Leçon 104 : Groupes finis. Exemples et applications.

Tout groupe G sera noté multiplicativement.

I Généralités

Soit G un groupe. e son élément neutre.

I.1 Ordre d'un élément

[Rom21]

Déf 1. L'ordre de $g \in G$ est $\text{ord}(g) := |< g >| \in \mathbb{N}^* \cup \{+\infty\}$, où $< g >$ désigne le sous-groupe de G engendré par g. Si $\text{ord}(g) < +\infty$, on dit que g est d'ordre fini.

Thm 2 (Lagrange)**.** Si G est fini, alors pour tout sous-groupe H de G, $|H| \,|\, |G|$. Entre autre, l'ordre de tout élément de G divise $|G|$.

Prop 3. Si φ est un isomorphisme de groupes de G dans un groupe G', alors $\text{ord}(\varphi(g)) = \text{ord}(g)$, pour tout $g \in G$.

Thm 4. Soient $g \in G$ et $\varphi : k \in \mathbb{Z} \mapsto g^k \in G$. Si g est d'ordre fini, alors $\text{Ker}(\varphi_g) = \text{ord}(g)\mathbb{Z}$.

Cor 5. Soient $g \in G$ et $n \in \mathbb{N}^*$. Alors sont équivalents :

i) $\text{ord}(g) = n$.

ii) $g^n = e$, et pour tout $1 \leq k < n$, $g^k \neq e$.

iii) Pour $k \in \mathbb{Z}$, $g^k = e$, si et seulement si, k est un multiple de n.

Cor 6. Si $g \in G$ est d'ordre fini, alors $g^{|G|} = e$.

App 7 (petit théorème de Fermat)**.** Pour tout $x \in \mathbb{Z}\backslash\{0\}$, pour tout p premier, $x^{p-1} \equiv 1 \pmod{p}$.

Prop 8. Soient $g, h \in G$ d'ordre fini, et $k \in \mathbb{Z}\backslash\{0\}$. Alors :

1. $\text{ord}(g^k) = \dfrac{\text{ord}(g)}{\text{pgcd}(\text{ord}(g), k)}$.
2. Si $gh = hg$, alors $\text{ord}(gh) \,|\, \text{ppcm}(\text{ord}(g), \text{ord}(h))$. On a égalité si $< g > \cap < h >= \{e\}$.

Thm 9. Si G est abélien. Soient $r \geq 2$, $g_1, \ldots, g_r \in G$, deux à deux distincts, d'ordres finis respectifs $m_1, \ldots, m_r$. Alors il existe dans G un élément g_0 d'ordre égal au ppcm de ces ordres.

Cor 10. Si G est abélien fini, on note $\exp(G) := \max_{g \in G} \text{ord}(g)$, appelé exposant du groupe. Alors $\exp(G) = \text{ppcm}\{\text{ord}(g) : g \in G\}$.

I.2 Groupes finis opérant sur un ensemble fini

[Odi23] On suppose que G opère sur un ensemble non vide X. Pour $x \in X$, on note $G \cdot x$ son orbite, et $\text{Stab}_G(x)$ son stabilisateur.

Thm 11 (Cayley)**.** Si G est un groupe fini de cardinal n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$, $\mathfrak{S}_n$ désigne le groupe symétrique.

Prop 12. Pour tout $x \in X$, l'application $f_x : \begin{cases} G/\text{Stab}_G(x) & \longrightarrow & G \cdot x \\ g\,\text{Stab}_G(x) & \longmapsto & g \cdot x \end{cases}$ est une bijection.

Cor 13 (Equation des classes)**.** Si G et X sont finis, alors pour tout $x \in X$, $|G| = |G \cdot x|\,|\text{Stab}_G(x)|$

Prop 14. Soient $x, y \in X$. La relation $x \sim y$, si et seulement si, il existe $g \in G$, $g \cdot x = y$, est une relation d'équivalence. Il découle que les orbites de l'action de G sur X forment une partition de X.

Rq 15. Les orbites formant une partition de X, on peut fixer un système de représentant que l'on note Ω.

