DM : Algèbre Générale (Structure de groupes)

Partie A : Indice d'un sous-groupe

Soit $(G,\cdot)$ un groupe, et H un sous-groupe de G. On définit sur G une relation d'équivalence (à vérifier quand-même) : $x\mathcal{R}y \Leftrightarrow \exists h \in H$ tel que $y = x.h$. On montre facilement que pour tout $x \in G$, la classe de x est $\dot{x} = x.H$. On pose alors $G/H = \{\dot{x} \text{ tel que } x \in G\}$, appelé ensemble quotient de G par H. L'indice de H dans G, noté $[G : H]$, est éventuellement infinie et définie par $[G : H] = \text{card}(G/H)$.

1. On suppose que H dit distingué dans G ($H \triangleleft G$), i.e., $g.H.g^{-1} \subset H$, $\forall g \in G$.
   Dire comment munir G/H d'une structure de groupe.

2. Montrer que dans, $(\mathbb{R},+)$, on a $[\mathbb{R},\mathbb{Z}] = +\infty$. Considérer les $\dot{x}$, où $x \in]0,1[$.

3. Montrer $(\mathbb{Z},+)$, on a $[\mathbb{Z},n\mathbb{Z}] = n$ et $[\mathbb{Z} : \{0\}] = +\infty$.

4. **Théorème de Lagrange**. On suppose que G est fini.

   a. Montrer que $[G : H]$ est fini, avec $[G : H] = \dfrac{\text{card}(G)}{\text{card}(H)}$.

   b. En déduire que $\text{card}(H)$ divise $\text{card}(G)$.

5. **Formule des indices (Multiplicativité)** : Soit $K \subset H \subset G$ trois sous-groupes emboîtés. Montrer que :$[G : K] = [G : H] \times [H : K]$.

6. **Sous-groupes d'indice 2** : Montrer que tout sous-groupe d'indice 2 dans G est distingué dans G.

Partie B : Action d'un groupe (les basics)

Soit $(G,.)$ un groupe et X un ensemble non vide.

- Une action (à gauche) de G sur X est une application $\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g,x) & \longmapsto & g \cdot x \end{array}$, vérifiant les deux axiomes :
  - $\forall x \in X, \quad e_G \cdot x = x$
  - $\forall g,h \in G, \forall x \in X, \quad (gh) \cdot x = g \cdot (h \cdot x)$
- Pour tout $x \in X$, $\mathcal{O}(x) = G \cdot x = \{g \cdot x \mid g \in G\} \subset X$, désigne l'orbite de x.
- Pour tout $x \in X$, $\text{Stab}(x) = G_x = \{g \in G \mid g \cdot x = x\} \subset G$, désigne le stabilisateur de x.
- Pour tout $g \in G$, on pose $X^g = \text{Fix}(g) = \{x \in X \mid g \cdot x = x\} \subset X$.
- On pose aussi $X^G = \text{Fix}(G) = \{x \in X \mid \forall g \in G, g \cdot x = x\} \subset X$.
- L'action est dite libre quand $\forall x \in X, \quad \text{Stab}(x) = \{e\}$.
- L'action est dite transitive s'il n'y a qu'une seule orbite : $X = \mathcal{O}(x), \forall x \in X$.
- L'action est dite simplement transitive, quand elle est à la fois transitive et libre.

1. Montrer que définir une action de G sur X équivaut à définir un morphisme de groupes $\phi : G \longrightarrow \mathfrak{S}(X)$, où $\mathfrak{S}(X)$ est le groupe des bijections de X dans lui-même.

2. Montrer alors que $\ker(\phi) = \bigcap_{x \in X} \text{Stab}(x)$.

3. Montrer que la relation $x \sim y \iff \exists g \in G, y = g \cdot x$ est une relation d'équivalence sur X, dont les classes d'équivalence sont les orbites $\mathcal{O}(x)$.

4. Montrer que l'action est fidèle si et seulement si ϕ est injectif.
5. Montrer que l'action est transitive $\Leftrightarrow \forall x, y \in X, \exists g \in G,$ tel que $y = g \cdot x$.
6. Montrer que l'action est simplement transitive si et seulement si $\forall x, y \in X, \exists! g \in G,$ tel que $y = g \cdot x$.

Partie C : Action d'un groupe (les classics)

Soit $(G, .)$ un groupe qui agit sur X un ensemble fini non vide.

