Première partie

Leçon 104 : Groupes finis. Exemples et applications.

Développements :

Automorphismes de S_n, Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

Bibliographie :

Calais, Rombaldi, FGN, Ulmer, Combes, H2G2, Perrin

1 Premiers outils pour l'étude des groupes finis

1.1 Ordre et exposant

Définition 1 (Calais p9). *Groupe fini, ordre du groupe.*

Exemple 2. *Z/nZ, S_n.*

Définition 3 (Calais p30). *Ordre d'un élément.*

Exemple 4. *Le neutre d'ordre* 1. *Transposition d'ordre* 2 *dans S_n. $\overline{1}$ est d'ordre n dans $\mathbb{Z}/nZ$.*

Théorème 5 (Rombaldi p9). *[Ulmer] g d'ordre n si et seulement si l'ordre de g est le plus petit entier naturel non nul tel que $g^n = e$ si et seulement si pour tout $k \in \mathbb{Z}$, on a $g^k = e$ si et seulement si n divise k.*

Proposition 6. *L'ordre de g^k vaut $n = ordre(g)/pgcd(n,k)$.*

Définition 7 (Rombaldi p10). *L'exposant d'un groupe fini est le maximum des ordres de ses éléments.*

Proposition 8 (Rombaldi). *L'exposant d'un groupe abélien fini est le ppcm des ordres de ses éléments.*

Exemple 9 (FGN al2 p185). *$(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ est d'exposant* 2 *mais infini.*
L'exposant de $\mathbb{Z}/n\mathbb{Z}$ est n.

Proposition 10. *Un groupe d'exposant* 2 *est abélien.*

1.2 Notion d'indice et théorème de Lagrange

Définition 11 (Ulmer p24). *[Calais p77] Indice de H dans G*

Exemple 12 (Ulmer p25). $[\mathbb{Z} : 2\mathbb{Z}]$

Proposition 13 (Ulmer p25, Calais p157). *Un groupe d'indice* 2 *est distingué.*

Théorème 14 (Ulmer p25). $|G| = |H|[G : H]$

Théorème 15 (Calais p75). *[Ulmer p25] Théorème de Lagrange*

Corollaire 16 (Calais p75). *L'ordre d'un élément divise l'ordre du groupe.*

Contre exemple 17 (Rombaldi p64 ex 2.17). *$\mathcal{A}_4$ n'a pas d'élément d'ordre* 6.

Application 18 (Combes p22). *Intersection de deux groupes d'ordres premiers entre eux. $\mathbb{U}_k \cap \mathbb{U}_m = \mathbb{U}_{pgcd(k,m)}$.*

2 Cas des groupes abéliens finis

2.1 Premiers exemples

Définition 19 (Romb p13). *[Combes p59] Groupe monogène, groupe cyclique.*

Exemple 20 (Romb p14). *Un groupe cyclique est abélien.*

Exemple 21 (Combes). *$\mathbb{Z}/n\mathbb{Z}$, U_n, groupe de cardinal p premier*

Exemple 22. *$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ est abélien mais pas cyclique.*

2.2 Etude des groupes cycliques

Théorème 23 (Romb p14). *Un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Théorème 24 (Comb p59). *Ordre de a^k, générateur si et seulement si n et k premiers entre eux. $\phi(n)$ générateurs.*

Exemple 25 (Combes p60). *Générateurs de $\mathbb{Z}/12\mathbb{Z}$.*

Proposition 26 (Romb p15). *Un groupe de cardinal p premier est cyclique.*

Théorème 27 (Romb p15). *Un groupe abélien d'ordre pq avec p et q premiers distincts est cyclique.*

Contre exemple 28 (Romb p15). *S_3 d'ordre* 6 *non commutatif.*

Contre exemple 29 (Romb p15). *$(\mathbb{Z}/p\mathbb{Z})^2$ d'ordre p^2 non cyclique.*

