Leçon 104 : Groupes abéliens et non abéliens finis. Exemples et applications.

Dans l'ensemble de la leçon, si rien n'est précisé G désigne un groupe fini.

I - Notion d'ordre

Définition 1.1 On dit que $x \in G$ est d'ordre fini si le sous-groupe $\langle x \rangle$ est fini. Le cas échéant, on dit que l'ordre de x est l'ordre de $\langle x \rangle$ et on le note $\mathrm{ord}(x)$.

Proposition 1.2 Soit $x \in G$ alors $\mathrm{ord}(x) = \min \{ k \in \mathbb{N}^* \mid x^k = e \}$.

Exemples 1.3
- $\bar{1}$ est d'ordre n dans $(\mathbb{Z}_n, +)$ avec $n \geq 2$
- le neutre d'un groupe est d'ordre 1
- $\begin{pmatrix} -\bar{1} & 0 \\ 0 & -\bar{1} \end{pmatrix}$ est d'ordre 2 dans $GL_2(\mathbb{Z}_3)$

Définition 1.4 Soit H un sous-groupe de G, on appelle indice de H dans G, le cardinal de l'ensemble quotient G/H. On le note $[G:H]$.

Théorème 1.5 (Lagrange) Soit H un sous-groupe de G, on a alors : $|G| = [G:H]|H|$.

Conséquence 1.6 Ainsi, l'ordre de tout sous-groupe de G divise l'ordre de G. En particulier, l'ordre de tout élément de G divise l'ordre de G.

Application 1.7 Tous les éléments différents du neutre d'un groupe d'ordre p premier sont d'ordre p.

Définition 1.8 On appelle exposant de G, noté $\exp(G)$, le plus petit entier $n \in \mathbb{N}^*$ qui vérifie que pour tout $x \in G$, $x^n = e$.

Proposition 1.9 On a $\exp(G) = \mathrm{ppcm} \{ \mathrm{ord}(x) \mid x \in G \}$.

Proposition 1.10 Si G est un groupe abélien alors il admet un élément d'ordre $\exp(G)$.

Exemples 1.11
- $\exp(\mathbb{Z}_3) = 3$
- $\exp(\mathfrak{S}_3) = 6$
- $\exp(D_8) = 4$

Théorème 1.12 (Burnside) Soit H un sous-groupe de $GL_n(\mathbb{C})$, d'exposant fini, alors H est d'ordre fini.

II - Actions de groupes

Définition 2.1. Soit X un ensemble quelconque. On appelle action de G sur X toute application $G \times X \longrightarrow X$, $(g, x) \longmapsto g \cdot x$ vérifiant :
(i) $\forall x \in X, e \cdot x = x$
(ii) $\forall g, g' \in G, \forall x \in X, g \cdot (g' \cdot x) = (gg') \cdot x$
On dit alors que G opère sur X.

Remarque 2.2 Il revient au même de se donner un morphisme $\varphi : G \longrightarrow \mathfrak{S}(X)$, on pose alors $g \cdot x = \varphi(g)(x)$.

Exemples 2.3
- G agit sur lui-même par conjugaison : $(g, g') \in G \times G \longmapsto g \cdot g' = gg'g^{-1}$
- G agit sur lui-même par translation à gauche : $(g, g') \in G \times G \longmapsto g \cdot g' = gg'$
- $\langle r \rangle$ agit sur $\mathbb{U}_n$

Application 2.4 (Théorème de Cayley) G est isomorphe à un sous-groupe de $\mathfrak{S}(G)$

Définition 2.5 Si G opère sur un ensemble X, on définit pour $x \in X$:
(i) le stabilisateur de x : $\mathrm{Stab}(x) := \{ g \in G \mid g \cdot x = x \}$
(ii) l'orbite de x : $O_x := \{ g \cdot x \mid g \in G \}$

Proposition 2.6 Pour tout $x \in X$, $\mathrm{Stab}(x)$ est un sous-groupe de G.

Lemme 2.7 (Équation aux classes) Si G agit sur un ensemble X et si X est fini, alors $|X| = \sum_{x \in \mathcal{R}} |O_x|$ où $\mathcal{R}$ est un système de représentants des orbites.

