104 - Groupes abéliens et non abéliens finis. Exemples et applications.

I - Outils de théorie des groupes.

1) Ordre et exposant.

Def 1 L'ordre d'un groupe fini est son cardinal.

Def 2 Soit G un groupe, l'ordre d'un élément $g \in G$ est l'ordre du sous groupe $\langle g \rangle$.

Def 3 On appelle exposant d'un groupe fini G le ppcm des ordres des éléments de G.

Prop 4 Un groupe abélien d'exposant m contient un élément d'ordre m.

2) Sous groupes et quotients.

Def 5 Un sous groupe $H \subset G$ est distingué dans G si $\forall g \in G,\ gHg^{-1} = H$. On note alors $H \triangleleft G$.

Ex 6
- Si $f : G \to K$ est un morphisme de groupe, $\operatorname{Ker} f \triangleleft G$
- $D(G) \triangleleft G$.

Def 7 Un groupe est dit simple s'il ne possède aucun sous groupe distingué non trivial.

Def 8 Soient G un groupe et H un sous groupe de G, les classes à gauche suivant H sont les classes de la relation d'équivalence $g_1 \sim_H g_2 \Leftrightarrow g_2^{-1} g_1 \in H$. On appelle indice de H dans G le nombre de classes à gauche que l'on note $[G:H]$

Thm 9 (Lagrange) $$|G| = |H| \cdot [G:H]$$

Cor 10 L'ordre d'un élément $g \in G$ divise l'ordre de G.

Def 11 Supposons $H \triangleleft G$, on peut munir l'ensemble des classes à gauche $G/H := \{gH,\ g \in G\}$ d'une loi de groupe par $(g_1H)\cdot(g_2H) = g_1g_2H$.

Thm 12 (1er théorème d'isomorphisme) Soit $f : G \to K$ un morphisme surjectif de groupes, f se factorise en $f = \bar{f} \circ \pi$ où $\pi : G \to G/\operatorname{Ker} f$ est la surjection canonique et $\bar{f} : G/\operatorname{Ker} f \to K$ est un isomorphisme.

3) Actions de groupes

Def 13 Soient X un ensemble et G un groupe, une action de G sur X est un morphisme de groupes $\alpha : G \to S(X)$, où $S(X)$ est le groupe des permutations de X.

Ex 14 G agit sur lui même par conjugaison.

Def 15 L'orbite d'un élément $x \in X$ est l'ensemble $\{g \cdot x,\ g \in G\}$, son stabilisateur est le sous groupe $\{g \in G,\ g \cdot x = x\} =: \operatorname{Stab}(x)$

Prop 16 Tout groupe d'ordre n est isomorphe à un sous groupe de S_n.

Prop 17 Soit G un groupe fini qui agit sur un ensemble fini X, soit $\{x_1, \cdots, x_k\}$ un système de représentants de chaque orbite, alors
$$|X| = \sum_{i=1}^{k} [G : \operatorname{Stab}(x_i)]$$

Prop 18 Soit G un groupe fini non abélien et $m(G)$ le nombre de couple d'éléments de G qui commutent, on a $m(G) \leq \frac{5}{8} |G|^2$.

Prop 18' Si p est un facteur premier de G alors G admet un élément d'ordre p.

4) Produits directs et semi-directs

Def 19 Soient N et H deux groupes, leur produit direct est le produit cartésien $N \times H$ munit de la loi de groupe $(n_1,h_1)\cdot(n_2,h_2) = (n_1n_2, h_1h_2)$

Def 20 Soient N et H deux groupes et $\varphi : H \to \operatorname{Aut}(N)$ un morphisme de groupe. Le produit semi direct $N \rtimes_\varphi H$ est le produit cartésien $N \times H$ munit de la loi de groupe
$(n_1,h_1)\cdot(n_2,h_2) = (n_1\varphi(h_1)(n_2), h_1h_2)$

Rq 21 Si φ est trivial alors $N \rtimes_\varphi H \simeq N \times H$

Prop 22 Si $\alpha \in \operatorname{Aut}(H)$ alors $N \rtimes_{\varphi\circ\alpha} H \simeq N \rtimes_\varphi H$

Prop 23 Si N et H sont deux sous groupes d'un groupe G qui vérifient :
- $N \triangleleft G$
- $N \cap H = \{1\}$
- $NH = G$

Alors $G \simeq N \rtimes_\varphi H$ où φ est l'action de H sur N par conjugaison.

II Groupes abéliens finis

1) Groupes cycliques

Def 24 Un groupe fini G est dit cyclique s'il existe un élément $g \in G$ tel que $G = \langle g \rangle$.

Prop 25 Pour $n \in \mathbb{N}^*$, tout groupe cyclique d'ordre n est isomorphe au groupe quotient $\mathbb{Z}/n\mathbb{Z}$.