1. Fixons $x \in X$ et posons $H = \text{Stab}(x)$. Notons $G/H = \{gH \mid g \in G\}$ et considérons l'application : $f : \begin{array}{ccc} G/H & \longrightarrow & \mathcal{O}(x) \\ gH & \longmapsto & g \cdot x \end{array}$.
   Montrer que f est bien définie et bijective.
2. En déduire que $|\mathcal{O}(x)| = \dfrac{|G|}{|\text{Stab}(x)|}, \forall x \in X$ (**Théorème Orbite-Stabilisateur**).
3. soit $\mathcal{R} \subset X$ est un système de représentants des différentes orbites X.
   Montrer que $|X| = \displaystyle\sum_{x \in \mathcal{R}} |\mathcal{O}(x)| = \sum_{x \in \mathcal{R}} \frac{|G|}{|\text{Stab}(x)|}$ (**Formule des orbites**).
4. Soit $(G, *)$ un groupe fini de cardinal n, qui agit sur lui-même par translation à gauche $(g \cdot x = g * x)$.
   a. Montrer que cette action est libre, fidèle et transitive.
   b. En déduire que G est isomorphe à $\mathfrak{S}_n$ (**Théorème de Cayley**).

Partie D : Lemme de Burnside

Soit G un groupe fini agissant sur un ensemble fini X.
$X/G|$ désigne le nombre d'orbites de cette action.
Considérons l'ensemble $E = \{(g, x) \in G \times X \mid g \cdot x = x\}$.

1. Vérifier que $|E| = \displaystyle\sum_{g \in G} |X^g| = \sum_{x \in X} |\text{Stab}(x)|$.
2. En déduire que $|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$.
   ☞ **Indication** : Utiliser le théorème orbite-stabilisateur

Partie E : Théorème de Cauchy

Soient G un groupe fini et p un nombre premier divisant l'ordre de G.
Soit $X = \{(x_1, \ldots, x_p) \in G^p \mid x_1.x_2 \cdots x_p = e\}$.
On fait agir le groupe $\mathbb{Z}/p\mathbb{Z}$ sur X par décalage circulaire, par exemple

☞ $\dot{1} \cdot (x_1, x_2, \ldots, x_p) = (x_2, \ldots, x_p, x_1)$

☞ $\dot{2} \cdot (x_1, x_2, \ldots, x_p) = (x_3, \ldots, x_1, x_2)$

1. Donner la forme générale de $\dot{k} \cdot (x_1, x_2, \ldots, x_p)$.
2. Justifier que $|X| = |G|^{p-1}$.
3. Justifier que p divise $\mathcal{O}(x), \ \forall x \in X \setminus \text{Fix}(\mathbb{Z}/p\mathbb{Z})$.
4. En déduire que p divise $|\text{Fix}(\mathbb{Z}/p\mathbb{Z})|$.
   ☞ **Indication** : Utiliser la formule des orbites.
5. Vérifier que $\text{Fix}(\mathbb{Z}/p\mathbb{Z}) = \{(x, x, \ldots, x) \in G^p$ tel que $x^p = e\}$
6. Vérifier que $\text{Fix}(\mathbb{Z}/p\mathbb{Z})$ est non vide, puis en déduire que $|F| \geq p \geq 2$.
7. En déduire qu'il existe donc au moins un élément $x \neq e$ tel que $x^p = e$.
8. Conclure alors G contient au moins un élément d'ordre p.

Corrigé

Partie A : Indice d'un sous-groupe

(1) On munit l'ensemble quotient G/H d'une structure de groupe à l'aide de la loi induite définie par

$$\dot{x} \cdot \dot{y} = \widehat{x \cdot y}$$

- **Justification de la bonne définition :** Soient $x, x' \in \dot{x}$ et $y, y' \in \dot{y}$. On a $x' = xh_1$ et $y' = yh_2$ avec $h_1, h_2 \in H$. Le produit s'écrit $x'y' = xh_1yh_2 = xy(y^{-1}h_1y)h_2$. Comme $H \triangleleft G$, l'élément $h_3 = y^{-1}h_1y \in H$, donc $x'y' = xy(h_3h_2) \in xyH = \dot{xy}$. La loi quotient ne dépend donc pas des représentants choisis.
- le reste associativité, élément neutre et inversibilité (à faire)

(2) Pour $x \in]0,1[$, la classe d'équivalence de x modulo $\mathbb{Z}$ est $\dot{x} = x + \mathbb{Z} = \{x + k \mid k \in \mathbb{Z}\}$.

