Leçon 104: Groupes finis. Exemples et applications.

Les groupes seront noté multiplicativement et l'élément neutre 1.

1 Généralités sur les groupes finis

1.1 Notion d'ordre

Définition 1 (TL1 p118)**.** Un groupe $(G, .)$ est dit fini si G est de cardinal fini. On appelle alors ordre de $(G, .)$ ce cardinal.

Définition 2 (BER 151)**.** L'ordre d'un élément $g \in G$ est l'ordre de $< g >$. Autrement dit, c'est le $min\{n \in \mathbb{N}^* | g^n = 1\} \in \mathbb{N}^* \cup \{+\infty\}$.

Exemple 3. $(Z/nZ, +)$ ordre n + ordre d'un élément.

Proposition 4 (ROM 2)**.** Soit H un sous-groupe non vide de G. La relation donné par $g_1 \sim g_2 \iff g_1^{-1} g_2 \in H$ est une relation d'équivalence.

Notation 5 (ROM)**.** On notera $\overline{g} = gH$ la classe d'équivalence de $g \in G$. L'ensemble des classes d'équivalence est noté G/H et on l'appelle l'ensemble des classes à gauche modulo H, c'est à dire $G/H = \{\overline{g} | g \in G\}$.

Remarque 6 (ROM)**.** On peut définir de la même manière la relation d'équivalence $g_1 \sim g_2 \iff g_1 g_2^{-1} \in H$. L'ensemble des classes Hg forme alors l'ensemble noté $H \setminus G$ des classes à droite modulo H. Si G est commutatif, les deux définitions sont les mêmes.

Définition 7 (ROM)**.** Soit H un suos groupe de G. Le cardinal de l'ensemble G/H est noté $[G : H]$ et on l'appelle l'indice de H dans G.

Théorème 8 (ROM 2)**.** [Théorème de Lagrange] Soient G un groupe fini d'ordre $n \geq 2$ et H un sous-groupe de G. Pour tout $g \in G$ on a $card(gH) = card(H)$ et $card(G) = [G : H]card(H)$, donc l'ordre de H divise celui de G.

Corollaire 9 (no ref)**.** L'ordre d'un élément de G divise l'ordre de G.

1.2 Sous-groupe distingué et simplicité

Définition 10. On dit que H est un sous-groupe distingué (ou normal) de G si pour tout $g \in G$, on a $gH = Hg$.

Proposition 11. Un sous-groupe H de G est distingué si et seulement si pour tout $g \in G$ on a $gHg^{-1} = H$.

Exemple 12. $\{1\}$ et G sont toujours des sous-groupes distingué de G.
Si G est commutatif, tout sous-groupe est distingué.

Définition 13. Un groupe G est dit simple si ses seuls sous-groupes distingués sont $\{1\}$ et lui-même.

Proposition 14 (BER 149)**.** Tout sous-groupe de G d'indice 2 est distingué dans G.

Contre-exemple 15 (A voir si je laisse là, si mettre ailleurs, ou si juste avoir en tête)**.** Le groupe alterné $\mathcal{A}_6$ qui est d'ordre 12 ne contient pas de sous-groupe d'ordre 6. Ce résultat montre que la réciproque du théorème de Lagrange est fausse.

2 Action de groupe

Définition 16 (Rom 19 E–> X ; TL2 58)**.** On dit que G opère à gauche sur X si on a une application de $G \times X$ dans X, notée $(g, x) \mapsto g \cdot x$ telle que :

1. $\forall g, h \in G, \forall x \in X, c \cdot (h \cdot x) = (gh) \cdot x$
2. $\forall x \in X, 1 \cdot x = x$

Une telle application est appelée action à gauche de G sur E. On peut définir de manière analogue l'action à droite.

Exemple 17 (TL2 66)**.** Considérons l'action $(g, h) \in G^2 \mapsto ghg^{-1}$. On peut définir cette action pour tout groupe G, on dit que G agit sur lui-même par conjugaison.

Définition 18 (TL2 65, 69)**.** Pour tout $a \in X$, l'orbite de a sous l'action de G est : $Orb(a) = \{g \cdot a | g \in G\}$.
L'ensemble des $g \in G$ laissant fixe x est appelé stabilisateur de x. Il et noté $Stab(x)$. Autrement dit $Stab(x) = \{g \in G | g \cdot x = x\}$.

