Leçon 104 - Groupes finis. Exemples et applications.

1. Etude générale des groupes finis. —

1. Ordre et exposant. —

- Def : L'ordre d'un groupe G est le cardinal de son ensemble sous-jacent. On le note $|G|$.
  On dit que G est fini lorsque $|G| \leq +\infty$.
- Ex : $\mathbb{Z}/n\mathbb{Z}$, $Bij(\{1,..,n\})$, $Gl_n(\mathbb{F}_p)$.
- Def : L'ordre d'un élément $g \in G$ est l'ordre de $< g > \subset G$.
- Ex : L'ordre de $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est $\frac{n}{pgcd(n,k)}$.
  Tout élément de $\mathbb{Q}/\mathbb{Z}$ est d'ordre fini, bien que $|\mathbb{Q}/\mathbb{Z}| = +\infty$.
- Pro : Si $g^k = e$ alors $ord(g)|k$.
- Def : Pour G un groupe dont tous les éléments sont d'ordre fini, on note $exp(G) = ppcm(ord(x_i)) \in \mathbb{N}^* \cup \{+\infty\}$ l'exposant de G.
- Ex : $exp(\mathbb{Z}/n\mathbb{Z}) = n$.
  $exp((\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}) = 2$, bien que $|(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}| = +\infty$.
- Pro : $exp(G) = 2 \Rightarrow G$ est abélien.

2. Indice et Théorème de Lagrange. —

- Def : Soit G un groupe et H sous-groupe de G, on note $(G : H)$ le cardinal de l'ensemble quotient G/H, appelé indice de H.
- Ex : L'indice de $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est $pgcd(n,k)$. $(\mathbb{Z} : 2\mathbb{Z}) = 2$.
- App : Tout sous-groupe d'indice 2 est distingué.
- Thm : Soit G un groupe fini et H sous-groupe de G. Alors on a $|G| = (G : H).|H|$.
- App : Théorème de Lagrange : L'ordre de tout sous-groupe de G divise l'ordre de G.
- App : Si H, K sont des sous-groupes de G avec $pgcd(|H|, |K|) = 1$, alors $H \cap K = \{e\}$.

3. Actions de groupes. —

- Def : Une action d'un groupe G sur un ensemble X est la donnée d'un morphisme de groupes $\sigma : g \in G \mapsto \sigma_g \in Bij(X)$.
  Pour tout $x \in X$, pour tout $g \in G$, on note $g.x := \sigma_g(x)$.
- Def : L'orbite de x sur G est $Orb(x) := \{g.x,\ g \in G\}$.
  Le stabilisateur de x dans G est $Stab(x) := \{g \in G \text{ tq } g.x = x\}$.
  L'ensemble des points fixes de g sur X est $X^g := \{x \in X \text{ tq } x.g = g\}$.
- Ex : On fait agir $\mathbb{Z}/n\mathbb{Z}$ sur $\mathbb{N}^n$ par décalage : $\overline{k}.(x_1,..,x_n) = (x_{\overline{1+k}},..x_{\overline{1+k}})$.
- Ex : On fait agir G sur G par conjugaison : $g.x = gxg^{-1}$.
- App : Théorème de Cayley : Soit G un groupe fini. Il existe un sous-groupe transitif de $Bij(\{1,..,|G|\}$ isomorphe à G.
- Pro : Si G est fini, $|G| = Card(Orb(x)).Card(Stab(x))\ \forall x \in X$.
- Pro : (Formule des classes) Soit G un groupe fini agissant sur un ensemble fini X, et soit $X = \mathbb{U}_{i=1}^r X_i$ la partition de X en orbites sous l'action de G. Pour $x_i \in X_i$, on a : $|X| = \sum_{i=1}^r |X_i| = \sum_{i=1}^r (G : Stab(x_i)) = \sum_{i=1}^r \frac{|G|}{|Stab(x_i)|}$.
- Cor : (Formule de Burnside) Le nombre r d'orbites de X sous l'action de G est : $r = \frac{1}{|G|} \sum_{g \in G} |X^g|$.

