104

Groupes finis - Exemples et applications.

Ulmer Théorie des groupes
FGN: Algèbre 2
C: Combes Algèbre et géométrie
Calais Théorie des gpes
Al: Alessandri, Thèmes de géométrie

ETUDE GÉNÉRALE DES GROUPES FINIS

I - DÉFINITIONS ET PREMIÈRES PROPRIÉTÉS

1 - Groupe fini et ordre. Ulmer p2→7 ou Calais

Def 1 : L'ordre d'un groupe G, noté $|G|$, est le cardinal de G.
On dit que G est un groupe fini si $|G|$ est fini. Ds la suite G est fini

Ex 2 : $\mathbb{Z}/n\mathbb{Z}$ est un gpe fini de cardinal n.

Def 3 : On appelle ordre d'un élément $g \in G$, l'ordre du sg engendré par g, $\langle g \rangle$. Il coïncide avec le plus petit entier $n \in \mathbb{N}^*$ tq $g^n = e_G$.

Ex 4 :
- $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$ est d'ordre 2.
- Les racines primitives n-èmes de l'unité sont d'ordre n dans $\mathbb{C}^*$.

FGN p171 38

Def 5 : On appelle exposant de G, le ppcm des ordres des éléments de G, si celui-ci est défini, ou $+\infty$, si les ordres des éléments de G n'ont aucun multiple commun.

Ex 6 : Un gpe fini d'exposant 2 est abélien

Thm 7 : Burnside : Tout sous groupe de $GL_n(\mathbb{C})$ d'exposant fini est fini. DEV → attention : utilise Thm 12

C-ex 8 : $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ est d'exposant fini égal à 2 mais est infini.

2 - Théorème de Lagrange. Ulmer p24→25 ou Calais

Def 9 : Soit G un groupe, H un sous groupe de G. On appelle indice de H dans G et on note $[G:H]$, le cardinal de l'ensemble quotient G/H.

Ex 10 : $[\mathbb{Z} : 2\mathbb{Z}] = 2$

Thm 11 : Soit H un sous groupe de G, alors $|G| = |H|\,[G:H]$.

Thm 12 : Lagrange : Soit G un gpe fini et $H < G$ alors $|H| \mid |G|$.
En particulier, l'ordre d'un elt de G divise toujours l'ordre de G.

C p22

Appl 13 : K, H deux sg de G d'ordre k, m. Si $k \wedge m = 1$ alors $K \cap H = \{e\}$.

3 - Théorème de factorisation de morphismes. C p24 ou Calais

Prop 14 : Soit G un gpe et $H \lhd G$. Soit $\pi : G \to G/H$ le morphisme canonique. Soit $f : G \to G'$ un morphisme de gpes. Si $H \subset \ker f$ alors il existe un unique morphisme $\bar{f} : G/H \to G'$ tq $\bar{f} \circ \pi = f$.
De plus $\ker \bar{f} = \pi(\ker f)$ et $\operatorname{Im} \bar{f} = \operatorname{Im} f$.

pas propre aux gpes finis.

Coro 15 : Soient G, G' deux gpes, $f : G \to G'$ un morphisme de gpes. Alors $G/\ker(f)$ et $f(G)$ sont isomorphes.
Si G et G' sont finis, l'ordre de $f(G)$ divise $|G|$ et $|G'|$.

Ex 16 :
- $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{U}_n$
- $\mathbb{R}/\mathbb{Z} \simeq \mathbb{S}^1$

4 - Actions de Groupes

II CAS DES GROUPES FINIS ABÉLIENS

1 - Groupes cycliques C p59→63 ou Calais p89

Def 17 : On dit qu'un groupe G est cyclique lorsqu'il est monogène et fini. Tout élément a de G tq $G = \langle a \rangle$ est appelé un générateur de G.

Ex 18 : Un gpe d'ordre p premier est cyclique.

Prop 19 : Soit $f \in \operatorname{Hom}(G, G')$ surjectif. Si G est cyclique alors G' l'est.