Théorème 19 (ROM 21, TL2 73)**.** Pour tout $x \in X$

1. $g \mapsto g \cdot a$ de G dans X induit une bijection de $G/Stab(a)$ sur $Orb(a)$.
2. L'orbite $G \cdot a$ est finie si et seulement si l'indice $[G : Stab(a)] = [G : Stab(a)]$
3. Si G est fini, $Orb(a)$ est également fini et $|Orb(a)| = \frac{|G|}{|stab(a)|}$

Blabla : On parlera plus en détail du groupe $\mathfrak{S}$ par la suite.

Proposition 20 (CAL 303)**.** Si G est un groupe fini agissant sur X, le cardinal de l'ensemble de ces orbites vérifie :

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$$

Application 21 (DEV 1)**.** Soit G un groupe d'ordre n et $Z(G)$ son centre. On note p_G la probabilité que deux éléments h, g de G choisis indépendamment et de façon équiprobable commutent.

1. Si G est non abélien, $p \leq \frac{5}{8}$
2. Si k est le nombre de classe de conjugaison, alors $p = \frac{k}{n}$

3 Autour de $\mathbb{Z}/n\mathbb{Z}$

3.1 Le groupe additif $\mathbb{Z}/n\mathbb{Z}$ et cyclicité

Proposition 22 (No ref, BER 32 un peu)**.** $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe additif, où $(\overline{a}, \overline{b}) \mapsto \overline{a} + \overline{b} = \overline{a + b}$.

Définition 23. On dit qu'un groupe fini G est cyclique si il existe un élément g de G tel que $G =< g >$.

Proposition 24 (TL1 131, ROM 280, BER 32, mixte)**.** Pour tout $n \geq 1$, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique d'ordre n. Ses éléments sont $\overline{0}, \overline{1}, ..., \overline{n-1}$.

Théorème 25 (ROM 14, BER 156)**.** Soit G un groupe cyclique d'ordre n. Alors il est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Proposition 26 (ROM 283)**.** Soit $a \in \mathbb{Z}$. LASSE :

1. $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$
2. a est premier avec n
3. $\overline{a}$ est un générateur du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$

Proposition 27 (ROM 14)**.** Si $G =< g >$ est un groupe cyclique d'ordre n, alors ses générateurs sont les g^k, où $1 \leq k \leq n-1$ est premier avec n.

Proposition 28 (No ref)**.** G cyclique ssi il admet un élément g d'ordre $card(G)$. On a alors $G =< g >$.

Corollaire 29 (un peu ROM p14)**.** Un groupe d'ordre premier est cyclique, et tout ses éléments sont générateurs.

Exemple 30. Soit $n \in \mathbb{N}^*$. L'ensemble des racines complexes n-ième de l'unité $\mathbb{U}_n$ est cyclique engendré par $e^{\frac{2i\pi}{n}}$. Il est donc d'ordre n et ainsi on a $\mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

Proposition 31 (No ref)**.** Tout sous groupe d'un groupe cyclique est cyclique.

3.2 Théorème de structure

Théorème 32 (thm chinois)**.** [TL1 149] Soient $m_1, .., m_r \geq 2$ des entiers premiers entre eux deux à deux ($r \geq 2$). On note M leur produit. Étant donné des entiers $a_1, .., a_r$, considérons le système de congruences :
$(S) : x \equiv a_i \ [m_i] \ (i = 1, ..., r)$
Ce système possède une solution $x \in \mathbb{Z}$ qui est unique modulo M.

Corollaire 33 (TL1 150)**.** Soient $m_1, .., m_r \geq 2$ des entiers premiers entre eux deux à deux ($r \geq 2$). On note M leur produit. On a alors :

$$\mathbb{Z}/M\mathbb{Z} \simeq \mathbb{Z}/m_i\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}$$

Théorème 34 (BER 364)**.** [théorème de structure des groupes abéliens de type fini, ADMIS] Soit G un groupe abélien de type fini. Alors, il existe des entiers $r, s \leq 0$ et des entiers $d_1, .., d_s \leq 2$ vérifiant $d_1|...|d_s$ tels que

$$G \simeq \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_s\mathbb{Z}$$

Exemple 35 (No ref)**.** Classification des groupes abéliens de petit ordre
Faire tabelau, cf Ewna

3.3 Groupe multiplicatif

Proposition 36. $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ est un groupe, c'est l'ensemble des éléments inversible de $\mathbb{Z}/n\mathbb{Z}$.

