, puisque $1^1 = 1$.
- $\mathrm{ord}(-1) = 2$, en effet $(-1)^2 = 1$.
- $\mathrm{ord}(i) = 4$, en effet $i^4 = 1$ et si $0 < n < 4$ on a $i^n \neq 1$.
- $\mathrm{ord}(2) = \infty$, puisque pour tout $n \geq 1$ on a $2^n \neq 1$.

Exemple 24 : Dans un groupe, l'élément neutre est d'ordre 1 et c'est le seul élément d'ordre 1.

Proposition V.12

Soit G un groupe, et $x \in G$. L'ensemble $\mathrm{Ord}(x) = \{k \in \mathbb{Z} \,|\, x^k = e\}$ *est un sous-groupe de $\mathbb{Z}$.*

L'ordre de x est donc l'unique générateur positif de $\mathrm{Ord}(x)$ *si celui-ci est non nul.*

Démonstration : On a

- $0 \in \mathrm{Ord}(x)$, car $x^0 = e$
- Si $k, l \in \mathrm{Ord}(x)$, alors $x^{k+l} = x^k x^l = ee = e$. Donc $k + l \in \mathrm{Ord}(x)$.
- $x^{-k} = (x^k)^{-1} = e^{-1} = e$. Donc $-k \in \mathrm{Ord}(x)$.

Par minimalité de $\mathrm{ord}(x)$, on a bien $\mathrm{Ord}(x) = \mathrm{ord}(x)\mathbb{Z}$. □

On peut se demander pourquoi le même mot est utilisé pour l'ordre d'un élément et l'ordre d'un sous-groupe.

Proposition V.13

L'ordre d'un élément est égal à l'ordre du sous-groupe engendré par cet élément.

Démonstration : Soit x un élément d'ordre fini de G et on note $n = \mathrm{ord}(x)$. On considère l'application $f : \{0, \ldots, n-1\} \to \langle x \rangle$ définie par $f(i) = x^i$. Cette application est bijective, en effet :

— Soient $i, j \in \{0, \dots, n-1\}$ tels que $f(i) = f(j)$. On suppose sans perte de généralité que $i \geq j$. On a alors $x^i = x^j$ et donc $x^{i-j} = e$. Comme $i - j \in \{0, \dots, n-1\}$ on en déduit que $i - j = 0$. L'application est donc injective.

— Soit $y \in \langle x \rangle$. Alors il existe $k \in \mathbb{Z}$ tel que $x^k = y$. On effectue la division euclidienne de k par n pour obtenir $k = qn + r$ avec $r \in \{0, \dots, n-1\}$. Alors $y = x^{qn+r} = (x^n)^q x^r = x^r = f(r)$. Donc f est surjective.

□

Proposition V.14
Dans un groupe fini, l'ordre d'un élément divise l'ordre du groupe.
En particulier, si G est un groupe d'ordre n, alors $\forall x \in G, x^n = e$

Démonstration : D'après le théorème de Lagrange l'ordre du sous-groupe $\langle x \rangle$ divise l'ordre du groupe. On conclut avec la proposition précédente que l'ordre de x divise l'ordre du groupe.

Comme l'ordre de x, noté m, divise l'ordre du groupe, on en déduit que $n \in m\mathbb{Z}$. Donc $n \in \mathrm{Ord}(x)$ et $x^n = e$. □

Remarque : Il peut y avoir des éléments d'ordre fini dans un groupe infini.

VI Groupe Quotient

Etant donné un groupe G et un sous-groupe H, on voudrait pouvoir définir une loi de composition interne sur l'ensemble G/H à partir de la loi de G, de sorte que G/H soit un groupe. Cependant, cela n'est pas toujours possible. On définit donc une propriété du sous-groupe H dans G qui permet cette construction.

A - Sous-groupe distingué

Définition VI.1
Soit G un groupe et H un sous-groupe de G. On dit que H est un sous-groupe distingué de G si pour tout $g \in G$ et tout $h \in H$, on a $ghg^{-1} \in H$.
On note dans ce cas $H \triangleleft G$.

Proposition VI.2
Si G est un groupe abélien, alors tout sous-groupe de G est distingué dans G.

Démonstration : Dans un groupe abélien, on a $ghg^{-1} = h$ pour tout $g, h \in G$.