App 20 : $\mathbb{Z}/n\mathbb{Z}$ est cyclique pour $n \geq 1$, engendré par $\bar{1}$

Prop 21 : Tout gpe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Ex 22 : $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$

Prop 23 : Tout sg d'un gpe cyclique est cyclique

Prop 24 : Soit G un gpe cyclique d'ordre n alors pour tout diviseur d de n, il existe un unique sg de G d'ordre d.

Ex 25 : sg de $\mathbb{Z}/20\mathbb{Z}$.

Thm 26 : Si $G = \langle x \rangle$ est cyclique d'ordre $n \geq 2$, alors les générateurs de G sont les x^k avec $k \wedge n = 1$
Il existe donc $\varphi(n)$ générateurs distincts.

Ex 27 : Les générateurs de $\mathbb{Z}/12\mathbb{Z}$ sont $\bar{1}, \bar{5}, \bar{7}, \overline{11}$.

Coro 28 : Si G est cyclique d'ordre n, le groupe $\operatorname{Aut}(G)$ est d'ordre $\varphi(n)$ et ses éléments sont les applications $\alpha_k : x \mapsto x^k$, $k \in [\![0, n-1]\!]$, $k \wedge n = 1$. C p61

2 - Décomposition en facteurs invariants (Ulmer p107) ou C p66 ou Calais - Thm de structure

Thm 29 chinois : Si m et n sont deux entiers premiers entre eux, $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

App 30 : Si $m \wedge n = 1$ $\varphi(mn) = \varphi(m)\varphi(n)$.

↗ ⚠ Ne pas faire le cas "type fini"

Thm 31 : Soit G un gpe abélien fini d'ordre $n \geq 2$. Il existe des entiers $q_1, \dots, q_k$ tq $q_1 \geq 2$ et $q_1 | q_2 | \dots | q_k$ uniques tq
$G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_k\mathbb{Z}$.

Def 32 : Cette suite $(q_1, \dots, q_k)$ est appelée la suite des invariants de G.

Coro 33 : Soit G abélien d'ordre p^m. Il existe une unique suite $r_1 \leq \dots \leq r_k$ dans $\mathbb{N}^*$ tq $G \simeq \mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_k}\mathbb{Z}$

Coro 34 : Soit G abélien d'ordre $n \geq 2$. $n = p_1^{k_1} \dots p_r^{k_r}$ alors
- pour tout diviseur d de n, il existe un sg de G d'ordre d.
- Pour chacun des $p_i^{k_i}$, $i \in \{1, \dots, k\}$, il existe un seul sg H_i d'ordre $p_i^{k_i}$ et $H_i = \{x \in G, \exists \alpha \ o(x) = p_i^{\alpha}\}$.
  On a $G = H_1 \times \dots \times H_r$.

Ex 35 : Décomposition de $G = (\mathbb{Z}/60\mathbb{Z}) \times (\mathbb{Z}/72\mathbb{Z})$ en $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/360\mathbb{Z}$.

III GROUPES ET SOUS GROUPES REMARQUABLES

1. Actions de groupes — Ulmer ou Calais

p 27-28-29

Def 36 : Une action de G sur X est une application $G \times X \to X$, $g, x \mapsto g.x$ où $g.(h.x) = (gh).x$ et $e.x = x$ pr $g, h \in G$, $x \in X$.

À une action de gpe sur un ensemble X correspond le morphisme
$G \to \mathfrak{S}(X)$
$g \mapsto \sigma_g$ où $\sigma_g(x) = g.x$, $x \in X$.

Def 37 : • L'orbite de x sous G est $Orb(x) = \{g.x, g \in G\}$
• Le stabilisateur de x dans G est $G_x = \{g \in G, g.x = x\} \subset G$.

