104 GROUPES FINIS. EX et APPL

Cadre : Soit G un groupe d'élément neutre e, fini.

Prérequis : On suppose connues les notions de groupe, sous-groupe, groupe abélien.

I. QUELQUES GÉNÉRALITÉS

1. Ordre et exposant

Def : Soit $a \in G$, on appelle ordre de a, le cardinal du sous groupe de G engendré par a. Le ppcm des ordres des éléments du groupe G s'appelle l'exposant du groupe [Com]

Rq : Tout groupe fini est d'exposant fini mais la réciproque est fausse : $\left(\mathbb{Z}/2\mathbb{Z}\right)^{\mathbb{N}}$ est un groupe infini d'exposant 2. [Or X-ENS 2]

Thm de Burnside : Réciproque pour les sous groupes de $GL_n(\mathbb{C})$

Tout sous groupe de $GL_n(\mathbb{C})$ d'exposant fini est fini. DVT(1)

2. Thm de Lagrange [Com]

Thm de Lagrange : Soit G un groupe fini, soient K, H deux sous groupes de G alors : $[G:K] = [H:K][G:H]$ si $K \subset H$ où $[G:H]$ est l'indice de H dans G.

Cor : Soit G un groupe fini alors l'ordre d'un élément divise $|G|$

Ex : K et M deux sous groupes d'ordre k et m d'un groupe fini G. Si $k \wedge m = 1$ alors $K \cap M = \{e\}$.

3. Actions de groupe [Com]

Prop : Équation aux classes : Soit G un groupe fini opérant sur un ensemble fini X, soit $\Lambda = \{\Theta_x, x \in X\}$ l'ensemble des orbites

Alors $\mathrm{card}(X) = \sum_{x \in \Lambda} \mathrm{Card}(\Theta_x) = \sum_{x \in \Lambda} \frac{|G|}{|\mathrm{Stab}\, x|}$

Appl : Lemme de Cauchy : Si p est premier et si p divise l'ordre de G alors G admet un élément d'ordre p

De plus, pour que l'ordre de G soit une puissance de p, il faut et il suffit que l'ordre de tout élément de G soit une puissance de p.

Prop : Formule de Burnside : Le nombre d'orbites est :
$$k = \frac{1}{|G|} \sum_{g \in G} \mathrm{Card}(\mathrm{Fix}(g))$$

Appl : Avec l'équation aux classes ou la formule de Burnside, on retrouve le petit théorème de Fermat. ???

II. GROUPES ABÉLIENS FINIS

1. Groupes cycliques [Com]

Notation : $\forall n \geq 2$, $\varphi(n) = \#\{k \in [\![0, n-1]\!], k \wedge n = 1\}$ et $\varphi(1) = 1$

La fonction $\varphi : \mathbb{N}^* \to \mathbb{N}$ est la fonction d'Euler.

Def : Soit G un groupe, il est cyclique s'il est monogène et fini. Tout élément $a \in G$ qui l'engendre est appelé générateur.

Exs : (1) $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ est un groupe cyclique et $\bar{1}$ est un de ses générateurs. Il est d'ordre n.

(2) $\mathbb{U}_n = \{\exp(\frac{2i\pi k}{n}), k \in [\![0, n-1]\!]\}$ et $\zeta = e^{\frac{2i\pi}{n}}$ est un de ses générateurs. Il est d'ordre n.

Prop : Soit G un groupe cyclique d'ordre $n \in \mathbb{N}$ et a un générateur de G. $\forall k \in \mathbb{Z}$, l'ordre de a^k est $\frac{n}{n \wedge k}$. En particulier, a^k est un générateur de G ssi $k \wedge n = 1$. Il y a donc $\varphi(n)$ générateurs dans G.

Exs : (1) Les générateurs de $\mathbb{Z}/12\mathbb{Z}$ sont $\bar{1}, \bar{5}, \bar{7}, \overline{11}$.

