Soit G un groupe fini

I/ Outils pour l'étude des groupes

1) Ordre d'un groupe

Définition 1 : On appelle ordre d'un groupe G, le cardinal de G, noté $|G|$.

Exemple 2 : Le groupe $\mathbb{Z}/n\mathbb{Z}$ est d'ordre n.

Définition 3 : Si H est un sous-groupe de G, le cardinal de G/H est noté $[G:H]$ et on l'appelle indice de H dans G.

Théorème 4 : (Lagrange) Soit H un sous-groupe de G. Alors, $|G| = [G:H]|H|$. En particulier $|H|$ divise $|G|$

Définition 5 : L'ordre d'un élément $x \in G$ est l'ordre du sous-groupe $\langle x \rangle$, noté $o(x)$.

Proposition 6 : Soit $x \in G$. Alors $\exists n > 0$ tel que $x^n = 1_G$

Dans ce cas, on a $o(x) = \min\{n \in \mathbb{N}^* / x^n = 1_G\}$

Proposition 7 : Si $|G| = n$, alors $\forall x \in G$, $x^n = 1_G$.

Théorème 8 : (Fermat) Soit $a \in \mathbb{Z}$ et p premier.

Alors $a^p \equiv a \ [p]$ et si $a \wedge p = 1$, $a^{p-1} \equiv 1 \ [p]$.

2) Actions de groupe

Définition 9 : Soit X un ensemble, on dit que G opère sur X si on s'est donné une application $G \times X \to X$, $(g,x) \mapsto g.x$ vérifiant

1) $\forall (g,g') \in G^2$, $\forall x \in X$ $g.(g'.x) = gg'.x$ 2) $\forall x \in X$ $1.x = x$

Remarque 10 : Il revient au même de se donner un morphisme $\varphi : G \to \mathcal{S}(X)$ où $\mathcal{S}(X)$ désigne le groupe des bijections de X.

Exemple 11 : G opère sur G par translation à gauche par $G \times G \to G$, $(g,h) \mapsto gh$.

Théorème 12 : (Cayley) Si $|G| = n$, alors G est isomorphe à un sous-groupe de $\mathcal{S}_n$.

Définition 13 : Si G opère sur X et $x \in X$, on définit $G_x = \{g \in G / g.x = x\}$ le stabilisateur de x et on appelle orbite de $x \in X$ l'ensemble $G.x = \{g.x / g \in G\}$

Proposition 14 : L'application $f : G/G_x \to G.x$, $\overline{g} \mapsto g.x$ est une bijection et on a $|G| = |G_x| \times |G.x|$

Proposition 15 : (Formule des classes) Soit G agissant sur un ensemble fini X

1) Si $X = \bigcup_{i=1}^{n} X_i$ est la partition de X en orbites sous l'action de G et si $x_i \in X_i$, alors $|X| = \sum_{i=1}^{n} |X_i| = \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|}$

2) Soit $g \in G$ et X^g l'ensemble des points fixes de X sous l'action de $\langle g \rangle$. Le nombre r d'orbites de X sous l'action de G est $r = \frac{1}{|G|} \sum_{g \in G} |X^g|$

Application 16 : 1) En moyenne, une permutation de S_n à 1 seul point fixe

2) Il y a 57 possibilités de colorier un cube en bleu, blanc, rouge.

3) p-groupe et théorème de Sylow

Définition 17 : Soit p un nombre premier. Un p-groupe est un groupe dont l'ordre est une puissance de p.

Proposition 18 : Soit p un nombre premier, G un p-groupe agissant sur X. Alors $|X^G| \equiv |X| \ [p]$.

Proposition 19 : Soit p premier et $G \neq \{e\}$ un p-groupe. Le centre $Z(G)$ de G ne se réduit pas au groupe trivial $\{e\}$.

Proposition 20 : Soit p premier. Un groupe d'ordre p^2 est toujours abélien.

Théorème 21 : (Cauchy) Soit G un groupe fini d'ordre divisible par p premier. Alors, il existe au moins un élément d'ordre p dans G.

Définition 22 : Soit $|G| = n$ et p un diviseur premier de n. Si $n = p^\alpha m$ avec $p \nmid m$, on appelle p-sous-groupe de Sylow de G un sous groupe de cardinal p^α

Exemple 23 : Soit $P = \{ A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{Z}/p\mathbb{Z}) \mid \begin{matrix} a_{i,i} = 1 \\ a_{i,j} = 0 \text{ si } i > j \end{matrix} \}$ est un p-Sylow de $GL_n(\mathbb{Z}/p\mathbb{Z})$.