□

Exemple 25 :

1. Le sous-groupe trivial $\{e\}$ est distingué dans G.

2. Le sous-groupe G est également distingué dans G.
3. Le sous-groupe $\mathrm{SL}_2(\mathbb{R})$ est distingué dans $\mathrm{GL}_2(\mathbb{R})$. En effet, si $M \in \mathrm{SL}_2(\mathbb{R})$ et $A \in \mathrm{GL}_2(\mathbb{R})$ on a $\det(AMA^{-1}) = \det(A)\det(M)\det(A^{-1}) = 1$.
4. Le sous-groupe des matrices diagonales $\mathcal{D} = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, a, b \in \mathbb{R}^* \right\}$ n'est pas un sous-groupe distingué de $\mathrm{GL}_2(\mathbb{R})$.
   En effet, en prenant $M = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{D}$ et $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ on a

$$AMA^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix} \notin \mathcal{D}$$

Définition VI.3
Soit E un ensemble muni d'une loi de composition interne et $\sim$ une relation d'équivalence. On dit que la relation d'équivalence est compatible avec la loi de E si

$$\forall x, x', y, y' \in E, (x \sim x' \text{ et } y \sim y') \Rightarrow (xy) \sim (x'y')$$

Cette définition nous dit que si la relation d'équivalence est compatible avec la loi alors la classe d'équivalence d'un produit ne depend que des classes d'équivalence des deux éléments, et ne dépend pas des représentants choisis. On peut donc définir une loi induite sur l'ensemble des classes.

Proposition VI.4
Soit H un sous-groupe de G. La relation d'équivalence $\underset{H}{\sim}$ est compatible avec la loi de G si et seulement si H est un sous-groupe distingué de G.

Démonstration : Supposons que $\underset{H}{\sim}$ est compatible avec la loi de G. Soit $x, y \in G$ et $h \in H$. On pose $y' = yh$, de sorte que $y' \underset{H}{\sim} y$. Alors la compatibilité donne que $(xy) \underset{H}{\sim} (xy')$. On en déduit que $(xy)(xy')^{-1} = xyy'^{-1}x^{-1} = xhx^{-1} \in H$. Donc H est distingué dans G.

Réciproquement, supposons que $H \triangleleft G$, et alors soit $x, x', y, y' \in G$ tels que $x \underset{H}{\sim} x'$ et $y \underset{H}{\sim} y'$. Il existe $h \in H$ tel que $xx'^{-1} = h$. De même il existe $k \in H$ tel que $yy'^{-1} = k$. On en déduit

$$(xy)(x'y')^{-1} = x(yy'^{-1})x'^{-1} = xkx'^{-1} = xkx^{-1}xx'^{-1} = xkx^{-1}h$$

Or H est un sous-groupe distingué donc $xkx^{-1} \in H$. On en déduit que $(xy)(x'y')^{-1} \in H$, donc $(xy) \underset{H}{\sim} (x'y')$. La relation est donc bien compatible avec la loi du groupe.

□

Grace à cette proposition, nous pouvons définir une loi, que nous noterons $*$, sur l'ensemble G/H de la façon suivante :

$$\forall x, y \in G, (xH) * (yH) = (xy)H$$

Cette loi est *bien définie.*

Théorème VI.5

Si $H \triangleleft G$, alors l'ensemble G/H muni de cette loi $*$ est un groupe, appelé groupe quotient de G par H.

De plus, l'application de projection canonique $\pi : G \to G/H$ est un morphisme surjectif

Démonstration : Soient xH, yH, zH des éléments de G/H.

- (Associativité) : $(xH * yH) * zH = (xy)H * zH = ((xy)z)H = (x(yz))H = xH * (yz)H = xH * (yH * zH)$
- (Element neutre) : $xH * eH = (xe)H = xH = (ex)H = eH * xH$. Donc eH est un élément neutre de $(G/H, *)$.
- (Inverses) : $xH * x^{-1}H = (xx^{-1})H = eH = (x^{-1}x)H = x^{-1}H * xH$. Donc xH est inversible et $x^{-1}H$ est son inverse.