Soient $x, y \in]0,1[$ avec $x \neq y$. Supposons $\dot{x} = \dot{y}$. Alors $x - y \in \mathbb{Z}$. Or, $x, y \in]0,1[\implies -1 < x-y < 1$. Le seul entier dans l'intervalle $]-1,1[$ étant 0, on a $x-y = 0 \implies x = y$, ce qui est contradictoire.

Les classes $(\dot{x})_{x \in]0,1[}$ sont deux à deux distinctes dans $\mathbb{R}/\mathbb{Z}$. L'application $x \mapsto \dot{x}$ est donc une injection de $]0,1[$ dans $\mathbb{R}/\mathbb{Z}$. Puisque $]0,1[$ est infini non dénombrable, $[\mathbb{R} : \mathbb{Z}] = \text{card}(\mathbb{R}/\mathbb{Z}) = +\infty$.

(3)
- Par la division euclidienne, tout $a \in \mathbb{Z}$ s'écrit de manière unique $a = nq + r$ avec $r \in \{0, 1, \ldots, n-1\}$. On a donc $a \equiv r \pmod{n}$, c'est-à-dire $\dot{a} = \dot{r}$. Les classes distinctes sont exactement $\{\dot{0}, \dot{1}, \ldots, \dot{n-1}\}$, d'où $[\mathbb{Z} : n\mathbb{Z}] = n$.
- Pour $H = \{0\}$, la relation d'équivalence est $x \mathcal{R} y \iff x - y \in \{0\} \iff x = y$. Chaque classe est un singleton $\dot{x} = \{x\}$. L'ensemble quotient $\mathbb{Z}/\{0\}$ est en bijection avec $\mathbb{Z}$, d'où $[\mathbb{Z} : \{0\}] = \text{card}(\mathbb{Z}) = +\infty$.

(4) **a** Les classes à gauche $\dot{x} = xH$ forment une **partition** du groupe fini G :

$$G = \bigsqcup_{i=1}^{[G:H]} x_i H$$

Pour chaque $x \in G$, l'application $h \mapsto xh$ est une bijection de H sur xH, donc $\text{card}(xH) = \text{card}(H)$. Toutes les classes possédant le même cardinal $\text{card}(H)$ et étant disjointes :

$$\text{card}(G) = \sum_{i=1}^{[G:H]} \text{card}(x_i H) = [G : H] \times \text{card}(H) \implies [G : H] = \frac{\text{card}(G)}{\text{card}(H)}$$

b Puisque $[G : H] = \text{card}(G/H)$ est un nombre entier, la formule précédente implique directement que $\text{card}(\mathbf{H})$ divise $\text{card}(\mathbf{G})$.

(5) Soient $K \subset H \subset G$ trois sous-groupes d'un groupe G.

- Partition de G par H : $G = \bigsqcup_{i \in I} g_i H$ avec $|I| = [G : H]$.
- Partition de H par K : $H = \bigsqcup_{j \in J} h_j K$ avec $|J| = [H : K]$.

En injectant la décomposition de H dans celle de G :

$$G = \bigsqcup_{i \in I} g_i \left(\bigsqcup_{j \in J} h_j K \right) = \bigsqcup_{(i,j) \in I \times J} (g_i h_j) K$$

Si $(g_i h_j)K = (g_{i'} h_{j'})K$, alors $g_i h_j \in g_{i'} h_{j'} K \subset g_{i'} H$. Ainsi $g_i H \cap g_{i'} H \neq \emptyset \implies i = i'$, puis $h_j K = h_{j'} K \implies j = j'$.

Les classes $(g_i h_j K)$ sont disjointes et au nombre de $|I| \times |J|$. On en déduit que $[G : K] = |I \times J| = |I| \times |J|$, soit :

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

Au fait on définit l'application basée sur la décomposition en classes à gauche présentée dans l'image :

$$\theta : I \times J \longrightarrow G/K$$

$$(i,j) \longmapsto (g_i h_j)K$$

- **Injectivité :** Soient $(i,j),(i',j') \in I \times J$ tels que $\theta(i,j) = \theta(i',j')$. On a :

$$(g_i h_j)K = (g_{i'} h_{j'})K \implies g_i h_j \in g_{i'} h_{j'} K \subset g_{i'} H$$

  Ainsi, $g_i h_j \in g_i H \cap g_{i'} H \neq \emptyset \implies g_i H = g_{i'} H \implies i = i'$.
  L'égalité initiale devient $(g_i h_j)K = (g_i h_{j'})K$. En simplifiant par g_i^{-1} à gauche, on obtient $h_j K = h_{j'} K \implies j = j'$.
  Donc $(i,j) = (i',j')$, ce qui montre que θ est injective.