Lemme 24 : Si $G = |n| = p^\alpha m$ avec $p \nmid m$ et soit H un sous groupe de G. Soit S un p-Sylow de G. Alors, $\exists a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

Théorème 25 (Sylow) : Soit p un diviseur premier de $|G|$, Alors G contient au moins un p-sous-groupe de Sylow

Théorème 26 : (Sylow) Soit $|G| = p^\alpha m$ avec $p \nmid m$.

1) Si H est un sous-groupe de G qui est un p-groupe, il existe un p-Sylow S, avec $H \subset S$.

2) Les p-Sylow sont tous conjugués et leur nombre $k \mid n$.

3) On a $k \equiv 1 \ [p]$ donc $k \mid m$.

Application 27 : Un groupe d'ordre 63 n'est pas simple.

II / Groupes Abéliens

1) Cyclicité dans un groupe

Définition 28 : On dit que G est cyclique si : $\exists g \in G, G = \langle g \rangle$.

Exemple 29 : $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique et $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$.

Théorème 30 : Soit G un groupe cyclique d'ordre n. G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

Exemple 31 : Le groupe des racines n-ièmes de l'unités U_n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

Définition 32 : On définit $\varphi : \begin{matrix} \mathbb{N}^* \to \mathbb{N}^* \\ n \mapsto \#\{k \mid \begin{matrix} k \in [\![1, n]\!] \\ k \wedge n = 1 \end{matrix}\} \end{matrix}$ appelé fonction d'Euler.

Théorème 33: Si $G = \langle g \rangle$ est cyclique d'ordre n. Les générateurs sont les g^k où $k \in [\![1, n-1]\!]$, premier avec n.

Remarque 34: G possède $\varphi(n)$ générateurs distincts.

Proposition 35: Un groupe d'ordre premier est cyclique.

Proposition 36: Le groupe $Aut(\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$ et est de cardinal $\varphi(n)$.

Proposition 37: Soit G un groupe cyclique d'ordre n, et a un générateur de G. Tout sous-groupe de G est cyclique, et pour tout diviseur d de n, il existe un unique sous-groupe H_d de G d'ordre d et $H_d = \langle a^{\frac{n}{d}} \rangle$

Exemple 38: Les éléments d'ordre 6 de $\mathbb{U}_{30}$ sont $e^{\frac{i\pi}{3}}$ et $e^{\frac{5i\pi}{3}}$

2) Théorème de Structure :

G désigne un groupe abélien

Lemme 39: Soit $a \in G$ d'ordre $o(a)$ maximum. Alors $\forall y \in G/\langle a \rangle$ il existe $x \in G$ tel que $\bar{x} = y$ et $o(x) = o(y)$

Théorème 40: Soit $n \geq 2$, alors $\exists! (q_1, \dots, q_k) \in \mathbb{N}^*$ tel que $q_1 \geq 2$ et $q_1 | q_2 | \dots | q_k$ tels que $G \simeq (\mathbb{Z}/q_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/q_k\mathbb{Z})$

Définition 41: La suite $(q_1, \dots, q_k) \in \mathbb{N}^*$ est appelée suite des invariants de G.

Exemple 42: $(\mathbb{Z}/60\mathbb{Z}) \times (\mathbb{Z}/72\mathbb{Z}) \simeq (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/360\mathbb{Z})$

III / Groupes Non-Abéliens Remarquables

1) Le groupe symétrique

Proposition 43: Soit $n \in \mathbb{N}^*$. S_n est d'ordre $n!$

Théorème 44: Soit $n \in \mathbb{N}^*$. Le groupe S_n est engendré par :
- soit les transpositions
- soit les $(1\ k)$ où $k \in [\![2, n]\!]$
- soit les $(i, i+1)$ où $i \in [\![1, n-1]\!]$

Exemple 45: $\begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 2&3&4&5&1&7&6&8 \end{pmatrix} = (1\ 2\ 3\ 4\ 5)(6\ 7)$

Définition 46: La signature d'une permutation σ, est notée $\varepsilon(\sigma)$ et est définie par $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$

Théorème 47: 1 et ε sont les seuls morphismes de $(S_n, \circ)$ vers $(\mathbb{R}^*, \cdot)$

2) Le groupe alterné

Définition 48: A_n est le sous-groupe de S_n formé des permutation de signature égale à 1.

Proposition 49: $|A_n| = \frac{n!}{2}$

Proposition 50: Pour $n \geq 3$, A_n est engendré par les 3-cycles

Définition 51: Un groupe G est dit simple si ses seuls sous groupes distingués sont $\{1\}$ et G.

Théorème 52: Pour $n \geq 5$, A_n est simple.