104

Groupes finis. Exemples et applications

I) Définitions et premiers théorèmes

1) Groupe fini et ordre [Calais + Oraux Alg 2]

Déf 1 : Un groupe G est dit fini s'il ne possède qu'un nombre fini d'éléments. Le cardinal de G s'appelle l'ordre de G et on le note $|G|$.

Ex 2 : $|\mathbb{Z}/n\mathbb{Z}| = n$, $|S_n| = n!$.

Déf 3 : Soit $x \in G$, où G est un groupe fini. On appelle ordre de x l'ordre du sous-groupe engendré par x, et il est noté $o(x)$.

Ex 4 : . Dans tout groupe G, $o(e_G) = 1$ et e_G est le seul élt d'ordre 1.
. Dans S_n, les transpositions sont d'ordre 2, les k-cycles sont d'ordre k.

Déf 4 : Un groupe G est d'exposant fini si $\exists N \in \mathbb{N}$ tq $\forall g \in G$, $g^N = e_G$.

Prop 5 : (Théorème de Burnside) Un sous-groupe de $GL_n(\mathbb{C})$, d'exposant fini est fini. DEV 1

2) Théorème de Lagrange [Combes]

Déf 6 : Soit G groupe fini, H sous-groupe de G. Le cardinal commun à G/H et $G\backslash H$ s'appelle l'indice de H dans G, on le note $[G:H]$. Si $H = \{e\}$, alors $[G:H] = |G|$.

Prop 7 : (Théorème de Lagrange) Soient K, H deux sous-groupes de G tq $K \subset H$. Alors $[G:K] = [G:H][H:K]$.

Cor 8 : l'ordre $o(g)$ de tout élément $g \in G$ divise $|G|$.

Appl 9 : * Si K et M sont deux ss-groupes de G d'ordre k et m avec $k \wedge m = 1$, alors $K \cap M = \{e\}$.
* Soient k et m deux diviseurs de n et $d = \text{pgcd}(k,m)$ alors : $U_k \cap U_m = U_d$
où $U_m = \{z \in \mathbb{C},\ z^m = 1\}$.

3) Théorème de factorisation d'homomorphisme (Combes)

Thm 10 : Soit $H \triangleleft G$, j l'homomorphisme canonique de G sur G/H. Soit $f : G \to G'$ un homomorphisme de groupes. Si $H \subset \operatorname{Ker} f$, il existe $\bar{f} : G/H \to G'$ unique tq $\bar{f} \circ j = f$. On a : $\operatorname{Ker} \bar{f} = j(\operatorname{Ker} f)$ et $\operatorname{Im}(\bar{f}) = \operatorname{Im}(f)$.

Cor 11 : $G/_{\operatorname{Ker} f}$ et $f(G)$ sont isomorphes.

Appli 12 : les groupes $\mathbb{Z}/_{n\mathbb{Z}}$ et U_n sont isomorphes.

4) Actions de groupe (Combes)

Déf 13 : * On appelle action à gauche du groupe G sur un ens. X, un homomorphisme t de G dans le groupe S_X des bijections de X sur X.
* On appelle orbite de x sous l'action de G la classe d'équivalence $\{g \cdot x \mid g \in G\}$ de $x \in X$.
* le sous-groupe G_x de G formé des éléments de G qui laissent fixe $x \in E$ s'appelle le stabilisateur de x.

Prop 14 : Notons $O_1, \dots, O_k$ les orbites pour une action de G sur X, et x_i un élément de O_i. On note $\text{fix}(g) = \{x \mid g \cdot x = x\}$.
Alors : i) $\text{Card}(X) = \sum_{i=1}^{k} \text{Card}(O_i)$ et $\text{Card}(O_i) = \dfrac{|G|}{|G_{x_i}|}$ (équation des classes)

ii) $k = \dfrac{1}{|G|} \sum_{g \in G} \text{card}(\text{fix}(g))$ (formule de Burnside).

App 15 : * Soit G groupe d'ordre p^m, p premier, agissant sur un ensemble fini X. Le nombre de points fixes de E est congru à $\text{card}(X) \bmod p$.
* Combien de colliers différents peut-on faire avec un fil circulaire, 4 perles bleues, 3 perles blanches et 2 perles orange.

Appli 16 : * (Th de Cauchy) Soit G groupe fini, p facteur premier de $m = |G|$. Il existe des éléments d'ordre p dans G.

* G fini, p premier. Pour que l'ordre de G soit une puissance de p, il faut et suffit que l'ordre de tout élément soit une puissance de p.
* G fini, p plus petit nombre premier divisant m. Si H est un sous-groupe de G d'indice p, alors $H \triangleleft G$.

II) Cas des groupes finis abéliens

1) Groupes cycliques (Combes)

Déf 17 : * G est cyclique s'il est engendré par un élément et fini.

Ex 18 * $\mathbb{Z}/n\mathbb{Z}$ est engendré par $\bar{1}$.

* U_m est engendré par $\xi_m = \exp\left(\frac{2i\pi}{m}\right)$.

Prop 19 : Soit a générateur du groupe cyclique G. L'homomorphisme $k \mapsto a^k$ de $\mathbb{Z}$ sur G se factorise en un isomorphisme de de $\mathbb{Z}/m\mathbb{Z}$ sur G.

Cor 20 : G et G' cycliques sont isomorphes ssi $|G| = |G'|$.

Cor 21 : $\mathrm{Aut}(G)$ est d'ordre $\varphi(m)$ où φ fonction d'Euler. et ses éléments sont les $x \mapsto x^k$, où $k \wedge m = 1$.