- **Surjectivité :** Soit $xK \in G/K$ avec $x \in G$.
  (a) Comme $G = \bigsqcup_{i \in I} g_i H$, il existe un unique $i \in I$ tel que $x \in g_i H$, d'où $g_i^{-1} x \in H$.
  (b) Comme $H = \bigsqcup_{j \in J} h_j K$, il existe un unique $j \in J$ tel que $g_i^{-1} x \in h_j K$.
  On en déduit $x \in g_i h_j K$, c'est-à-dire $xK = (g_i h_j)K = \theta(i,j)$. θ est donc surjective.

θ étant une bijection, les ensembles $I \times J$ et G/K ont même cardinalité :

$$[G : K] = |G/K| = |I \times J| = |I| \times |J| = [G : H] \times [H : K]$$

6 Soit H un sous-groupe de G tel que $[G : H] = 2$.

(a) L'ensemble des classes à gauche G/H contient 2 classes : H et son complémentaire $G \setminus H$. Ainsi, pour tout $g \notin H$, la classe à gauche est $gH = G \setminus H$.

(b) L'ensemble des classes à droite contient H et $G \setminus H$. Pour tout $g \notin H$, la classe à droite est $Hg = G \setminus H$.

(c) Pour tout $g \in G$:
- Si $g \in H$, alors $gH = H = Hg$.
- Si $g \notin H$, alors $gH = G \setminus H = Hg$.

Dans tous les cas, $\forall g \in G,\ gH = Hg \iff gHg^{-1} = H$. H est donc distingué dans G.

Partie B : Action d'un groupe (les basics)

1 .
($\Leftarrow$) : Soit $\cdot : G \times X \to X$ une action. Pour tout $g \in G$, on définit $\phi(g) : X \to X$ par $\phi(g)(x) = g \cdot x$.

- ☞ L'égalité $\phi(g) \circ \phi(g^{-1}) = \phi(gg^{-1}) = \phi(e) = \mathrm{id}_X$ prouve que $\phi(g) \in \mathfrak{S}(X)$.
- ☞ L'égalité $\phi(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = (\phi(g) \circ \phi(h))(x)$ montre que ϕ est un morphisme.

($\Rightarrow$) : Soit $\phi : G \to \mathfrak{S}(X)$ un morphisme. On pose $g \cdot x = \phi(g)(x)$.

- $e \cdot x = \phi(e)(x) = \mathrm{id}_X(x) = x$.
- $(gh) \cdot x = \phi(gh)(x) = (\phi(g) \circ \phi(h))(x) = g \cdot (h \cdot x)$.

2 Par définition du noyau :

$$\ker(\phi) = \{g \in G \mid \phi(g) = \mathrm{id}_X\}$$

Or :

$$\phi(g) = \mathrm{id}_X \iff \forall x \in X,\ g \cdot x = x \iff \forall x \in X,\ g \in \mathrm{Stab}(x)$$

Ainsi :

$$\ker(\phi) = \bigcap_{x \in X} \mathrm{Stab}(x)$$

3 Soit $x \sim y \iff \exists g \in G,\ y = g \cdot x$.

- **Réflexivité :** $x = e \cdot x \implies x \sim x$.
- **Symétrie :** $y = g \cdot x \implies x = g^{-1} \cdot y \implies y \sim x$.
- **Transitivité :** $y = g \cdot x$ et $z = h \cdot y \implies z = (hg) \cdot x \implies x \sim z$.

La classe d'équivalence de x est $\bar{x} = \{g \cdot x \mid g \in G\} = \mathcal{O}(x)$, l'orbite de x.

④ Par définition, l'action de G sur X est fidèle si :

$$(\forall x \in X,\ g \cdot x = x) \implies g = e$$

Or, la condition $\forall x \in X,\ g \cdot x = x$ s'écrit $\phi(g) = \mathrm{id}_X$, c'est-à-dire $g \in \ker(\phi)$.