Proposition 37. Soient $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$ d'ordre respective $o(a), o(b)$. Alors si $o(a)$ et $o(b)$ sont premiers entre eux, on a $o(ab) = o(a)o(b)$.

Lemme 38. Notons $m = ppcm(\{o(x)|x \in (\mathbb{Z}/n\mathbb{Z})^\times\}$. Alors $(\mathbb{Z}/n\mathbb{Z})^\times$ possède un élément d'ordre m.

Théorème 39. Soit $p \geq 3$ premier. Alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

Remarque 40. Déterminer ces générateurs est un problème "difficile".

Théorème 41 (cf preuve Rostam ou EWna)**.** Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

Corollaire 42. $\mathbb{F}_p^*$ est cyclique, et on a même $\mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

4 Un groupe non abélien : $\mathfrak{S}(E)$

On suppose connues les premières notions autour de $\mathfrak{S}(E)$ (définition, support, orbites, cycles, transpositions, signature).

4.1 Générateurs de $\mathfrak{S}(E)$

Lemme 43. Soit ω une σ-orbite à p éléments et soit $a \in \omega$. Alors, p est le plus petit entier positif tel que $\sigma^p(a) = a$ et on a $w = \{a, \sigma(a), ..., \sigma^{p-1}(a)\}$.

Lemme 44. Soit $\omega \in \Omega^*$. On définit $\sigma_\omega \in \mathfrak{S}(E)$ par $\sigma_\omega(a) = \sigma(a)$ si $a \in \omega$ et $\sigma_\omega(a) = a$ si $a \notin \omega$. Alors σ_ω est un cycle de support ω, et pour tout $a \in \omega$, on a $\sigma_\omega = (a \ \ \sigma(a) \ ... \ \sigma^{p-1}(a))$, où p est lenombre d'éléments dans ω.
De plus, tout p-cycle est de cette forme.

Théorème 45 (BER 204, ROM42 DEV 1)**.** Soit $\sigma \in \mathfrak{S}(E)$. Alors σ se décompose en produit de cycles à support disjoints, et cette décomposition est unique à l'ordre des facteurs près. Cette décomposition est donnée par : $\sigma = \prod_{\omega \in \Omega^*} \sigma_\omega$ où Ω^* représente l'ensemble des σ-orbites non réduite à un singleton.

Corollaire 46 (BER 206, DEV 1)**.** $\mathfrak{S}(E)$ est engendré par

1. les cycles.
2. les transpositions.

Corollaire 47 (BER 207, DEV 1)**.** $\mathfrak{S}_n$ est engendré par

1. les transpositions $(k \ k+1)$ pour $1 \leq k \leq n-1$
2. les transpositions $(1 \ k+1)$ pour $1 \leq k \leq n-1$
3. (12) et $(1 \ 2 \ ... \ n \ )$

Exemple 48. $(12345678)(43265871)$ a pour décomposition en cycle $(1468)(23)$ et pour décomposition en transposition $(14)(46)(68)(23)$

On peut alors cité un résultat en lien avec les groupes et $\mathfrak{S}(E)$ qui montre l'importance de cet exemple

Application 49 (ROM 53)**.** [Cayley] Tout groupe G est isomorphe à un sous groupe de $\mathfrak{S}(G)$.

4.2 Le sous groupe alterné

Définition 50. Le groupe alterné, noté $\mathfrak{A}_n$, est l'ensemble des permutations de $\mathfrak{S}_n$ de signature 1.

Proposition 51. $\mathfrak{A}_n$ est un sous groupe distingué de $\mathfrak{S}_n$ de cardinal $\frac{n!}{2}$.

Exemple 52. La sginature d'un p-cycle σ est $(-1)^{p-1}$.

Proposition 53. Si $n \geq 3$, le groupe alterné $\mathfrak{A}_n$ est engendré par chacune des familles suivantes :

1. les produits de deux transpositions
2. les 3-cycles.

Théorème 54 (DVP 2)**.** Soit $n \geq 3$. Le groupe alterné $\mathfrak{A}_n$ est simple si et seulement si $n \neq 4$.