(2) Les générateurs de $\mathbb{U}_{18}$ sont $\{\zeta^k = \exp(\frac{2ik\pi}{18}), k \wedge 18 = 1\} = \{\zeta, \zeta^5, \zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{17}\}$

Classification des groupes cycliques :

Tout groupe cyclique d'ordre $n \in \mathbb{N}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

D'où deux groupes cycliques G et G' sont isomorphes ssi ils ont le même ordre.

Ex : $\mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$, $\forall n$

Sous groupes d'un groupe cyclique :

Soit G un groupe cyclique d'ordre $n \in \mathbb{N}$ alors :

(i) Tout sous groupe de G est cyclique

(ii) Pour tout diviseur de n, il existe un unique sous groupe H_d d'ordre d : $H_d = \{x \in G, x^d = e\}$.

Ex : Les sous groupes de $\mathbb{Z}/20\mathbb{Z}$ sont :

$H_1 = \{\bar{0}\}$ $H_2 = \{\bar{0}, \overline{10}\} = \langle \overline{10} \rangle$ $H_3 = \{0, \bar{5}, \overline{10}, \overline{15}\} = \langle \bar{5} \rangle$ $H_4 = \langle \bar{4} \rangle$ $H_{10} = \langle \bar{2} \rangle$

$H_{20} = \langle \bar{1} \rangle = \mathbb{Z}/20\mathbb{Z}$.

Appl : Détermination des éléments d'ordre 6 dans $\mathbb{U}_{30}$: Il y en a 2 qui sont : $\exp(i\pi/3)$ et $\exp(5i\pi/3)$

bien compris ça c'est sympa mais ça n'a pas l'air d'en vrai pour c'est dangereux

Appl : $\forall n \geq 1$, $n = \sum_{n \mid d} \varphi(d)$.

2. Groupes abéliens finis [Com]

Exs de groupes abéliens finis : (1) Soit G un groupe fini contenant que des éléments d'ordre 2 alors G est abélien.

(2) Soit G un groupe d'ordre p^2 avec p premier alors G est abélien.

Décomposition cyclique d'un groupe abélien fini :

Prop : Soit G un groupe abélien fini d'ordre $n \geq 2$ alors il existe des entiers $(q_i)_{1 \leq i \leq k}$

$$G = \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_k\mathbb{Z} \quad \text{avec } 1 < q_1 \mid q_2 \mid \dots \mid q_k.$$

Cette suite $(q_1, \dots, q_k)$ est la suite d'invariants de G.

Cor 1 : Soit G un groupe abélien fini, il existe un élément $a \in G$ dont l'ordre est le ppcm des ordres des éléments de G.

Cor 2 : Soit G un groupe abélien d'ordre $n = p_1^{k_1} \dots p_r^{k_r}$ (décomposition en facteurs premiers de n) alors :

(i) Pour tout diviseur d de n, il existe un sous groupe de G d'ordre d.

(ii) Pour $i = 1, \dots, k$, pour chaque diviseur de $p_i^{k_i}$ (n de la forme), il existe un seul sous groupe H_i d'ordre $p_i^{k_i}$ et $G = H_1 \times \dots \times H_r$

Ex : $G = (\mathbb{Z}/60\mathbb{Z}) \times (\mathbb{Z}/72\mathbb{Z}) \simeq (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/360\mathbb{Z})$ et $12 \mid 360$.

III. GROUPES NON ABÉLIENS FINIS

Produit semi direct : [Per] + [Com]

Soient H, N 2 groupes, soit $\varphi : H \to Aut(N)$ un morphisme qui définit une action de groupe de H sur N par :

$\forall h \in H, \forall n \in N, \ h \cdot n = \varphi(h)(n)$

Alors $G = N \times H$ muni de la loi de composition interne : $(n, h)(n', h') = (n \varphi(h)(n'), hh')$ est un groupe que l'on note $N \rtimes_\varphi H$. → dans l'autre sens $\ltimes_\varphi$!!!