Prop 26 Pour $n \in \mathbb{N}^*$ et $s \in \mathbb{Z}$ les propriétés suivantes sont équivalentes
- (i) $s \wedge n = 1$
- (ii) $\bar{s}$ est générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$
- (iii) $\bar{s} \in (\mathbb{Z}/n\mathbb{Z})^\times$

Def 27 On appelle indicatrice d'Euler la fonction définie sur $\mathbb{N}^*$ par $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

Prop 28 Si $p \wedge q = 1$, alors $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

Prop 29 Si la décomposition de n en facteurs premiers est $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, alors :

$$\mathbb{Z}/n\mathbb{Z} = \prod_{i=1}^{k} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$

$$(\mathbb{Z}/n\mathbb{Z})^\times = \prod_{i=1}^{k} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times,$$

et $\varphi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$

Prop 30. Si p est un nombre premier impair alors pour $\alpha \geq 1$
$(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$
· Pour $\alpha \geq 3$ $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

2) Structure des groupes abéliens finis

Def 31 Si G est un groupe abélien fini, on appelle groupe dual de G le groupe $\hat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$. Les éléments de $\hat{G}$ sont appelés caractères de G.

Ex 32 $\widehat{(\mathbb{Z}/n\mathbb{Z})} \simeq \mathbb{Z}/n\mathbb{Z}$

Prop 33 Tout élément de $\hat{G}$ est à valeur dans $\mathbb{U}_m$, où m est l'exposant de G.

DEV 1

Prop 34 Soit H un sous groupe d'un groupe abélien fini G et $\chi \in \hat{H}$. Il existe $\tilde{\chi} \in \hat{G}$ tel que $\chi = \tilde{\chi}_{|H}$

Thm 35 (Structure) Tout groupe abélien fini est isomorphe à un produit $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ où $n_1, \dots, n_k$ sont des entiers vérifiant $n_1 | \cdots | n_r$ et sont déterminés de manière unique

Rq 36 n_k est l'exposant de G.

Ex 37 Les groupes abéliens d'ordre 12 sont $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Prop 38 Soit K un corps, tout groupe fini de K^* est cyclique.

Prop 39 Pour tout groupe G abélien et fini $G \simeq \hat{G}$.

III Autres groupes finis particuliers.

1) Groupes symétriques et alternés.

Def 40 Le groupe symétrique S_n est le groupe formé des permutations de $[\![1,n]\!]$.

Prop 41 Toute permutation $\sigma \in S_n$ se décompose comme produit de permutations cyclique à support disjoints de manière unique à permutation des facteurs près.

Prop 42 Pour $(i_1, \dots, i_k)$ un cycle de longueur k et $\sigma \in S_n$
$\sigma(i_1, \dots, i_k)\sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_k))$

Prop 43 Deux éléments de S_n sont conjugués si et seulement si les cycles disjoints de leurs décompositions sont de mêmes longueurs.

Prop 44 $Z(S_n) = \{Id\}$ pour $n \geq 3$.

Prop 45 Les parties suivantes sont génératrices de S_n,
— les transpositions
— $\{(1\,i),\ i \in [\![2,n]\!]\}$
— $\{(12), (1, \dots, n)\}$

Prop 46 Pour $n \neq 6$, les automorphismes de S_n sont intérieurs.

Def 47 La signature est le morphisme $\varepsilon : S_n \to \{\pm 1\}$ définit par $\varepsilon(\sigma) = \prod_{j > i} \frac{\sigma(j) - \sigma(i)}{j - i}$

Def 48 On appelle groupe alterné d'ordre n le groupe $A_n = \ker \varepsilon$
C'est un sous groupe distingué d'indice 2 dans S_n.

Prop 49 $S_n \simeq A_n \rtimes \mathbb{Z}/2\mathbb{Z}$

Prop 50 A_n est engendré par les 3-cycles pour $n \geq 3$

Thm 51 Pour $n \geq 5$, A_n est simple.

Rq 52 A_4 est non simple car $V_4 \trianglelefteq A_4$ avec
$V_4 = \{Id, (12)(34), (13)(24), (14)(23)\}$.

2) Groupes d'isométries et groupes diédraux.

Def 53 Soit X une partie d'un espace affine euclidien $\mathcal{E}$. On note $\mathrm{Isom}(X)$ le sous groupe $\{f \in \mathrm{Isom}(\mathcal{E}),\ f(X) = X\}$

Ex 54 Si T est un tétraèdre régulier dans $\mathbb{R}^3$ alors
$\mathrm{Isom}(T) \simeq S_4$, $\mathrm{Isom}^+(T) \simeq A_4$

Ex 55 Si C est un cube dans $\mathbb{R}^3$ alors
$\mathrm{Isom}(C) \simeq \mathbb{Z}/2\mathbb{Z} \times S_4$, $\mathrm{Isom}^+(C) \simeq S_4$

Def 56 Pour $n \geq 2$, soit P_n le polygone régulier d'ordre n.
Le groupe diédral d'ordre n est $D_n = \mathrm{Isom}(P_n)$.

