Leçon N° 104 : Groupes finis. Exemples et applications.

Dans toute cette leçon, $(G,\cdot)$ est un groupe d'élément neutre e et G est supposé fini.

I) Présentations

Définition 1 : Le nombre d'éléments de G est appelé l'ordre de G.

Exemple 2 : $\forall n \in \mathbb{N}^*$, l'ordre de $(\mathbb{Z}/n\mathbb{Z}, +)$ est n.

Notation 3 : Pour H un sous groupe de G, on note G/H l'ensemble des classes à gauche relativement à H, i.e. $G/H = \{gH, g \in G\}$.

Définition 4 : On appelle indice de H dans G noté $[G:H]$ le cardinal de G/H.

Théorème 5 : (Lagrange) Soit H un sous groupe de G.
$\forall g \in G$, $|gH| = |H|$ et $|G| = [G:H]\,|H|$.
En particulier $|H| \mid |G|$.

Remarque 6 : Nous verrons plus loin que le groupe $\mathfrak{A}_4$ d'ordre 12 n'a pas de sous groupes d'ordre 6.

Exemple 7 : Les sous groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont exactement les $\frac{1}{n}\mathbb{Z}/n\mathbb{Z}$ avec $d \mid n$.

Proposition 8 : Soit G' un groupe. Soit $\varphi : G \to G'$ un morphisme de groupes. $|G| = |\ker\varphi| \times |\mathrm{Im}\,\varphi|$.

Définition 9 : Soit $g \in G$. L'ordre de g est $|\langle g\rangle|$. On le note $o(g)$.

Proposition 10 : Soient G un groupe et $\varphi : G \to G'$ un isomorphisme de groupe alors G est fini, $|G| = |G'|$ et $\forall g \in G$, $o(\varphi(g)) = o(g)$.

Proposition 11 : $\forall g \in G$ et $\forall n \in \mathbb{N}^*$, il y a équivalence entre :
i) g est d'ordre n.
ii) $g^n = e$ et $g^k \neq e$ $\forall k \in [\![1, n-1]\!]$
iii) $\forall k \in \mathbb{Z}$, $g^k = e$ ssi k est un multiple de n.

Contre exemple 12 : Ordre d'un groupe ne coïncide avec aucun désordre des éléments : le groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ d'ordre 4, mais ses éléments sont d'ordre ≤ 2.

II) Cas des groupes finis abéliens

1) Groupes cycliques

Définition 13 : On dit que G est cyclique lorsqu'il $\exists g \in G$ tq $G = \langle g\rangle$.

Exemple 14 : $\forall n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1}\rangle$
$U_n = \langle e^{\frac{2i\pi}{n}}\rangle$.

Remarque 15 : Ces groupes sont isomorphes via l'application $\bar{k} \mapsto e^{\frac{2ik\pi}{n}}$

Proposition 16 : Si G est cyclique d'ordre $n \in \mathbb{N}^*$, alors G est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Proposition 17 : Si G est cyclique d'ordre $n \in \mathbb{N}^*$, $G = \langle g\rangle$, alors ses générateurs sont les g^k, g étant un générateur et $k \in [\![1, n-1]\!]$ étant premier avec n.

Proposition 18 : Un groupe de cardinal premier est cyclique.

Proposition 19 : Un groupe commutatif d'ordre pq où p et q sont deux nombres premiers distincts est cyclique.

Définition 20 : $\forall n \geq 1$, on note $\varphi(n)$ le nombre d'entiers de $[\![1, n]\!]$ premiers avec n. φ est alors appelé la fonction indicatrice d'Euler.

Proposition 21 : Si $n \geq 2$ est premier avec $\varphi(n)$, alors tout groupe commutatif d'ordre n est cyclique.

Théorème 22 : Supposons que $G = \langle g\rangle$ et que H est un sous groupe distingué de G. Les sous groupes de G/H sont de la forme K/H où K est un sous groupe de G qui contient H.

Dev 1

Application 23 : $\forall n \geq 2$, on a $n = \sum_{d \mid n} \varphi(d)$

Lemme 24 : Si G est commutatif, $r \geq 2$ et $g_1, \dots, g_r$ des éléments 2-à-2 distincts de G d'ordre respectifs $m_1, \dots, m_r$, il existe $g_0 \in G$ d'ordre égal au ppcm de ces ordres.

Théorème 25 : Tout sous groupe fini de groupe multiplicatif $\mathbb{K}^*$, $\mathbb{K}$ étant un corps commutatif est cyclique.

Exemple 26 : $\mu_n(\mathbb{K}) = \{\lambda \in \mathbb{K}, \lambda^n = 1\}$ est un sous groupe cyclique de $\mathbb{K}^*$.

2) Groupes abéliens finis.

Théorème 27 : (Cauchy). Si G est abélien d'ordre ≥ 2. $\forall$ diviseurs premiers p de n, $\exists g \in G$ tq $o(g) = p$.

Théorème 28 : ADMIS. Si G est abélien.
Alors il existe des entiers $d_1, \dots, d_s \geq 2$ vérifiant $d_1 | d_2 | \dots | d_s$ tels que $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$.
De plus, la suite d'entiers $(d_1, \dots, d_s)$ est unique et ne dépend que de la classe d'isomorphisme de G.