Cor 16 (Equation aux classes)**.** Si G et X sont finis, alors $|X| = \sum_{x \in \Omega} |G \cdot x| = \sum_{x \in \Omega} \dfrac{|G|}{|\text{Stab}_G(x)|}$

Thm 17 (Formule de Burnside)**.** On suppose G et X finis. Pour tout $g \in G$, on note $\text{Fix}(g) := \{x \in X : g \cdot x = x\}$ l'ensemble des points fixes de g. Alors $|\Omega| = \dfrac{1}{|G|} \sum_{g \in G} |\,\text{Fix}(g)|$.

I.3 p-groupes et p-groupes de Sylow

[Per96] [Ulm21] Soit p un nombre premier.

Notation 18. On note $X^G := \{x \in E : G \cdot x = \{x\}\}$ l'ensemble des éléments de X dont l'orbite est réduite à un point.

Déf 19. On dit que G est un p-groupe si $|G| = p^\alpha$, où $\alpha \in \mathbb{N}^*$.

Prop 20. Soit G un p-groupe agissant sur un ensemble fini X. Alors $|X| \equiv |X^G| \pmod p$.

Cor 21. Le centre d'un p-groupe distinct de $\{e\}$ n'est pas réduit à $\{e\}$.

Thm 22 (Théorème de Cauchy)**.** Soit G un groupe fini d'ordre $n \geq 2$. Si $p \mid n$, alors il existe un élément d'ordre p.

Déf 23. Si G est fini, de cardinal $n := p^\alpha m$, où $p \nmid m$. On appelle p-sous-groupe de Sylow de G un sous-groupe de G de cardinal p^α.

Rq 24. Dire que S est un p-sous-groupe de Sylow de G revient à dire que S est un p-groupe tel que $[G : S]$ est premier à p.

Ex 25 (DEV 1)**.** Soient $\mathbb{F}_p$ le corps fini à p éléments et $n \in \mathbb{N}^*$. Alors l'ensemble des matrices triangulaires supérieurs strictes est un p-sous-groupe de Sylow de $GL_n(\mathbb{F}_p)$.

Lemme 26 (DEV 1)**.** Si G est fini, d'ordre $|G| = n = p^\alpha m$, $p \nmid m$, et soit H un sous-groupe de G. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H

Thm 27 (DEV 1 - Premier théorème de Sylow)**.** Si G est fini, et $p \mid |G|$, alors G contient au moins un p-sous-groupe de Sylow.

Ex 28. Un groupe G d'ordre 36 possède au moins un 3-Sylow S. Celui-ci est de cardinal 9 et d'indice 4 dans G.

Cor 29. Si $|G| = p^\alpha m$, $p \nmid m$, G contient des sous-groupes d'ordre p^i, pour $0 \leq i \leq \alpha$.

Thm 30 (DEV 1 - Deuxième théorème de Sylow)**.** Si $|G| = p^\alpha m$, $p \nmid m$, alors si l'on note n_p le nombre de p-Sylow de G :

1. Si $H \leq G$ est un p-groupe, il existe un p-Sylow S de G contenant H.
2. Les p-Sylow sont tous conjugués.
3. $n_p \equiv 1 \pmod p$. Entre autre, $n_p \mid m$.

Cor 31. Si S est un p-Sylow de G, alors S est distingué dans G, si et seulement si, il est l'unique p-Sylow de G.

App 32. Un groupe d'ordre 200 n'est pas simple.

App 33. Un groupe d'ordre 77 est toujours cyclique.

App 34. Tout groupe d'ordre 85 est isomorphe à $\mathbb{Z}/85\mathbb{Z}$.

II Exemples de groupes finis

II.1 Groupe symétrique

[Rom21] Soit E un ensemble fini de cardinal n non nul.

Déf 35. On appelle groupe des permutations de E, noté $\mathfrak{S}(E)$, le groupe des bijections de E dans lui même. Si $E = \{1, \dots, n\} \subseteq \mathbb{N}$, on le note $\mathfrak{S}_n$, et on l'appelle groupe symétrique.