2. Cas des groupes finis abéliens. —

1. Groupes cycliques. —

- Def : Un groupe G est cyclique lorsqu'il est fini et engendré par un seul élément. Tout élément $a \in G$ tel que $< a >= G$ est appelé générateur de G.
- Ex : $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n, engendré par $\overline{1}$.
  Le groupe des racines n-ièmes de l'unité U_n est cyclique d'ordre n, engendré par $exp^{\frac{2i\pi}{n}}$.
  Le groupe des inversibles de l'anneau $\mathbb{Z}/p\mathbb{Z}$ est cyclique d'ordre p-1.
- Pro : Soit G cyclique et a un générateur de G.
  Pour tout $k \geq 1$, a^k est d'ordre $\frac{n}{pgcd(k,n)}$.
  Ainsi, a^k est un générateur de G ssi $pgcd(k,n) = 1$.
  Il existe alors $\phi(n) := Card((\mathbb{Z}/n\mathbb{Z})^\times)$ générateurs de G.
- Ex : Les générateurs de $\mathbb{Z}/12\mathbb{Z}$ sont $\overline{1}, \overline{5}, \overline{7}, \overline{11}$.
- Cor : Deux groupes cycliques G, G' sont isomorphes ssi ils ont le même ordre.
  Pour G cyclique, il existe $\phi(n)$ automorphismes de groupes sur G.
- Pro : Pour G cyclique, tout sous-groupe de G est cyclique. Pour tout $d||G|$, il G possède un unique sous-groupe d'ordre d.

2. Théorème de structure. —

- Théorème de structure des groupes abéliens finis : Soit G abélien fini.
  Alors il existe des entiers $d_1|..|d_r$ tels que $G \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times .. \times (\mathbb{Z}/d_r\mathbb{Z})$.
  De plus, les d_i sont uniques. On les appelle facteurs invariants de G.
- Ex : Un groupe abélien d'ordre 600 est isomorphe à $(\mathbb{Z}/10\mathbb{Z}) \times (\mathbb{Z}/60\mathbb{Z})$,$(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/120\mathbb{Z})$,$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/300\mathbb{Z})$, ou $\mathbb{Z}/600\mathbb{Z}$.
- Cor : On a $exp(G) = d_r$.
  Pour tout d tel que $d||G|$, G possède un sous-groupe d'ordre d.

3. Groupes et sous-groupes remarquables. —

1. Groupes symétriques et alternés. —

- Def : On définit le n-ième groupe symétrique Σ_n par $\Sigma_n := Bij\{1,..,n\}$.
- Def+Pro : Pour $2 \leq k \leq n$, $\sigma \in \Sigma_n$ est un k-cycle ssi l'action de $< \sigma >$ sur $\{1,..,n\}$ ne possède qu'une orbite non-réduite à un seul élément, et que cette orbite est de cardinal k.
  Les 2-cycles sont aussi appelés transpositions. Soit i dans cette orbite. Pour tout autre j dans l'orbite, il existe r tq $j = \sigma^r(i)$.
  On note alors $\sigma := (i, \sigma(i), .., \sigma^{k-1}(i))$.
- Def : Pour $\sigma \in \Sigma_n$, on définit le support de σ, $Supp(\sigma)$ comme la réunion des orbites de $< \sigma >$ non-réduites à un élément.