Proposition 30 (Combes p61). *Aut(G) d'ordre $\phi(n)$ et ses éléments sont les $x \mapsto x^k$*

Théorème 31 (Romb p16). *Si G cyclique d'ordre n alors les sous-groupes de G sont tous cycliques d'ordre divisant n.*

Exemple 32 (Combes p62). *Sous-groupes de $\mathbb{Z}/20\mathbb{Z}$.*

Contre exemple 33 (Romb p17). *A_4 n'a pas de sous-groupes d'ordre 6.*

Théorème 34 (Romb p17). *Si un groupe abélien fini d'ordre n est cyclique alors pour tout diviseur d de n il existe un unique sous groupe d'ordre d de G.*

Application 35 (Romb p18). $n = \sum_{d|n} \phi(d)$

Théorème 36 (Combes p63). *Théorème des restes chinois. Le produit de deux groupes cycliques est cyclique si et seulement si ils sont cycliques d'ordres premiers entre eux.*

Exemple 37. *$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z}/4\mathbb{Z}$ (pas d'élément d'ordre 4.)*

Application 38 (Combes p63). *Calcul de $\phi(n)$.*

Définition 39 (Combes p64). *Groupe simple.*

Proposition 40 (Combes p64). *Un groupe G est d'ordre p premier si et seulement si il est cyclique et simple.*

2.3 Automorphismes de $\mathbb{Z}/n\mathbb{Z}$

Proposition 41 (Romb p280). *[Combes p206] Aut$(\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.*

Proposition 42. *Expression de $\phi(n)$, ϕ est multiplicative.*

Proposition 43 (Romb p293). *$(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique si et seulement si $n = 2, 4, p^\alpha, 2p^\alpha$.*

Proposition 44 (Perrin). *Si p est premier et $\alpha \geq 3$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \sim \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.*

2.4 Théorème de structure des groupes abéliens finis

Théorème 45 (Combes p66). *Théorème de structure des groupes abéliens finis.*

Définition 46 (Combes p67). *Suite des invariants.*

Corollaire 47 (Combes p67). *Réciproque de Lagrange et décomposition en puissance de nombres premiers.*

Exemple 48 (Combes p68). *$\mathbb{Z}/60\mathbb{Z} * \mathbb{Z}/72\mathbb{Z}$.*

Exemple 49 (Combes). *Groupes d'ordre 600.*

Application 50. *Groupes d'ordre p^2 sont abéliens donc il n'y a que $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

3 Exemples de groupes finis non abéliens

3.1 Les groupes symétriques et alternés

Définition 51 (Romb p39). *$S(E)$*

Proposition 52 (Romb p42). *Tout groupe de permutations d'un ensemble à n éléments est isomorphes au groupe symétrique S_n des permutations de $\{1, .., n\}$. card(S_n).*

Proposition 53. *Pour $n \geq 3$ S_n non abélien*

Théorème 54 (Romb p20). *Théorème de Cayley. Tout groupe fini d'ordre n est isomorphe à un sous-groupe de S_n.*

Définition 55 (Romb p40). *Cycle. Transposition.*

Proposition 56 (Romb). *Un r-cycle est d'ordre r.*

Théorème 57 (Romb p45). *[Combes p79] Décomposition en produit de cycles 2 à 2 disjoints. L'ordre est le ppcm des ordres des cycles.*

Proposition 58 (Romb p46). *S_n est engendré par les transpositions. Détailler d'autres générateurs.*

Proposition 59. *Automorphismes de S_n.*

Proposition 60. *Il existe un unique morphisme de groupes $\epsilon : S_n \mapsto \{-1, 1\}$ non trivial.*