Caractérisation du produit semi-direct : Soit G un groupe, H et K deux sous-groupes tels que : [Per]

$H \triangleleft G$, $H \cap K = \{e\}$ $HK = G$

Alors $f : H \times K \to G$, $(h, k) \to hk$ est un isomorphisme du produit semi-direct $H \times_\alpha K$ sur G où $\alpha : K \to Aut(H)$, $k \mapsto (h \mapsto k \cdot hk^{-1})$

1. Thms de Sylow [Com]

Thms de Sylow : G un groupe fini, p un facteur premier de l'ordre n de G et $n = p^k q$ avec $p \wedge q = 1$.

(i) Il existe dans G, un p sous-groupe de Sylow (ie un sous groupe d'ordre p^k)

(ii) Tout p sous-groupe de G est contenu dans un p-sous groupe de Sylow

(iii) Les p sous-groupes de Sylow de G sont tous conjugués

(iv) Le nombre n_p de p-sous groupes de Sylow divise q et vérifie $n_p \equiv 1 [p]$.

Cor : Si H est un p-sous groupe de Sylow de G distingué, c'est le seul p-sous groupe de Sylow et réciproquement.

Ex : Structure d'un groupe fini G d'ordre 153 : On obtient deux possibilités : $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/51\mathbb{Z}$ et $\mathbb{Z}/153\mathbb{Z}$ et finalement G est abélien.

Appl: Si G est un groupe fini d'ordre pq avec p,q premiers 5 et $p<q$. (i) Si $q \not\equiv 1 [p]$ alors G est cyclique et isomorphe à $\mathbb{Z}/pq\mathbb{Z}$. (ii) Si $q \equiv 1 [p]$, à isomorphisme G a deux structures possibles : ou bien G est abélien, cyclique et isomorphe à $\mathbb{Z}/pq\mathbb{Z}$ ou alors $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\theta \mathbb{Z}/p\mathbb{Z}$ où $\theta \in \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}))$ tel que $\theta(\bar{1}) = \nu$ est d'ordre p dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.

Ex: Soit G un groupe fini d'ordre $6 = 2\times3$, $2<3$
$3 \equiv 1 [2]$ et alors : $G \simeq \mathbb{Z}/6\mathbb{Z}$
ou $G \simeq \mathbb{Z}/3\mathbb{Z} \rtimes_\theta \mathbb{Z}/2\mathbb{Z}$

2. Groupes Symétriques [Com]

Def: Soit $E = \{1,2,\dots n\}$, le groupe symétrique S_n est le groupe des bijections de $E \to E$. Son ordre est $n!$

Thm de Cayley: Tout sous groupe fini d'ordre n est isomorphe à un sous groupe de S_n.

Prop: Il existe un unique morphisme $\varepsilon : S_n \to \{-1,+1\}$, son noyau est le groupe alterné A_n.

Prop: S_n est engendré par les transpositions, $\forall n \geq 2$
A_n est engendré par les 3-cycles, $\forall n \geq 3$
Les 3 cycles sont conjugués dans A_n, $\forall n \geq 5$.

Prop: $\forall n > 5$, A_n est simple [Per] DVT②

Prop: $S_n = A_n \rtimes \mathbb{Z}/2\mathbb{Z}$. ← **Prop**: A_5 est le seul groupe simple d'ordre 60.

Rq: Dans l'exemple précédent : le groupe d'ordre 6 non abélien est isomorphe à S_3.

3. Groupes Diédraux [Nou]

Def: Soit G un groupe fini, il est dit diédral s'il est engendré par deux éléments x,y distincts d'ordre respectivement 2 et n et vérifiant $xyx = y^{-1}$.

Prop: Soit G un groupe diédral (même notation que pour la définition) alors $\forall z \in G$, z s'écrit de façon unique $z = x^a y^b$ avec $a \in \{0,1\}$, $b \in \{0,\dots,n-1\}$
En particulier, l'ordre de G est égal à $2n$

Prop: $\forall n \geq 2$, il existe un unique groupe diédral d'ordre $2n$ (à isomorphisme près). On le note D_{2n}.