- Ex : $n = 6$, $\sigma = (1,2)(4,5,3)$. $Supp(\sigma) = \{1,2,3,4,5\}$.
- Pro : Pour $n \geq 3$, Σ_n n'est pas abélien.
  On a $(1,2)(1,2,3) = (2,3) \neq (1,2,3)(1,2) = (1,3)$.
- Pro : Deux permutations ayant des supports disjoints commutent.
- Thm : Toute permutation $\sigma \in \Sigma_n$ s'écrit comme produit de cycles à support disjoints.
  Cette écriture est unique à l'ordre près.
- Def+Pro : On définit l'application signature sur Σ_n par :
  $\varepsilon : \sigma \in \Sigma_n \mapsto \begin{cases} 1 \text{ si } \sigma \text{ est un produit de carrés} \\ -1 \text{ sinon} \end{cases}$.
  ε est un morphisme de groupes de Σ_n vers $\{-1,1\}$, de noyau l'ensemble des produits de carrés de permutations.
- Def : On appelle n-ième groupe alterné A_n le sous-groupe de Σ_n qui engendré par les carrés.
- Rem : A_n est un sous-groupe distingué de Σ_n.
- Pro : On a $\varepsilon((i,j)) = -1$.
  Ainsi, pour tout $n \geq 2$, A_n est un sous-groupe strict de Σ_n, de cardinal $\frac{n!}{2}$.
- Pour $n = 2$, $A_2 = \{Id\}$. Pour $n = 3$, $A_3 = \{Id, (1,2,3), (1,3,2)\} \simeq \mathbb{Z}/3\mathbb{Z}$.
- Cor : Pour $\sigma = c_1..c_r$, avec c_i de longueur m_i, on a $\varepsilon(\sigma) = \Pi_i(-1)^{m_i}$.
- Pro : On a aussi : $\varepsilon(\sigma) = \Pi_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$
- Pro : Pour tout $n \geq 3$, A_n est $(n-2)$-transitif, engendré par les 3-cycles.
- **Dev** : Pour tout $n \geq 5$, le groupe alterné A_n est simple.

2. p-groupes et théorème de Sylow. —

- Def : Soit p premier. Un p-groupe est un groupe de cardinal une puissance de p.
- Pro : Soit G un p-groupe et X un ensemble fini sur lequel G agit. Alors $|X^G| \equiv |X|$ $mod(p)$.
- App : Théorème de Cauchy : Soit G un goupe fini et p premier divisant $|G|$. Alors G possède un élément d'ordre p.
- Cor : Un groupe G est un p-groupe ssi l'ordre de tout élément est une puissance de p.
- Pro : Pour G un p-groupe et $Z(G)$ son centre, on a $|Z(G)| \equiv 0$ $mod(p)$.
- Pro : Les p-groupes de cardinal p ou p^2 sont toujours abéliens.
- Def : Soit G un groupe fini de cardinal n. Soit p premier divisant n. Un sous-groupe H de G est un $p - Sylow$ de G ssi $|H| = p^{v_p(n)}$.
- Ex : Le groupe $UT_n(\mathbb{F}_p)$ des matrices trigonales supérieures avec des 1 sur la diagonale est un p-Sylow de $Gl_n(\mathbb{F}_p)$.
- Pro : Soit G un groupe et H un sous-groupe de G. Soit S un p-Sylow de H. Alors il existe un p-Sylow S' de G tel que $S = S' \cap H$.
- Théorèmes de Sylow : Soit G un groupe fini de cardinal n, et p premier divisant n.
  i) G admet un p-Sylow.
  ii) Tous les p-Sylow de G sont conjugués.
  iii) Le nombre n_p de p-Sylow de G vérifie $n_p | \frac{n}{p^{v_p(n)}}$ et $n_p \equiv 1$ $mod(p)$.
- App : Un p-Sylow de G est distingué ssi $n_p = 1$.
- App : Tout groupe d'ordre 63 possède un sous-groupe distingué non-trivial.
- App : Tout groupe d'ordre pq avec $p < q$ premiers et $q \neq 1$ $mod(p)$ est cyclique.