Définition 61 (Romb p51). *Permutation paire, impaire.*

Définition 62 (Romb p51). *Groupe alterné.*

Proposition 63 (Romb p52). *An est engendré par les 3-cycles.*

Proposition 64. *A_n est d'indice 2.*

Proposition 65 (Romb p52). *Pour $n = 3$ ou $n \geq 5$, A_n est simple.*

3.2 En géométrie : le groupe diédral et le groupe des isométries

Définition 66 (Ulmer p8). *Groupe diédral*

Proposition 67 (Ulmer p8). *D'ordre $2n$engendré par s et r.*

Proposition 68. *D_n est composée des symétries d'ordre 2, et la rotation des abscisses est d'ordre n.*

Proposition 69. *Dans D_n les rotations r^k sont donc d'ordre $n/pgcd(k, n)$.*

Proposition 70 (Ulmer p9). *$\langle r \rangle$ est distingué dans D_n car d'indice 2.*

Proposition 71. *Isométries du cube et du tétraèdre.*

4 Actions de groupes

4.1 Actions d'un groupe fini sur un ensemble

Définition 72 (Rombaldi p20)**.** *Soit G opérant sur E. Orbite. Stabilisateur.*

Théorème 73 (Rombaldi p22)**.** *Relation orbite-stabilisateur : $Card(O_x) = [G : G_x]$.*

Théorème 74 (Romb p22)**.** *Equation aux classes avec E fini.*

Application 75. *Soit G un groupe d'ordre 77, agissant sur un ensemble de card 41 alors il existe un point fixe sous cette action.*

Définition 76 (Romb p23)**.** *Points fixes de E sous l'action de G.*

Définition 77 (Romb p23)**.** *p-groupe.*

Application 78 (Romb p23)**.** *Si G de card p^n alors $card(E^G) = card(E) mod p$.*

Application 79 (Romb p24)**.** *Pour tout nombre premier p, le centre d'un p-groupe n'est pas trivial.*

Corollaire 80 (Romb p24)**.** *Tout groupe d'ordre p^2 est abélien.*

Application 81 (Romb p25)**.** *Théorème de Cauchy.*

Théorème 82 (Combes p45)**.** *L'ordre est une puissance de p si et seulement si l'ordre de tout élément est une puissance de p. [Combes p 45]*

Application 83 (H2G2)**.** *Loi de réciprocité quadratique.*

Théorème 84 (Ulmer p68)**.** *Formule de Burnside.*

Application 85 (Combes p44)**.** *Collier de perles.*

4.2 Représentation des groupes

Définition 86 (Romb p179)**.** *Représentation linéaire*

Définition 87 (Romb)**.** *Caractère*

Définition 88 (Romb)**.** *Sous espace G-invariant. Représentation irréductible. Caractère irréductible.*

Théorème 89. *Théorème de Maschke.*

Théorème 90. *Caractère d'une somme directe de représentations.*

Théorème 91. *Orthogonalité des caractères.*

Proposition 92. *Les caractères sont les fonctions centrales.*

Proposition 93. *Table de caractères.*

Exemple 94. *Table de S_4*

Proposition 95. *Les lignes sont orthogonales.*

Définition 96. *Noyau d'une représentation.*

Proposition 97. *Sous-groupes distingués de G en fonction des noyaux.*

Proposition 98. *Caractérisation de G simple.*

Exemple 99. *Sous groupes distingués de S_4 ou A_4 ou D_6.*

Deuxième partie
Plan

1 Quelques propriétés des groupes finis

1.1 Ordre et exposant

1.2 Notion d'indice et théorème de Lagrange

2 Structure des groupes finis

2.1 Parties génératrices

Parler des automorphismes de S_n.

2.2 Cas des groupes abéliens cycliques

Parler des automorphismes de $\mathbb{Z}/n\mathbb{Z}$.

2.3 Théorème de structure des groupes abéliens finis

3 Actions de groupes

3.1 Actions d'un groupe fini sur un ensemble

Parler des groupes d'isométries sur le cube et le tétraèdre.

3.2 Représentations et tables de caractères pour les groupes finis