Remarque 2.8 On obtient ainsi $|X| = \sum_{x \in \mathcal{R}} \frac{|G|}{|\mathrm{Stab}\, x|}$

Application 2.9 Le centre de tout p-groupe est non trivial.

Application 2.10 Tout groupe d'ordre p^2 est abélien.

Application 2.11 Le groupe diédral D_{2n}, des isométries préservant les polygônes réguliers à n côtés, est d'ordre $2n$.

III - Groupes abéliens finis

Définition 3.1 Un groupe est dit cyclique s'il est monogène fini.

Proposition 3.2 Tout groupe monogène est abélien.

Remarque 3.3 Ainsi, en particulier tout groupe cyclique est abélien.

Proposition 3.4 Si G est cyclique d'ordre n alors $G \simeq \mathbb{Z}_n$.

Application 3.5 Tout groupe d'ordre premier p est cyclique donc isomorphe à $\mathbb{Z}_p$.

Proposition 3.6 Tout groupe cyclique admet, pour tout diviseur d de $|G|$, un unique sous groupe d'ordre d.

Exemples 3.7
- $\mathbb{U}_n = \{ e^{2ik\pi/n} \mid k \in [\![0, n-1]\!] \}$
- $(\mathbb{Z}_{17}^*, \cdot)$
- $\mathbb{Z}$ n'est pas cyclique car infini

Proposition 3.8 Tout sous-groupe d'un groupe cyclique est cyclique.

Théorème 3.9 (Théorème chinois) Soient $n, m \in \mathbb{N}^*$ premiers entre eux alors $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$.

Lemme 3.10 Soient G un groupe abélien fini et H un sous-groupe de G. Alors tout caractère χ de H se prolonge en un caractère de G.

Théorème 3.11 (Théorème de structure des groupes abéliens finis) Soit G un groupe abélien fini non trivial. Il existe alors $r \geq 1$ et $n_1, \dots, n_r \geq 2$ vérifiant $n_i \mid n_{i+1}$, tels que $G \simeq \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$. De plus, il y a unicité des entiers i et n_i.

développement 1

Application 3.12 Tout groupe d'ordre p^2, avec p premier, est isomorphe à $\mathbb{Z}_p \times \mathbb{Z}_p$ ou à $\mathbb{Z}_{p^2}$.

Exemples 3.13
- $\mathbb{Z}_{150} \simeq \mathbb{Z}_5 \times \mathbb{Z}_{30}$
- $\mathbb{U}_4 \times \mathbb{U}_2^2 \times \mathbb{U}_9 \times \mathbb{U}_3 \times \mathbb{U}_5 \simeq \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{180}$

IV - Groupes remarquables

1. Les p-Sylow

Définition 4.1 Soit p un nombre premier. Si $|G| = p^\alpha m$, avec $\alpha \geq 1$ et $p \nmid m$, on appelle p-sous groupe de Sylow, ou p-Sylow, de G, tout sous-groupe d'ordre p^α.

Exemple 4.2
$|GL_n(\mathbb{F}_p)| = (p^n - 1) \dots (p^n - p^{n-1}) = p^{n(n-1)/2} \prod_{k=1}^{n} (p^k - 1)$
$H = \{ M = (m_{ij})_{ij} \in GL_n(\mathbb{F}_p) \mid m_{ij} = \bar{0} \text{ si } i > j \text{ et } m_{ii} = \bar{1} \}$ est un p-Sylow de $GL_n(\mathbb{F}_p)$

Lemme 4.3 Soit G un groupe d'ordre $p^\alpha m$, avec $\alpha \geq 1$ et $p \nmid m$, et soit H un sous-groupe de G. Si G admet un p-Sylow P alors il existe $g \in G$ tel que gPg^{-1} soit un p-Sylow de H.

Conséquence 4.4 G admet un p-Sylow.