Prop 22 : Soit G groupe cyclique d'ordre m, a un générateur de G. Tout sous-groupe de G est cyclique et pour tout diviseur d de m, il existe un unique sous-groupe H d'ordre d.

Appl 23 : * sous-groupes de $\mathbb{Z}/30\mathbb{Z}$

* éléments d'ordre 6 dans U_{30}.

Déf 23 : Un groupe G est simple si $\{e\}$ et G sont les seuls sous-groupes distingués de G.

Prop 24 : G est d'ordre premier ssi il est cyclique et simple.

Cor 25 : Si $|G| = p^2$, p premier, alors G est abélien.

Prop 26 : $(G_1 \times G_2)$ est cyclique ssi G_1 et G_2 sont cycliques d'ordres premiers entre eux.

2) Décomposition en facteurs invariants (Combes)

Prop 27 : Soit G un groupe abélien fini d'ordre $m \geq 2$. Il existe des entiers $q_1 \geq 2$, q_2 multiple de q_1, ..., q_k multiple de q_{k-1} uniques tq G soit isomorphe à :

$$(\mathbb{Z}/q_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/q_k\mathbb{Z}).$$

Déf 28 : Cette suite $q_1 \dots q_k$ s'appelle la suite des invariants.

Cor 29 : Pour tout diviseur d de m, il existe un sous-groupe de G d'ordre d. (G abélien).

Ex 30 : * décomposition de $\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}$.

* structures possibles pour un groupe abélien d'ordre 600.

III) Cas des groupes finis non abéliens

1) Théorème de Sylow (Combes)

Déf 31 : Soit G un groupe, $m = |G|$ et $m = p_1^{k_1} \cdots p_s^{k_s}$ la décomposition en facteurs premiers. Un p_i-Sylow de G est un sous groupe de G d'ordre $p_i^{k_i}$.

Thm 32 : (théorème de Sylow) $|G| = m$, $m = p^k q$ avec $p \wedge q = 1$.

i) il existe un p-Sylow de G

ii) tout p-sous-groupe de G est contenu dans un p-Sylow.

iii) les p-Sylow de G sont conjugués.

iv) le nombre n_p de p-Sylow divise q et $n_p \equiv 1 [p]$

Cor 33 : S'il existe un seul p-Sylow H, alors H est distingué.

App 34 : * structure d'un groupe d'ordre 153

* G d'ordre pq, p et q premiers, alors G n'est pas simple. (Calais)

2) Le groupe symétrique (Nourdine Combes)

Déf 35 : Soit E un ensemble fini. L'ensemble des bijections de E dans E est un groupe appelé groupe symétrique et noté S_E. Si E est de cardinal n, $|S_E| = n!$.

Thm 36 : (Cayley) : Tout groupe fini G est isomorphe à un sous-groupe de S_n où $n = |G|$.

Déf 37 : on appelle k-cycle un élément de S_n qui permute circulairement k éléments de E, et laisse fixe les autres. Un 2-cycle est une transposition.

Prop 38 : Tout élément de S_n se décompose de manière unique en produit de cycles disjoints.

Déf 39 : . $s \in S_n$ présente une inversion en (i,j) si $i<j$ et $s(i)>s(j)$
. l'entier $\varepsilon(s) = (-1)^{N_s}$ est la signature de s (où N_s est le nombre d'inversions).

Prop 40 : L'application $\varepsilon : s \mapsto \varepsilon(s)$ est le seul homomorphisme surjectif de S_n sur $\{1;-1\}$.

Déf 41 : l'ensemble $A_n = \varepsilon^{-1}\{1\}$ est appelé sous-groupe alterné de S_n.

Appli 42 :
* A_n est simple pour $n \geq 5$
* Si G est simple d'ordre 60, alors $G \simeq A_5$ (DEV 2)

3) Le groupe diédral (Alessandri)

Déf 43 : Le groupe diédral d'ordre n, noté D_n est l'ensemble des isométries du plan qui conservent un polygone régulier à n côtés centré en O.

Prop 44 : Soit r la rotation d'angle $\frac{2\pi}{n}$, et s la réflexion d'axe (OA) où A sommet du polygone.
Alors $D_n = \langle r, s \rangle$, $|D_n| = 2n$
et $D_n = \{id, r, \dots r^{n-1}, s, sr, \dots sr^{n-1}\}$.

IV) Application

1) Géométrie (Alessandri)

Soit E un $\mathbb{R}$-espace affine euclidien de dimension 3.
On note $Isom(X)$ l'ensemble des isométries affines qui conservent X et $Isom^+(X)$ les éléments de $Isom(X)$ de déterminant positif.
Notons T un tétraèdre centré en O et C un cube centré en O.

Prop 45 : $Isom(T) \simeq S_4$, $Isom^+(T) \simeq A_4$
$Isom(C) \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}$, $Isom^+(C) \simeq S_4$

2) Représentations de groupe (Rauch)

Déf 46 :
* On appelle représentation linéaire d'un groupe G la donnée d'un espace vectoriel V et d'un morphisme de groupes : $\rho : G \to Gl(V)$.
* On appelle caractère de la représentation $\rho : G \to Gl(V)$ la fonction $\chi_\rho : G \mapsto \mathbb{C}$ définie par
$\chi_\rho(g) = \mathrm{Trace}(\rho(g))$.

Ex 47 : Table de caractère de S_4 :

	1_1	$(12)_6$	$(1,2,3)_8$	$(1,2,3,4)_6$	$(12)(34)_3$
Id	1	1	1	1	1
ε	1	-1	1	-1	1
χ_2	2	0	-1	0	2
χ_3	3	-1	0	1	-1
χ_3'	3	1	0	-1	-1