L'action est donc fidèle si et seulement si $\ker(\phi) = \{e\}$. Comme ϕ est un morphisme de groupes, cela équivaut à la propriété que ϕ **est injectif**.

⑤ L'action est transitive si et seulement si X ne forme qu'une seule orbite sous l'action de G.

⇒ Si l'action est transitive, pour tout $x \in X$, l'orbite $\mathcal{O}(x) = \{g \cdot x \mid g \in G\}$ est égale à X. Ainsi, pour tout $y \in X$, $y \in \mathcal{O}(x)$, d'où l'existence d'un $g \in G$ tel que $y = g \cdot x$.

⇐ Supposons que $\forall x, y \in X, \exists g \in G,\ y = g \cdot x$. Pour un $x \in X$ fixé, tout $y \in X$ appartient à $\mathcal{O}(x)$, donc $X = \mathcal{O}(x)$. L'action est bien transitive.

⑥ Une action est simplement transitive si elle est à la fois transitive et libre ($\forall x \in X$, $\mathrm{Stab}(x) = \{e\}$).

⇒ La transitivité donne l'existence d'un $g \in G$ tel que $y = g \cdot x$. Si $g_1 \cdot x = g_2 \cdot x = y$, alors $g_2^{-1} g_1 \cdot x = x$, donc $g_2^{-1} g_1 \in \mathrm{Stab}(x) = \{e\}$, ce qui implique $g_1 = g_2$. D'où l'unicité de g.

⇐ L'existence de g assure la transitivité. De plus, si $g \in \mathrm{Stab}(x)$, alors $g \cdot x = x = e \cdot x$. L'unicité de l'élément envoyant x sur x impose $g = e$. Le stabilisateur de tout élément est donc réduit à $\{e\}$, l'action est libre et donc simplement transitive.

Partie C : Action d'un groupe (les classics)

① ☞ **Bonne définition :** Soient $g_1, g_2 \in G$ tels que $g_1 H = g_2 H$. Alors $g_2^{-1} g_1 \in H = \mathrm{Stab}(x)$, d'où $(g_2^{-1} g_1) \cdot x = x$, ce qui donne $g_1 \cdot x = g_2 \cdot x$. Ainsi $f(g_1 H) = f(g_2 H)$.

☞ **Injectivité :** Si $f(g_1 H) = f(g_2 H)$, alors $g_1 \cdot x = g_2 \cdot x \implies g_2^{-1} g_1 \cdot x = x \implies g_2^{-1} g_1 \in \mathrm{Stab}(x) = H$. D'où $g_1 H = g_2 H$.

☞ **Surjectivité :** Pour tout $y \in \mathcal{O}(x)$, il existe $g \in G$ tel que $y = g \cdot x = f(gH)$.

Par conséquent, f est une **bijection**.

② Par bijectivité de f, $|\mathcal{O}(x)| = |G/H|$. D'après le théorème de Lagrange appliqué au sous-groupe $H = \mathrm{Stab}(x)$:

$$|\mathcal{O}(x)| = \frac{|G|}{|\mathrm{Stab}(x)|}, \quad \forall x \in X$$

③ Les orbites forment une partition de X. Si $\mathcal{R}$ est un système de représentants des orbites, alors $X = \bigsqcup_{x \in \mathcal{R}} \mathcal{O}(x)$. Par additivité du cardinal :

$$|X| = \sum_{x \in \mathcal{R}} |\mathcal{O}(x)| = \sum_{x \in \mathcal{R}} \frac{|G|}{|\mathrm{Stab}(x)|}$$

④ **a.**
- **Libre :** $g \cdot x = x \iff g * x = x \iff g = e$. Donc $\mathrm{Stab}(x) = \{e\}$.
- **Fidèle :** $\ker(\phi) = \bigcap_{x \in G} \mathrm{Stab}(x) = \{e\}$.
- **Transitive :** Pour tous $x, y \in G$, en posant $g = y * x^{-1}$, on a $g \cdot x = y$.

b. L'application $\phi : G \to \mathfrak{S}(G)$ définie par $\phi(g)(x) = g * x$ est un morphisme de groupes. L'action étant fidèle, ϕ est injectif. Ainsi, $G \simeq \mathrm{Im}(\phi) \leq \mathfrak{S}(G) \simeq \mathfrak{S}_n$.
Tout groupe fini d'ordre n est donc isomorphe à un sous-groupe de $\mathfrak{S}_n$ (**Théorème de Cayley**).

