Groupes finis. Exemples et applications

I Généralités

1) Définition et premières propriétés

Def : Un groupe $(G,\cdot)$ est dit fini lorsque le cardinal de G est fini. On appelle ordre du groupe ce nombre et on le note $|G|$.

Def : Soit $g\in G$. On appelle ordre de l'élément g le plus entier n tel que $g^n=1_G$. On le note $\mathrm{ord}(g)$.

Th de Lagrange : Soit G un groupe fini et H un sous-groupe de G. Alors $|H|\,|\,|G|$ et $|G|=|H|\times[G:H]$ où $[G:H]$ est l'indice de H dans G et correspond au cardinal de l'ensemble $G/H=\{aH/a\in G\}$.

Cor : $\forall g\in G$, $\mathrm{ord}(g)\,|\,|G|$

Ex : $\mathbb{Z}/6\mathbb{Z}$ groupe fini d'ordre 6 et $\{\bar{0},\bar{3}\}<\mathbb{Z}/6\mathbb{Z}$ d'indice 3

2) Action de groupes finis

Def : On appelle action d'un groupe G (de neutre e) sur un ensemble X une application $\left(\begin{array}{ccc} G\times X & \to & X \\ (g,x) & \mapsto & g\cdot x\end{array}\right)$ telle que $\forall x\in X$, $e\cdot x=x$ et $\forall x\in X$, $\forall g,g'\in G$, $g\cdot(g'\cdot x)=(gg')\cdot x$.

On appelle stabilisateur de $x\in X$ l'ensemble $\mathrm{Stab}(x)=\{g\in G/g\cdot x=x\}$ qui est un sous-groupe de G.
On appelle orbite de $x\in G$ l'ensemble $G(x)=\{g\cdot x/g\in G\}$ qui est un sous-ensemble de X.

Prop : L'ensemble des orbites sous une action par G fournit X. via la relation d'équivalence $x\mathcal{R}x' \Leftrightarrow \exists g\in G$ tq $g\cdot x=x'$.
On note $X/\mathcal{R}$ et l'on parle de représentant sous cette rel^n d'équiv.

Prop : Supposons G fini. Alors $|\mathrm{Orb}(x)|=\dfrac{|G|}{|G:\mathrm{Stab}(x)|}$.

Def : Notons $F(g)=\{x\in X/g\cdot x=x\}$ pour $g\in G$ l'ensemble des éléments de X fixés par g.

Prop : Supposons G et X finis. Alors :
- $\mathrm{card}(G)=\sum_{x\in X/\mathcal{R}} |G(x)|$ (équation aux classes)
- $|G(x)|\cdot|\mathrm{Stab}(x)|=|G|$
- $\mathrm{card}(X/\mathcal{R})$ qui correspond au nombre d'orbites est égal à : $\mathrm{card}(X/\mathcal{R})=\frac{1}{|G|}\sum_{g\in G}\mathrm{card}(F(g))$ (formule de Burnside)

Rq : // via la partition en ensembles disjoints $F=\{(g,x)\in G\times X/g\cdot x=x\}$
// en comptant de 2 manières distinctes

Prop : Une action peut être vue aussi comme la donnée d'une application $\rho\left(\begin{array}{ccc} G & \to & \mathcal{S}_X \\ g & \mapsto & \sigma_g\end{array}\right)$ où $\mathcal{S}_X=\{\text{bijections de } X\to X\}$

Exemple : G est un p-groupe si $|G|=p^l$, p premier, $l\in\mathbb{N}$. Alors
- le centre de G n'est pas réduit à 1_G et son cardinal est congru à 1 modulo p
- les groupes d'ordre p ou p^2 premier sont abéliens
- il existe $\forall k\in\{1,\dots,l-1\}$ un sous-groupe d'ordre p^k de G.

Th de Cayley : Soit G un groupe fini d'ordre n. Alors G est isomorphe à un sous-groupe de $\mathcal{S}_n$

Th de Cauchy : Soit G un groupe fini dont l'ordre est divisible par p premier. Alors il existe un élément d'ordre p.

3) Représentations des groupes finis.

II Exemples et applications

1) Groupes cycliques (fin) et classification des groupes abéliens finis

Déf : Un groupe G est cyclique s'il est fini et s'il existe $a \in G$ tel que $\langle a \rangle = G$ (G monogène via a et a générateur)

Ex : $(\mathbb{Z}/n\mathbb{Z}, +)$ où $n \in \mathbb{N}^*$
$(U_n, \times)$ où $n \in \mathbb{N}^*$ avec $U_n = \{1, \zeta, \dots, \zeta^{n-1}\}$ et $\zeta = e^{\frac{2i\pi}{n}}$.