Prop 57 D_n est d'ordre $2n$ et $D_n = \{r^k,\ k \in [\![0,n-1]\!]\} \cup \{r^k s,\ k \in [\![0,n-1]\!]\}$ avec r la rotation d'angle $\frac{2\pi}{n}$ et s la réflexion par rapport à l'axe (Ox).

Prop 58 D_n possède la définition par générateurs et relations suivante $D_n \simeq \langle r, s \mid rs = sr^{-1} \rangle$

Prop 59 $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

Prop 60 • Si n est impair, les classes de conjugaisons de D_n sont : $\{Id\}, \{r^k, k \in [\![1, n-1]\!]\}, \{r^k s, k \in [\![0, n-1]\!]\}$

• Si n est pair, elles sont :
$\{Id\}, \{-Id\}, \{r^k, k \in]\!]-\frac{n}{2}, \frac{n}{2}[\![\setminus \{0\}\}, \{r^{2k}s, k \in [\![0, \frac{n}{2}[\![\}, \{r^{2k-1}s, k \in]\!]0, \frac{n}{2}[\![\}$

IV Théorèmes de Sylow et classification des groupes finis.

1) p-groupes

Def 61 Soit p un nombre premier, un p-groupe est un groupe d'ordre p^α pour un $\alpha \geq 1$.

Prop 62 Si G est un p-groupe qui agit sur un ensemble fini X alors $|X^G| = |X|\ (p)$ avec $X^G = \{x \in X, \forall g \in G, g \cdot x = x\}$

Th 63 Le centre d'un p-groupe est non trivial

Prop 64 Tout groupe d'ordre p^2 est abelien.

Prop 65 Un groupe d'ordre p^3 est soit abelien soit isomorphe à un produit semi direct $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$ ou $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. lorsque p est impair.

Prop 65' Les groupes non abeliens d'ordre 8 sont D_4 et H_8.

2) Les theorèmes de Sylow

Def 66 Soit G un groupe d'ordre $p^\alpha s$ où p est premier, $\alpha \geq 1$ et $p \wedge s = 1$. Un p-Sylow de G est un sous groupe d'ordre p^α.

DEV 2

Lemme 67 Si G est d'ordre $p^\alpha s$ et H est un sous groupe de G et S est un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

Th 68 (1er thm de Sylow) Soit G un groupe fini et p un diviseur premier de $|G|$. G admet un p-Sylow.

Thm 69 Si G est d'ordre $p^\alpha s$ avec $p \wedge s = 1$ Alors
- Tout p sous groupe de G est inclus dans un p-Sylow de G
- Les p-Sylow sont conjugués entre eux
- Le nombre de p-Sylow de G vérifie $n_p = 1\ [p]$ et $n_p \mid s$

Rq 70 Si G admet un unique p-Sylow alors ce dernier est distingué.

Ex 71 Les 2 Sylows de S_4 sont au nombre de 3 et sont conjugués à $\{Id, (12)(34), (13)(24), (14)(23), (1234), (1423), (24), (13)\}$.

3) Groupes d'un cardinal donné.

Ex 72 Tout groupe d'ordre 255 est cyclique

Prop 73 Soient $p < q$ deux nombres premiers. Si $p \mid q-1$ alors tout groupe d'ordre pq est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$, sinon il est soit produit semi direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$, soit cyclique.

Prop 74 Si G est d'ordre $p^\alpha q$ où p et q sont premiers et où $p^\alpha \nmid (q-1)!$. Alors G est non simple.

Prop 75 A_5 est le seul groupe simple d'ordre 60.

Prop 76 Les groupes d'ordre 6 sont $\mathbb{Z}/6\mathbb{Z}$ et S_3

Prop 77 Groupes de petits cardinaux :

m	Groupes d'ordre m
4	$\mathbb{Z}/4\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z})^2$
6	$\mathbb{Z}/6\mathbb{Z}$; S_3
8	$\mathbb{Z}/8\mathbb{Z}$; $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z})^3$; D_4 ; H_8
9	$\mathbb{Z}/9\mathbb{Z}$; $(\mathbb{Z}/3\mathbb{Z})^2$
10	$\mathbb{Z}/10\mathbb{Z}$; D_{10}
12	$\mathbb{Z}/12\mathbb{Z}$; $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; D_{12} ; A_4 ; $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$