Partie D : Lemme de Burnside

① Pour $x \in X$ fixé, $\{g \in G \mid (g, x) \in E\} = \mathrm{Stab}(x)$. Par Fubini discret :

$$|E| = \sum_{x \in X} |\mathrm{Stab}(x)|$$

D'où l'égalité :

$$|E| = \sum_{g \in G} |X^g| = \sum_{x \in X} |\mathrm{Stab}(x)|$$

(2) D'après la question précédente et le théorème Orbite-Stabilisateur ($|\text{Stab}(x)| = \frac{|G|}{|\mathcal{O}(x)|}$) :

$$\sum_{g\in G} |X^g| = \sum_{x\in X} \frac{|G|}{|\mathcal{O}(x)|} = |G| \sum_{x\in X} \frac{1}{|\mathcal{O}(x)|}$$

En décomposant la somme sur X selon la partition formée par l'ensemble X/G des orbites :

$$\sum_{x\in X} \frac{1}{|\mathcal{O}(x)|} = \sum_{\Omega\in X/G} \left(\sum_{x\in\Omega} \frac{1}{|\Omega|} \right) = \sum_{\Omega\in X/G} 1 = |X/G|$$

En réinjectant ce résultat, on obtient $|E| = |G| \cdot |X/G|$, d'où la formule de Burnside :

$$|X/G| = \frac{1}{|G|} \sum_{g\in G} |X^g|$$

Partie E : Théorème de Cauchy

(1) L'action de $\mathbb{Z}/p\mathbb{Z}$ sur X est le décalage circulaire :

$$\dot{k} \cdot (x_1, x_2, \ldots, x_p) = (x_{1+k}, x_{2+k}, \ldots, x_{p+k})$$

où les indices sont calculés modulo p dans $\{1, \ldots, p\}$.

(2) Un élément $(x_1, \ldots, x_p) \in G^p$ appartient à X si et seulement si $x_p = (x_1 \cdots x_{p-1})^{-1}$. Les $p-1$ premiers éléments sont choisis de façon indépendante dans G, ce qui donne :

$$|X| = |G|^{p-1}$$

(3) Par le théorème Orbite-Stabilisateur, $|\mathcal{O}(x)| = \frac{p}{|\text{Stab}(x)|}$. Comme $\text{Stab}(x)$ est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$ (d'ordre premier p), son cardinal est 1 ou p. Si $x \notin \text{Fix}(\mathbb{Z}/p\mathbb{Z})$, alors $\text{Stab}(x) \neq \mathbb{Z}/p\mathbb{Z}$, donc $|\text{Stab}(x)| = 1$ et $|\mathcal{O}(x)| = p$. Par conséquent, p divise $|\mathcal{O}(x)|$.

(4) Notons $F = \text{Fix}(\mathbb{Z}/p\mathbb{Z})$. La formule des orbites s'écrit :

$$|X| = |F| + \sum_{x\in\mathcal{R}\setminus F} |\mathcal{O}(x)|$$

p divise $|G|$, donc p divise $|X| = |G|^{p-1}$. De plus, p divise chaque terme $|\mathcal{O}(x)|$ pour $x \notin F$. On en déduit que p divise $|F|$.

(5) $(x_1, \ldots, x_p) \in \text{Fix}(\mathbb{Z}/p\mathbb{Z}) \iff x_1 = x_2 = \cdots = x_p = x$. La condition $x_1 \cdots x_p = e$ devient $x^p = e$. D'où :

$$\text{Fix}(\mathbb{Z}/p\mathbb{Z}) = \{(x, x, \ldots, x) \in G^p \mid x^p = e\}$$

(6) Le p-uplet $(e, \ldots, e) \in F$, donc $F \neq \emptyset$ ($|F| \geq 1$). Puisque p divise $|F|$, on a nécessairement $|F| \geq p \geq 2$.

(7) Comme $|F| \geq 2$, il existe au moins un élément non trivial $(x, x, \ldots, x) \in F$ avec $x \neq e$, satisfaisant $x^p = e$.

(8) Soit $x \in G \setminus \{e\}$ tel que $x^p = e$. L'ordre de x divise p. Comme p est premier et $x \neq e$, l'ordre de x est exactement p. G **contient donc au moins un élément d'ordre p.**

FiN