L'application π est surjective par définition. C'est un morphisme par construction puisque

$$\forall x, y \in G, \pi(xy) = (xy)H = xH * yH = \pi(x) * \pi(y)$$

□

Exemple 26 : Le groupe $\mathbb{Z}$ étant abélien, on en déduit qu'un sous-groupe $n\mathbb{Z}$ est distingué. Donc $\mathbb{Z}/n\mathbb{Z}$ est un groupe pour la loi induite par $+$. On peut regarder la table de $\mathbb{Z}/6\mathbb{Z}$:

$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

B - Théorème d'isomorphisme

On commence par un résultat sur le noyau d'un morphisme

Proposition VI.6

Soit G, G' deux groupes et $f : G \to G'$ un morphisme de groupe. Le noyau $\ker f$ *est un sous-groupe distingué de G.*

Démonstration : On pose $K = \ker(f)$. Soit $k \in K$ et $a \in G$. Alors

$$f(aka^{-1}) = f(a)f(k)f(a^{-1}) = f(a)f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H$$

Donc $aka^{-1} \in K$. Donc $K \triangleleft G$. □

Théorème VI.7 (d'Isomorphisme)
Soit $f : G \to G'$ un morphisme de groupe et $K = \ker(f)$. Alors l'application f passe au quotient par K et l'application induite $\overline{f} : G/K \to G'$ est injective.
Le groupe G/K est donc isomorphe à $\mathrm{Im}(f)$.

Démonstration : On montre d'abord que f passe au quotient. Soient $x, y \in G$ tels que $xK = yK$. On a donc $xy^{-1} \in K$. On en déduit

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

Donc $f(x) = f(y)$. L'application f est donc constante sur chaque classe d'équivalence et passe au quotient.

L'application $\overline{f}$ est un morphisme. En effet, soit $x, y \in G$.

$$\overline{f}(xK * yK) = \overline{f}((xy)K) = f(xy) = f(x)f(y) = \overline{f}(xK)\overline{f}(yK)$$

Le morphisme $\overline{f}$ est injectif. En effet, soit $xK \in \ker \overline{f}$. Alors $\overline{f}(xK) = e = f(x)$. Donc $x \in K$ et $K = eK$. Donc $xK = eK$. □

Exemple 27 :

— $G = (\mathbb{C}^*, \times)$ et $f : G \to \mathbb{R}^{*+}$ le morphisme défini par $f(z) = |z|$. Ce morphisme est surjectif et son noyau est $\mathbb{U}$. Donc on en déduit que $\mathbb{C}^*/\mathbb{U} \simeq \mathbb{R}^{*+}$.

— On prends $G = \mathrm{GL}_2(\mathbb{R})$ et $\det : G \to \mathbb{R}^*$ le déterminant. On sait que det est un morphisme.
$\ker(\det) = \mathrm{SL}_2(\mathbb{R})$, le groupe des matrices de déterminant 1. Et det est surjectif donc $\mathrm{GL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{R})$ est isomorphe à $\mathbb{R}^*$.

VII Groupes de congruence

A - Le groupe $\mathbb{Z}/n\mathbb{Z}$

Le groupe $\mathbb{Z}$ est commutatif, donc $n\mathbb{Z}$ est un sous-groupe distingué de $\mathbb{Z}$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est donc un groupe pour la loi + définie par $\overline{x} + \overline{y} = \overline{x + y}$.

Proposition VII.1
Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique à n éléments

Démonstration : L'element $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ est un générateur. En effet, si $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Alors on peut supposer que $x \in \{0, 1, \ldots, n-1\}$. Donc $x = 1 + \cdots + 1$ et donc $\overline{x} = \overline{1 + \cdots + 1} = \overline{1} + \cdots + \overline{1} \in \langle \overline{1} \rangle$. □

Théorème VII.2

Tout groupe monogène est soit isomorphe à $\mathbb{Z}$, soit isomorphe à un certain $\mathbb{Z}/n\mathbb{Z}$.

Démonstration : Soit G un groupe monogène et x un générateur. On considère l'application $f : \mathbb{Z} \to G$ définie par $f(i) = x^i$. Cette application est un morphisme surjectif.

Si $\ker f = \{0\}$ alors f est également injective et est donc un isomorphisme entre $\mathbb{Z}$ et G.

Supposons maintenant que $\ker f = n\mathbb{Z}$ pour un certain $n \geq 0$. On applique le théorème d'isomorphisme et on obtient $\mathbb{Z}/n\mathbb{Z}$ isomorphe à $\mathrm{Im}(f) = G$. □

Corollaire VII.3

Soit G un groupe d'ordre p avec p premier. Alors G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Démonstration : Voir exercice

□

Exemple 28 : Classification des groupes d'ordre inférieur à 7 :

$$\mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^2,\ \mathbb{Z}/5\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z},\ \mathfrak{S}_3,\ \mathbb{Z}/7\mathbb{Z}$$

B - Théorème chinois

Soient $n, m \in \mathbb{N}$. Pour distinguer les éléments de $\mathbb{Z}/n\mathbb{Z}$ et ceux de $\mathbb{Z}/m\mathbb{Z}$. On note ${}^n\overline{x}$ et ${}^m\overline{x}$ la classe d'un entier $x \in \mathbb{Z}$ dans chacun des deux groupes.