Prop 36. Si E est de cardinal $n \geq 1$, $|\mathfrak{S}(E)| = n!$.

Prop 37. Le centre du groupe $\mathfrak{S}(E)$ est $Z(\mathfrak{S}(E)) = \mathfrak{S}(E)$ si $|E| = 2$, $\{Id_E\}$ si $|E| \geq 3$.

Prop 38. Soit $\sigma \in \mathfrak{S}(E)$. Le groupe $H = <\sigma>$ agit sur E par $\sigma^k \cdot x = \sigma^k(x)$, $x \in E$. Les orbites de cette action sont les ensemble $H \cdot x = \{\sigma^k(x) : k \in \mathbb{Z}\}$. On les appelle σ-orbite.

Prop 39. Soit $\sigma \in \mathfrak{S}(E) \backslash \{\mathrm{Id}_E\}$ et O une σ-orbite de cardinal $r \geq 2$. Pour tout $x \in O$, r est le plus entier naturel non nul tel que $\sigma^r(x) = x$, et $O = <\sigma> \cdot x = \{x, \sigma(x), \dots, \sigma^{r-1}(x)\}$.

Thm 40. Une permutation $\sigma \in \mathfrak{S}(E)$ est un cycle d'ordre $r \geq 2$, si et seulement si, il n'y a qu'une seule σ-orbite non réduite à un point.

Déf 41. Soit $\sigma \in \mathfrak{S}(E)$. On appelle support de σ l'ensemble $\mathrm{Supp}(\sigma) = \{x \in E : \sigma(x) \neq x\}$. Deux cycles de E sont disjoints s'ils ont un support un disjoint.

Thm 42. Toute permutation $\sigma \in \mathfrak{S}(E) \backslash \{Id_E\}$ se décompose en produit de cycles deux à deux disjoints, c'est à dire que le groupe $\mathfrak{S}(E)$ est engendré par les cycles. Une telle décomposition est unique, et si l'on a $\sigma = \gamma_1 \dots \gamma_p$, alors $\mathrm{Supp}(\sigma) = \bigcup_{i=1}^{p} \mathrm{Supp}(\gamma_i)$, et $\mathrm{ord}(\sigma) = \mathrm{ppcm}(\mathrm{ord}(\gamma_1), \dots, \mathrm{ord}(\gamma_p))$.

Cor 43. Le groupe $\mathfrak{S}(E)$ est engendré par les transpositions.

Ex 44. Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$, on a $\sigma = (1,2)(2,3)(3,4)(4,5)(6,7)$

Déf 45. Pour $\sigma \in \mathfrak{S}(E)$, on note $\mu(\sigma)$ le nombre de $\sigma-$orbites distinctes. La signature d'une permutation $\sigma \in \mathfrak{S}(E)$ est alors l'élément défini par $\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)}$

Lemme 46. Pour tout $\sigma \in \mathfrak{S}(E)$, et toute transposition τ, $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$

Cor 47. Si $\sigma \in \mathfrak{S}(E)$ est produit de p transpositions, alors $\varepsilon(\sigma) = (-1)^p$.

Thm 48. Les seuls morphismes de groupes de $(\mathfrak{S}(E), \circ)$ dans $(\mathbb{R}^*, \cdot)$ sont l'application constante égale à 1, et ε.

II.2 $(\mathbb{Z}/n\mathbb{Z}, +)$, $\mathbb{U}_n$ et groupes abéliens fini

Soit $n \in \mathbb{N}^*$.

Déf 49. Soit $k \in \mathbb{Z}$. On note $\overline{k}$ la classe de k pour le relation d'équivalence : $h \sim k \iff h \equiv k \pmod n$. On note $\mathbb{Z}/n\mathbb{Z} := \{\overline{k} : 0 \leq k \leq n-1\}$

Thm 50. $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique.

Déf 51. On note $\mathbb{U}_n := \{z \in \mathbb{C} : z^n = 1\}$ l'ensemble des racines n-ième de l'unité.