Prop: $D_{2n} \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. [Per]

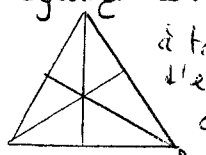
4. Groupes d'ordre 8 : un exemple. [Com]

Soit G un groupe d'ordre 8 :
→ Si G est abélien il est isomorphe à $\mathbb{Z}/8\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^3$ ou $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
→ Si G n'est pas abélien, il est engendré par 2 éléments a,b vérifiant soit → (1) $a^4 = e$, $b^2 = e$, $b^{-1}ab = a^3$ ie $bab = a^{-1}$ et alors $G \simeq D_4$
soit → (2) $a^4 = e$, $b^2 = a^2$, $b^{-1}ab = a^3$ et alors G est isomorphe au sous-groupe de $GL_2(\mathbb{C})$ engendré par $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

IV EN GÉOMÉTRIE (on peut la répartir dans les autres parties)

1. Une autre façon de voir les groupes diédraux [Nou] [Lad]

Def: $\forall n \geq 2$, le groupe D_{2n} est (à isomorphisme près) le groupe des isométries conservant le polygône régulier convexe à n côtés noté P_n.



à titre d'ex et appl.

Ex du triangle: $\mathrm{Isom}(T) \simeq D_6 \simeq S_3$.

Prop: On peut en déduire tous les sous groupes finis de $O_2(\mathbb{R})$:
- $\forall n \geq 1$, $\mathrm{Isom}^+(P_n)$
- $\forall n \geq 2$, D_{2n}.

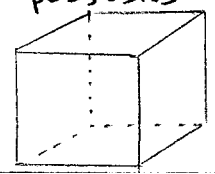
2. Sous groupes finis de $SO_3(\mathbb{R})$ [Orx X-ENS ①]

Prop: Soit G un sous groupe fini de $SO_3(\mathbb{R})$ d'ordre $n \geq 2$: alors, soit
- G est cyclique $\simeq \mathbb{Z}/n\mathbb{Z}$
- G est diédral $\simeq D_{2n}$
- $G \simeq A_4$
- $G \simeq S_5$
- $G \simeq A_5$

3. Coloriage d'un cube [Leh] - [Lad]

Question: Quel est le nombre de façons possibles de colorier un cube avec m couleurs ?

$$n = \frac{1}{24}\left(m^6 + 3m^4 + 12m^3 + 8m^2\right)$$ DVT③



Références :

[Com] Combes Algèbre & Géométrie

[Per] Perrin Cours d'algèbre

[Orx X-ENS] Alg ①-②③

[Nou] Nourdin Agrégation de Mathématiques épreuve orale

[Lad] Ladegaillerie Géométrie

[Leh] Lehman Mathématiques pour l'étudiant de 1ère année. Algèbre & Géométrie.

PLAN. • Il manque ce $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ en plus de $(\mathbb{Z}/n\mathbb{Z}, +)$ avec App RSA pr $n = pq$

• On peut mentionner TR. $G \subset k^*$ $|G| < \infty$ $\Rightarrow$ G est cyclique

• Les cyl. - j° le gp sym, on peut parler de déf
- Galois
- $\exists^{\circ p} = 5$ qui est S_5 comme gp de Galois [PER]

Exos - déterminer à iso près les gp de card 10

abéliens $10 = 2 \times 5$

$\mathbb{Z}/10\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

c'est le m pour le Th chinois

non abélien n_5 le nb de sg d'ordre 5 de G

Sylow : $n_5 = 1[5]$

$n_5 \mid 2 \Rightarrow n_5 = 1$. H ce sg. est $\triangleleft$ $H \triangleleft G$.

$n_2 = 1[2]$

$n_2 \nmid 5 \rightarrow n_2 = 1$ ou 5