Soit a, n tels que a divise n. Alors l'application

$$\begin{aligned} \phi : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/a\mathbb{Z} \\ {}^n\overline{x} &\longmapsto {}^a\overline{x} \end{aligned}$$

est bien définie. En effet, si ${}^n\overline{x} = {}^n\overline{y}$ alors $x - y \in n\mathbb{Z}$. Comme $n\mathbb{Z} \subset a\mathbb{Z}$, on en déduit que $x - y \in a\mathbb{Z}$. Donc ${}^a\overline{x} = {}^a\overline{y}$.

Remarque : Attention, cette propriété n'est plus vérifiée si a ne divise pas n. Par exemple ${}^4\overline{2} = {}^4\overline{6}$ dans $\mathbb{Z}/4\mathbb{Z}$ mais ${}^3\overline{2} \neq {}^3\overline{6}$ dans $\mathbb{Z}/3\mathbb{Z}$.

Théorème VII.4 (Chinois)

Soient $m, n \in \mathbb{Z}$. Les nombres m et n sont premiers entre eux si et seulement si $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe au groupe produit $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Démonstration : l'application

$$\begin{aligned}\phi : \mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ k &\longmapsto ({}^m\overline{k},\ {}^n\overline{k})\end{aligned}$$

est un morphisme. En effet,

$$\phi(k+k') = ({}^m\overline{k+k'},\ {}^n\overline{k+k'}) = ({}^m\overline{k} + {}^m\overline{k'},\ {}^n\overline{k} + {}^n\overline{k'})$$

Par définition de la loi sur le groupe produit, on en déduit

$$\phi(k+k') = ({}^m\overline{k},\ {}^n\overline{k}) + ({}^m\overline{k'},\ {}^n\overline{k'}) = \phi(k) + \phi(k')$$

Supposons $m \wedge n = 1$, c'est à dire $\langle m, n\rangle = \mathbb{Z}$. Soit $k \in \ker\phi$. Alors ${}^m\overline{k} = \overline{0}$ et ${}^n\overline{k} = \overline{0}$. Donc $k \in m\mathbb{Z} \cap n\mathbb{Z} = (m \vee n)\mathbb{Z} = mn\mathbb{Z}$. Donc $k \in \mathbb{Z}/mn\mathbb{Z}$. D'après le théorème d'isomorphisme $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe à l'image de ϕ. On en déduit que $|\mathrm{Im}(\phi)| = \mathrm{mn}$. Donc $\mathrm{Im}(\phi) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Réciproquement, si $m \wedge n \neq 1$. Alors soit $p = m \vee n < mn$. Soit $(x, y) \in G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Aors $p(x, y) = (px, py) = (0, 0)$. Donc tous les éléments de G sont d'ordre inférieur à mn. Donc G n'est pas cyclique, sinon il aurait un élément d'ordre mn. Donc G n'est pas isomorphe à $\mathbb{Z}/mn\mathbb{Z}$. □

Le théorème suivant, dont la démonstration est hors programme, montre l'importance des groupes $\mathbb{Z}/n\mathbb{Z}$.

Théorème VII.5 de Classification des groupes abéliens finis

Soit G un groupe abélien fini d'ordre N.
Il existe une unique décomposition $N = d_1 d_2 \cdots d_n$ avec $d_n \geq 2$, et d_{i+1} divise d_i telle que :

$$G \text{ est isomorphe à } (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_n\mathbb{Z})$$

On peut donc donner la liste exacte des groupes abéliens d'un ordre donné. Il suffit pour cela de déterminer toutes les décompositions possibles de N comme un produit satisfaisant les hypothèses.

Par exemple, on peut obtenir la liste des groupes abéliens d'ordre 72 en décomposant de toutes les façons différentes 72 en un produit $d_1 d_2 \cdots d_n$. On a

$$72 = 36 \times 2 = 24 \times 3 = 12 \times 6 = 6 \times 6 \times 2$$

On a donc 5 groupes abéliens d'ordre 72 à isomorphisme près.

$$\mathbb{Z}/72\mathbb{Z}\,;\ \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\,;\ \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\,;\ \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\,;\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Chacun de ces groupes peut s'écrire de façon différente (à isomorphisme près) grace au théorème chinois. Par exemple $\mathbb{Z}/72\mathbb{Z} \simeq \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Ou encore $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

C - Le groupe $\mathbb{Z}/n\mathbb{Z}^*$

Proposition VII.6
La relation d'équivalence modulo $n\mathbb{Z}$ est compatible avec la multiplication sur $\mathbb{Z}$.