Exemple 29 : À isomorphismes près, les groupes d'ordre 24 abéliens sont : $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

II) Exemples remarquables de groupes finis non abéliens

1) Le groupe symétrique et le groupe alterné.

Définition 30 : Soit $n \in \mathbb{N}^*$, on note $\mathfrak{S}_n$ l'ensemble des permutations de $[\![1, n]\!]$ dans lui même. C'est un groupe pour la composition.

Proposition 31 : $\forall n \geq 1$, $|\mathfrak{S}_n| = n!$

Proposition 32 : $\forall \sigma \in \mathfrak{S}_n$, σ se décompose en produit de cycles à supports deux-à-deux disjoints. Cette décomposition est unique à l'ordre près.

Proposition 33 : $\mathfrak{S}_n$ est engendré par les transpositions.

Proposition 34 : $\forall n \geq 3$, $\mathfrak{S}_n$ n'est pas commutatif.

Théorème 35 : Il existe un unique morphisme non trivial $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$. C'est la signature.

Définition 36 : $\forall n \geq 2$, $\mathfrak{A}_n := \ker(\varepsilon)$, c'est le groupe alterné.

Exemple 37 : $\mathfrak{A}_n$ est d'ordre $\frac{n!}{2}$ mais n'a pas de sous groupe d'ordre 6.

Théorème 38 : (Cayley) G est isomorphe à un sous groupe de $\mathfrak{S}(G)$.

Application 39 : Soit $n \in \mathbb{N}^*$ et $M \in \mathcal{M}_n(\mathbb{K})$, on définit le déterminant de M par $\det(M) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} m_{i,\sigma(i)}$.

2) Le groupe diédral.

Définition 40 : Soit $n \geq 2$. Le groupe diédral D_n est le groupe des isométries du plan euclidien conservant un polygone régulier à n côtés. On note O le centre du polygone.

Proposition 41 : D_n est engendré par la rotation de centre O et d'angle $\frac{2\pi}{n}$ et une réflexion par rapport à une droite passant par O et un sommet du polygone.

Proposition 42 : $\forall n \geq 3$, D_n n'est pas abélien.

Proposition 43 : $\forall n \geq 2$, $|D_n| = 2n$.

IV) Actions de groupes

1) La théorie

Définition 44: Soit X un ensemble. On dit que G opère sur X lorsqu'on s'est donné une application : $G \times X \longrightarrow X$, $(g, x) \mapsto g.x$.
vérifiant les axiomes suivants : 1) $\forall g, g' \in G \ \forall x \in X, \ g.(g'.x) = (gg').x$
2) $\forall x \in X, \ 1_G . x = x$.

Remarque 45: Il revient au même de se donner un morphisme $\varphi : G \to \mathfrak{S}(X)$ en posant $g.x = \varphi(g)(x)$.

Définition 46: $\forall x \in X$, $G.x = \{g.x, g \in G\}$ est l'orbite de x.

Définition 47: $\forall x \in X$, $G_x = \{g \in G, g.x = x\}$ est le stabilisateur de x

Proposition 48: (Équation aux classes) Si G opère sur X fini alors
$$|X| = \sum_{i=1}^{r} |G.x_i| = \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}$$
Où x_i est un représentant des r orbites formant une partition de X.

Application 49: Si p est premier, tout groupe d'ordre p^2 est abélien

Définition 50: Si G opère sur X fini, $\forall g \in G$, on note
$Fix_X(g) = \{x \in E, \ g.x = x\}$.

Proposition 51: (Formule de Burnside) Si on note $\mathcal{R}$ l'ensemble des orbites, alors $|\mathcal{R}| = \frac{1}{|G|} \sum_{g \in G} |Fix_X(g)|$.

2) La pratique

Définition 52: On note $|G| = p^\alpha m$ avec p premier et $p \nmid m$.
On appelle p-Sylow de G un sous groupe de cardinal p^α.

Lemme 53. Si $|G| = n = p^\alpha m$. Soit H un sous groupe de G.
Supposons que G admette un p-Sylow S alors $\exists g \in G$ tq $gSg^{-1} \cap H$ soit un p-Sylow de H.

Théorème 54: (Sylow) Soit G un groupe fini, et soit p un nombre premier.
$|G| = p^m q$ avec $m \geq 0$ et $p \nmid q$. Alors :
1) $\exists$ des p-Sylow et tout p-~~Sylow~~ groupes est contenu dans un p-Sylow
2) Le conjugué d'un p-Sylow de G est un p-Sylow de G et tout les p-Sylow sont conjugués.
3) Si N_p est le nombre de p-Sylow de G, on a $N_p \equiv 1 [p]$ et $N_p \mid q$.

Application 55: $\mathcal{A}_n$ est simple $\forall n \geq 5$.

Théorème 56: Les groupes d'isométries des cube sont :
$T_h^+(C_6) \simeq \mathfrak{S}_4$
$T_h(C_6) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Proposition 57: Le nombre de colorations du cube à isométrie positive près est $\frac{1}{24}(C^6 + 8C^2 + 6C^3 + 3C^4 + 6C^3)$ pour C couleurs.

V) Classification des groupes fini de cardinal ≤ 8

Cardinal	groupes
1	$\{e\}$
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$.
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $D_3 \simeq \mathfrak{S}_3$
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$ D_4 Q_8