3. Groupes diédraux. —

- Def : Soit $n \geq 2$. Dans le plan complexe $\mathbb{C}$ identifié $\mathbb{R}^2$, considérons le polygone régulier connexe P_n à n sommets, formé par les affixes des $exp^{2i\pi\frac{k}{n}}$.
  Le groupe diédral D_n est le sous-groupe des isométries affines du plan qui laissent P_n invariant.
- Pro : D_n est d'ordre $2n$, et il est engendré par la symétrie axiale s et la rotation d'angle $\theta = \frac{2\pi}{n}$ données par $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $r = \begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix}$.
  Ces générateurs satisfont aux relations $r^n = e$, $s^2 = e$ et $srsr = e$.
  Les éléments de D_n sont ainsi exactement les $r^k.s^\varepsilon$ avec $0 \leq k \leq n-1$ et $\varepsilon \in \{0,1\}$.
  Le sous-groupe $< r >$ est d'ordre n et distingué dans D_n.
- Pro : $D(D_{2m}) =< r^2 >$ et $D(D_{2m+1}) =< r >$.
- App : Les classes de conjugaison de D_n sont de la forme $\{r^k, r^{-k}\}$ ou $\{s.r^k, s.r^{-k}\}$ pour $0 \leq k \leq n-1$. Si n est pair il y a 3 classes de conjugaisons avec 1 élément. Il n'y en a qu'une si n est impair.

4. Représentations des groupes finis. —

- Def : Une représentation linéaire ρ sur un groupe fini G est un morphisme de groupes $\rho : G \to GL(V)$ où V est un $\mathbb{C} - ev$ de dimension finie.
- Def : Le caractère χ_ρ d'une représentation linéaire ρ est l'application $g \in G \mapsto \chi_\rho(g) := Tr(\rho(g)) \in \mathbb{C}$.
- Def : Une sous-représentation d'une représentation $\rho : G \to GL(V)$ est une représentation $\rho' : G \to GL(V')$ avec V' s-ev de V tel que $\forall g \in G$, V' est $\rho(g)$-stable avec $\rho(g)|_G = \rho'(g)$.
  Une représentation est dite irréductible si elle n'admet aucune sous-représentation stricte non-triviale.
  Un caractère irréductible est le caractère d'une représentation irréductible.
- Pro : Caractère d'une somme directe de représentations.
- Pro : Orthogonalité des caractères irréductibles pour le produit scalaire donné.
- Pro : Les caractères sont des fonctions centrales.
- Def : Table de caractères.
- Pro : Les colonnes d'une table de caractères sont orthogonales.
- Ex : Table de caractères de Σ_4, d'un groupe cyclique.
- **Dev** : Soit G un groupe d'ordre n. Soient $\rho_1, ..., \rho_r$ un ensemble de représentants des classes d'isomorphie des représentations irréductibles de G, et soient $\chi_1, ..., \chi_r$ les caractères irréductibles associés.
  On note $K_{\chi_i} := \{g \in G \text{ tq } \chi_i(g) = \chi_i(e)\}$.

Alors $K_{\chi_i} = Ker(\rho_i)$ et les sous-groupes distingués de G sont exactement les $\cap_{i\in I} K_{\chi_i}$, pour tout $I \subset \{1, ;r\}$.

- Cor : G est simple ssi pour tout caractère irréductible χ non-trivial et $\forall g \neq e$ on a $\chi(g) \neq \chi(e)$.
- App : V_4 est le seul sous-groupe distingué non-trivial de A_4. (Table de caractères en annexe)
- App : Sous-groupes distingués de D_6. (Table de caractères en annexe)

Références

Perrin : Sous-groupes distingués, propriétés. p-Sylow, application au premier th de Sylow.
Ulmer : Ordre d'un groupe, d'un élément, exemples. Indice, propriétés, Th de Lagrange, exemples. Action de groupe, stabilisateur, orbites, formule des classes, propriétés, exemples. Groupe symétrique, support, cycle, propriétés, signature, groupe alterné. p-groupes, Th de Cauchy. Groupes diédraux, générateurs, classes de conjugaison, exemples. Représentations des groupes finis. Sous-groupes distingués et caractères d'un groupe.(Dev)
Lang : A_n est simple.(Dev)
Combes : Groupe cyclique, propriétés, exemples. Th de structure des groupes abéliens finis.
FGN (Algèbre 2) : Exposant d'un groupe, exemples.
Peyré : Représentations des groupes finis.

September 18, 2017

Vidal Agniel, École normale supérieure de Rennes