Théorème 4.5 (Théorème de Sylow) Soit G un groupe fini d'ordre $p^\alpha m$, avec p premier, $\alpha \geq 1$ et $p \nmid m$, alors :
(i) tout sous-groupe de G est contenu dans un p-Sylow
(ii) les p-Sylow sont conjugués
(iii) si n_p est le nombre de p-Sylow, $n_p \equiv 1 \ [p]$ et $n_p \mid m$

Exemple 4.6
- un groupe d'ordre 63 n'est pas simple
- un groupe d'ordre 33 est cyclique

2. Groupe symétrique

Définition 4.7 Soit X un ensemble non vide. L'ensemble des bijections de X est un groupe pour la loi de composition, on l'appelle groupe symétrique sur X et on le note $\mathfrak{S}(X)$.

Remarque 4.8 Lorsque $X = [\![1, n]\!]$, on le note $\mathfrak{S}_n$. Lorsque $|E| = n$, on a $\mathfrak{S}(E) \simeq \mathfrak{S}_n$.

Lemme 4.9 Pour $n \geq 3$, $\mathfrak{S}_n$ est non abélien.

Remarque 4.10 Le groupe $\mathfrak{S}_n$ est fini d'ordre $n!$.

Théorème 4.11 Soit $\sigma \in \mathfrak{S}_n$. Alors σ se décompose, de manière unique à l'ordre des facteurs près, en un produit de cycles à supports disjoints.

Proposition 4.12 Le groupe $\mathfrak{S}_n$ est engendré par les transpositions, par les transpositions de la forme $(1, i)$, par les transpositions de la forme $(i, i+1)$ et par $(1\ 2)$ et $(1\ 2 \dots n)$.

Définition - proposition 4.13 Il existe un unique morphisme $\varepsilon : \mathfrak{S}_n \longrightarrow \mathbb{C}^*$ non trivial, appelé signature. De plus, si σ est produit de k transpositions, $\varepsilon(\sigma) = (-1)^k$.

Définition 4.14 Le groupe alterné, noté $\mathcal{A}_n$, est l'ensemble des permutations de signature 1.

Proposition 4.15 Le groupe alterné $\mathcal{A}_n$ est l'unique sous-groupe de $\mathfrak{S}_n$ d'indice 2.

Proposition 4.16 Le groupe $\mathcal{A}_n$ est simple si et seulement si $n = 3$ ou $n \geq 5$.

Application 4.17 Le groupe $\mathcal{A}_5$ est l'unique groupe simple d'ordre 60 à isomorphisme près.

développement 2

3. Groupe linéaire sur des corps finis

Proposition 4.18 Le groupe linéaire $GL_n(\mathbb{F}_q)$ est fini d'ordre $q^{n(n-1)/2} \prod_{k=1}^{n} (q^k - 1)$.

Proposition 4.19 Soient $n \geq 1$ et $q \geq 2$, alors $Z(GL_n(\mathbb{F}_q)) = \{\lambda I_n \mid \lambda \in \mathbb{F}_q^*\} \simeq \mathbb{F}_q^*$.

Conséquence 4.20 Ainsi, pour $n \geq 2$, $GL_n(\mathbb{F}_q)$ n'est pas abélien.

Proposition 4.21 Les matrices de transvections et de dilatation engendrent $GL_n(\mathbb{F}_q)$.

Proposition 4.22 Pour $n \geq 1$ et $q \geq 2$, si $(n,q) \neq (2,2)$, $D(GL_n(\mathbb{F}_q)) = SL_n(\mathbb{F}_q)$.

Remarque 4.23 Dans le cas $GL_2(\mathbb{F}_2)$, le groupe dérivé est $\{I_n\}$.

Proposition 4.24 (Isomorphismes exceptionnels) On a les isomorphismes suivants :

(i) $GL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$

(ii) $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ et $PSL_2(\mathbb{F}_3) \simeq \mathcal{A}_4$

(iii) $PGL_2(\mathbb{F}_4) \simeq PSL_2(\mathbb{F}_4) \simeq \mathcal{A}_5$

(iv) $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ et $PSL_2(\mathbb{F}_5) \simeq \mathcal{A}_5$

Remarque 4.25 Ces isomorphismes permettent de trancher sur la simplicité ou non de ces groupes.