Rq 38 : $|G| = |G_x| \, |Orb(x)|$.

p 67-68

Thm 39 : Formule des classes : Soit G un gpe fini, $G \curvearrowright X$.
Si $X = \bigsqcup_{i=1}^{r} X_i$ (partit° de X en orbites) et si $x_i \in X_i$ alors
$|X| = \sum_{i=1}^{r} |X_i| = \sum_{i=1}^{r} [G : Orb(x_i)] = \sum_{i=1}^{r} \frac{|G|}{|Orb(x_i)|}$

Thm 40 Formule de Burnside. Pour $g \in G$, on note $X^g = \{x \in X, g.x = x\}$.
Le nb d'orbites de X sous l'action de G est donnée par.
$r = \frac{1}{|G|} \sum_{g \in G} |X^g|$

2. Groupes symétriques. Ulmer et Calais 111

Def 41 : $\mathfrak{S}_n$ est le groupe des permutations de $[\![1, n]\!]$, il est d'ordre $n!$

Thm 42 Cayley : Tout groupe fini d'ordre n est isomorphe à un sg de $\mathfrak{S}_n$. Up 31

Def 43 : σ est un cycle de longueur r si …
• Un cycle de longueur 2 est appelé transposition.
• $supp(\sigma) = \{i \in [\![1, n]\!], \sigma(i) \neq i\}$. U 31

Thm 44 : Toute permutat° $\sigma \neq e$ se décompose en produit de cycles à support disjoint. Cette décomposition est unique à l'ordre des facteurs près.

Thm 45 : Les transpositions engendrent $\mathfrak{S}_n$.

Thm 46 : Pour $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont intérieurs. DEV Ulmer p 49

Def 47 : Il existe un uniq morphisme non trivial de $\mathfrak{S}_n \to \{-1, 1\}$.
Ce morphisme est appelé signature, noté ε et est défini par
$\varepsilon(\sigma) = \prod_{i < j} \frac{\sigma(i) - \sigma(j)}{i - j}$

Prop 48 : Si σ est un produit de k transpositions, $\varepsilon(\sigma) = (-1)^k$.

Def 49 : Le noyau de ε est un sg distingué de $\mathfrak{S}_n$, noté $\mathfrak{A}_n$, le gpe alterné.

Prop 50 : $n \geq 3$, $\mathfrak{A}_n$ est engendré par les cycles de la forme $(1, i, j)$ $i \neq j$. En particulier, il est engendré par les 3 cycles.

Prop 51 : $\mathfrak{A}_n$ est le seul sg d'indice 2 de $\mathfrak{S}_n$.

App 52 : • Isométries du tétraèdre et du cube dev Al p 63
• $\mathfrak{A}_n$ est simple, $n \geq 5$ dev

3. Théorèmes de Sylow — Calais p 207

Def 53 : • On dit que G est un p-gpe si $o(G) = p^n$, p premier, $n \in \mathbb{N}$.
• Si $p | o(G)$, H est un p-sg de G si $o(H) = p^r$, $r \in \mathbb{N}$.
• Si $o(G) = sp^n$ avec $p \wedge s$, tout sg d'ordre p^n de G est appelé p-sg de Sylow de G.

Thm 54 1er thm de Sylow : Si $o(G) = sp^n$, avec p premier $p \wedge s$. Alors pour tout entier $1 \leq r \leq n$, il existe un sg de G d'ordre p^r.

App 55 : Thm de Cauchy : si $p | o(G)$ alors G a au ⊖ un élt d'ordre p

Thm 56 2^{nd} thm de Sylow : si $p | o(G)$ alors. $o(G) = sp^n$ $p \nmid s$

- tout p-sg de G est contenu dans un p-sg de Sylow de G.
- les p-sg de Sylow de G sont conjugués
- le nb de p-sg de Sylow de G est $n_p \equiv 1 [p]$, $n_p | s$.

Cor 57 : G a un unique p-sg de Sylow ssi $S \triangleleft G$.

App 58 : Un gpe d'ordre 42 n'est pas simple.

4- Groupe diédral. Ulmer p8

déf, ordre, générateurs

IV REPRESENTATIONS DES GROUPES FINIS. Ulmer p144

Ulmer, H262 ou Peyre.

déf d'une représentat°, d'un caractère, sous représentat°, irréductible,

décomposit° somme d'irréd.

lemme de Schur, orthogonalité,

table de caractères et prop. + ex