Prop : Soit G cyclique avec a générateur de G et G d'ordre n.
Alors $f_a : \left(\begin{array}{ccc} \mathbb{Z} & \to & G \\ k & \mapsto & a^k \end{array}\right)$ est un morphisme de groupes surjectif avec $\ker(f_a) = n\mathbb{Z}$. Ainsi $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Rq : Les $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les prototypes de groupes cycliques.

Cor : Deux groupes cycliques sont isomorphes si et ssi $|G| = |G'|$

Prop : Soit G groupe cyclique d'ordre n et $a \in G$ tel que $\langle a \rangle = G$
- a^k est générateur ssi $n \wedge k = 1$
- il existe $\varphi(n)$ générateurs de G
- $\mathrm{Aut}(G) = \{G \to G, x \mapsto x^k \mid k \wedge n = 1\}$ et $\mathrm{Aut}(G) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Ex : Les générateurs de U_{18} sont $\zeta, \zeta^5, \zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{17}$ où $\zeta = e^{\frac{2i\pi}{18}}$

Prop : Le produit de deux groupes cycliques est cyclique ssi leurs ordres sont premiers entre eux.

App : Th de classification des groupes abéliens finis

Th : Soit G un groupe abélien fini.
Alors il existe une unique liste (coefficients) d'entiers naturels ≥ 0 et $\neq 1$ tels que $p_1 | \dots | p_r$ et
$$G \simeq \mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_r\mathbb{Z}$$
Cette liste est appelée les invariants de G

Rq : Découle de la théorie plus générale des modules sur les anneaux principaux.

Cor : Soit E l'exposant de G (le ppcm des ordres). Alors $\exists g \in G$ tq $\mathrm{ord}(g) = e$

Ex : Structure des groupes abéliens d'ordre 600 ?
Lesquels ont des éléments d'ordre 300 ? Combien ?

3?.2) Le groupe symétrique $\mathfrak{S}_n$

Déf : $\mathfrak{S}_n = \{f : [\![1,n]\!] \to [\![1,n]\!] \mid f \text{ bijective}\}$, $n \in \mathbb{N}^*$.

Prop : $\mathfrak{S}_n$ est un groupe fini (sur $\circ$) d'ordre $n!$

Prop : $\mathfrak{S}_n$ est engendré par les transpositions
Tout élément de $\mathfrak{S}_n$ s'écrit en cycles disjoints.

Déf : σ présente une inversion en (i,j) si $1 \leq i < j \leq n$ et $\sigma(j) < \sigma(i)$
Soit N_σ le nombre d'inversions de σ.
On appelle signature de σ l'entier $\varepsilon(\sigma) = (-1)^{N_\sigma}$.
Si $\varepsilon(\sigma) = 1$ on dit que σ est paire et $|A_n| = \frac{n!}{2}$.

Rq : $A_n = \mathfrak{S}_n \cap \{\sigma \in G \mid \varepsilon(\sigma) = 1\} \leq \mathfrak{S}_n$ et $A_n \trianglelefteq \mathfrak{S}_n$

Rq : Etude des ordres des $\sigma \in \mathfrak{S}_n$ en décomposant σ en cycles disjoints :
$\mathrm{ord}(\sigma) = \mathrm{ppcm}$ (longueurs des cycles)

App : Isométries et groupes symétriques

Prop : Soit $\mathrm{Isom}(\mathcal{A})$ le groupe des isométries préservant un tétraèdre régulier (dans un espace affine)
Alors $\mathrm{Isom}(\mathcal{A}) \simeq \mathfrak{S}_4$ et $\mathrm{Isom}^+(\mathcal{A}) \simeq A_4$

Soit $\mathrm{Isom}(\square)$ resp. $\mathrm{Isom}^+(\square)$ le groupe des isométries (resp. isométries directes) préservant un cube.
Alors $\mathrm{Isom}(\square) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{Isom}^+(\square) \simeq \mathfrak{S}_4$

Rq : Via encodage sur les 4 sommets du tétraèdre et sur les 4 grandes diagonales du cube.

Prop : Soit G un groupe fini d'ordre $n \geq 2$ du groupe des isométries directes de l'espace affine E_3.
Alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, à D_n (ou autre),
à A_4, à $\mathfrak{S}_4$ ou à $\mathfrak{S}_5$.

Rq : On peut dresser le tableau des caractères de $\mathfrak{S}_4$ en utilisant ~~l'équivalence~~ $\mathrm{Isom}^+(\square) \simeq \mathfrak{S}_4$.