Démonstration : Soient $x, x', y, y' \in \mathbb{Z}$ tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$. On en déduit que $x - x' \in n\mathbb{Z}$ et que $y - y' \in n\mathbb{Z}$. On en déduit $(xy) - (x'y') = (x - x')y + (y - y')x'$ est également dans $n\mathbb{Z}$. Donc $\overline{xy} = \overline{x'y'}$ □

On a donc bien un ensemble $(\mathbb{Z}/n\mathbb{Z}, \times)$ muni d'une loi de composition interne. Cette loi est bien associative et son élément neutre est $\overline{1}$.

Cependant, $(\mathbb{Z}/n\mathbb{Z}, \times)$ n'est pas un groupe, car $\overline{0}$ n'est pas inversible. En effet, $\forall x \in Z, \overline{0} \times \overline{x} = \overline{0x} = \overline{0} \neq \overline{1}$.

Définition VII.7
On note $\mathbb{Z}/n\mathbb{Z}^*$ le groupe des éléments inversibles pour la multiplication

Proposition VII.8
Un élément $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible pour $\times$ si et seulement si $k \wedge n = 1$.

Démonstration : Soit $k \in \mathbb{Z}$.
$\overline{k}$ est inversible
$\Leftrightarrow$ $\exists \overline{u} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{k} \times \overline{u} = \overline{1}$
$\Leftrightarrow$ $\exists \overline{u} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{ku - 1} = \overline{0}$
$\Leftrightarrow$ $\exists u \in \mathbb{Z}$, $ku - 1$ est divisible par n
$\Leftrightarrow$ $\exists u, v \in \mathbb{Z}$, $ku - 1 = nv$.
$\Leftrightarrow$ k et n sont premiers entre eux.

□

Définition VII.9
L'indicatrice d'Euler, notée $\varphi(n)$, est le cardinal de $\mathbb{Z}/n\mathbb{Z}^*$. En utilisant la proposition précédente on a

$$\varphi(n) = \{k \in \mathbb{N} \,|\, 0 < k < n, k \wedge n = 1\}$$

Exemple 29 :
— $\varphi(5) = |\{1, 2, 3, 4\}| = 4$.
— $\varphi(12) = |\{1, 5, 7, 11\}| = 4$.
— $\varphi(16) = |\{1, 3, 5, 7, 9, 11, 13, 15\}| = 8$.

Théorème VII.10 (d'Euler)

Soit $a, n \in \mathbb{N}$, tels que $a \wedge n = 1$, alors $a^{\phi(n)} \equiv 1 \,\mathrm{mod}\ (\mathrm{n})$

Démonstration : Voir exercice

□

Exemple 30 : Soit $a = 5$ et $n = 16$. Alors $5^8 \equiv 1 \mod (16)$. Autrement dit $5^8 - 1$ est divisible par 16. En effet $5^8 - 1 = 16 \times 24414$.

Exemple 31 : Quel est le chiffre des unités de 7^{222} ?

On cherche à connaitre le reste de la division euclidienne de 7^{222} par 10. Comme $7 \wedge 10 = 1$, et $\phi(10) = 4$, on en déduit que $7^4 \equiv 1 \mod 10$. Comme $222 = 4 \times 55 + 2$, on en déduit $7^{222} = (7^4)^{55} \times 7^2$. En passant dans $\mathbb{Z}/10\mathbb{Z}$, on voit que le chiffre des unités de 7^{222} est le même que celui de 7^2 et donc est 9.

Théorème VII.11 (petit théorème de Fermat)

Soit p un nombre premier et $a \in \mathbb{Z}$. On a $a^p \equiv a \,\mathrm{mod(p)}$

Démonstration : Voir exercice

□

Exemple 32 : Avec $p = 11$ et $a = 2$. Le théorème me dit que $2^{11} - 2$ est divisible par 11 (ce qui n'est pas trivial à première vue). En effet, $2^11 - 2 = 2046 = 11 \times 186$.

En général, le résultat est faux lorsque p n'est pas premier. Par exemple, $3^4 - 3 = 78$ n'est pas divisible par 4.