Rq : $\mathfrak{S}_n \simeq A_n \rtimes \mathbb{Z}/2\mathbb{Z}$

3) Le groupe diédral D_n.

Déf. Soit G un groupe, H et K deux sous-groupes de G.
Soit $\varphi : H \to \mathrm{Aut}(K)$ une action de H sur K où $h.k = \varphi(h)(k)$.
On munit $K \times H$ de la loi : $(k,h)(k',h') = (k\varphi(h)(k'), hh')$
qui fait de $(K \times H, \cdot)$ un groupe appelé produit semi-direct de K par H et est noté $K \rtimes_\varphi H$.

Rq : On note D_n le groupe des symétries du plan euclidien qui laissent invariant un polygone régulier à n côtés.

Rqté : On est obligé des n rotations de centre O (où O désigne le centre du polygone) et d'angle $\frac{2\pi k}{n}$, $k \in [\![0, n-1]\!]$
et des n symétries par rapport aux droites passant par O
et par { les n sommets du polygone si n impair
les milieux des n côtés du polygone si n pair

En particulier, $|D_n| = 2n$

Rq : D_n n'est pas abélien (la composée n'est pas commutative !)

Th : Soit R la rotation de centre O et d'angle $\frac{2\pi}{n}$
S une symétrie d'axe de D_n
Alors $D_n \simeq \langle R \rangle \rtimes \langle S \rangle \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

4) Les groupes linéaires sur les corps finis

Déf : Soit K un corps et E un K-espace vectoriel de dimension finie n.
Le groupe linéaire linéaire $GL(E)$ est le groupe des automorphismes de E. On a alors $GL(E) \simeq GL_n(K)$,
où $GL_n(K)$ le groupe des matrices $n \times n$ inversibles à coeff dans K

Rqté : Lorsque $K = \mathbb{F}_q$ un corps fini, $GL_n(\mathbb{F}_q)$ est fini
et $|GL_n(\mathbb{F}_q)| = (q^n - 1)\cdots(q^n - q^{n-1})$

Déf : On définit le groupe spécial linéaire $SL(E)$ par
$\ker(\det)$ où $\det : \begin{pmatrix} GL(E) \to K^* \\ f \mapsto \det(f) \end{pmatrix}$
Si $K = \mathbb{F}_q$, $SL_n(\mathbb{F}_q) = \frac{|GL_n(\mathbb{F}_q)|}{q-1}$

Déf : On peut définir $PGL(E)$ le groupe projectif linéaire de E
Prop : On a les isomorphismes exceptionnels

$GL_2(\mathbb{F}_2) \simeq SL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$ etc... (suite)

Rq : On peut plonger $\mathfrak{S}_n \hookrightarrow GL_n(\mathbb{F}_2)$

5) p-groupes de Sylow et théorèmes de Sylow

Déf : Soit G un groupe fini d'ordre $p^k m$ où $p \in \mathbb{P}$ et $p \nmid m$
On appelle p-sous-groupe de Sylow (p-Sylow) de G
tout sous-groupe d'ordre p^a.

Ex/Lemme : $GL_n(\mathbb{F}_p)$ admet un p-Sylow : les matrices triangulaires supérieures strictes.

Rq : Le th de Cayley va permettre d'obtenir le diagramme
$G \hookrightarrow \mathfrak{S}_n \hookrightarrow GL_n(\mathbb{F}_p)$

Th de Sylow : Soit G un groupe fini d'ordre $p^k m$, $p \in \mathbb{P}$, $p \nmid m$.
1/ G admet au moins un p-Sylow
2/ Les p-Sylow sont conjugués
3/ Si $n_p = 1$ (p-Sylow), alors $n_p \mid m$ et $n_p \equiv 1 \ [p]$

Conv : Si $n_p = 1$, le p-Sylow est distingué dans G.

Appli : Etude de la simplicité des groupes finis
Etude de la cyclicité des groupes finis

6) Exemples et applications autres

- $\mathbb{H}_8$ le groupe des quaternions : $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$
où $i^2 = j^2 = k^2 = -1$
$ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$

Rqté : $|\mathbb{H}_8| = 8$, il est non abélien car cyclique
$\mathrm{ord}(\pm 1) = 2$ et $\mathrm{ord}(\pm 1) = \mathrm{ord}(\pm j) = \mathrm{ord}(\pm k) = 4$
$\mathbb{H}_8$ n'est pas produit semi-direct.

Th de Wedderburn : Tout anneau intègre fini est commutatif

Réf. Perrin
Combes