Thm 52. $(\mathbb{U}_n, \cdot) \simeq (\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique d'ordre n.

Déf 53. Soit G un groupe abélien fini. On appelle *caractère* de G un morphisme $\chi : (G, \cdot) \to (\mathbb{C}^*, \cdot)$.

Lemme 54. Soit G un groupe abélien fini, et $H \leq G$. Tout caractère de H se prolonge en un caractère de G.

App 55 (Théorème de structure)**.** Soit G un groupe abélien fini. Il existe des uniques $r \in \mathbb{N}^*$, $2 \leq n_1 | n_2 | \dots | n_r$ tels que

$$G \simeq \mathbb{U}_{n_1} \times \cdots \times \mathbb{U}_{n_r} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

II.3 Groupes cycliques

[Rom21] Soient $n \geq 2$ et $G =< a >$ un groupe cyclique d'ordre n.

Prop 56. Les sous-groupes de $G =< a >$ sont tous cycliques.

Prop 57. Pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d de G.

Thm 58. Un groupe abélien fini G d'ordre $n \geq 1$ est cyclique, si et seulement si, pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d de G.

Cor 59. Soit p un nombre premier. Alors $(\mathbb{Z}/p\mathbb{Z}, \cdot)^\times$ est cyclique.v Plus généralement, si $\mathbb{K}$ est un corps fini, alors $\mathbb{K}^*$ est cyclique.

App 60 (DEV 2)**.** Si p est un nombre premier de Fermat, alors $\zeta := e^{\frac{2i\pi}{p}}$ est constructible à la règle et au compas.

Cor 61 (Gauss-Wantzel)**.** Soit $n \in \mathbb{N}^*$, le polygone régulier à n côtés est constructible si et seulement si soit $n = 2^m$ où $m \geq 2$, soit $n = 2^m p_1 \dots p_r$ où $m \in \mathbb{N}$, $r \geq 1$ et les p_i sont des nombres premiers de Fermat distincts.

II.4 Groupes linéaires finis

[Rom21] Soit $\mathbb{F}_q$ le corps fini à $q = p^m$ éléments, p premier. Soit $n \geq 2$.

Déf 62. Soit $\mathbb{K}$ un corps. On appelle groupe projectif linéaire, noté $PGL_n(\mathbb{K})$, le groupe $GL_n(\mathbb{K})/Z(GL_n(\mathbb{K}))$. On appelle groupe projectif spécial linéaire, noté $PSL_n(\mathbb{K})$, le groupe $SL_n(\mathbb{K})/Z(SL_n(\mathbb{K}))$.

Lemme 63. $Z(GL_n(\mathbb{K})) = I_n\mathbb{K}^*$ et $Z(SL_n(\mathbb{K})) = \{\lambda I_n : \lambda \in \mathbb{K},\ \lambda^n = 1\}$

Prop 64. $|GL_n(\mathbb{F}_q)| = \prod_{i=1}^{n-1}(q^n - q^i) = q^{\frac{n(n-1)}{2}}(q^n-1)\dots(q-1)$.

Prop 65. $|SL_n(\mathbb{F}_q)| = |PGL_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}(q^n-1)\dots(q^2-1)$ et $|PSL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)|/\operatorname{pgcd}(n, q-1)$.

III Cryptosystème à clef publique El-Gamal

[Ulm18] Alice et Bob veulent échanger des messages un système à clef publique sans que d'autres puissent déchiffrer leurs messages. Ici, un message est un nombre entier.

Prop 66. Considérons un groupe cyclique $G =< \gamma >$ d'ordre n. γ et n sont publiques.

1. Alice choisit une clef privée $1 < a < n-1$, et envoie $\gamma^a \in G$ à Bob.
2. Bob choisit une clef privée $\rho := \gamma^b \in G$, et envoie la paire $(\gamma^k, \rho \cdot (\gamma^a)^k)$ à Alice, où k est un entier choisit aléatoirement.

Alice peut alors lire le message de Bob, en calculant l'inverse de $(\gamma^a)^k = (\gamma^k)^a$. Le cryptosystème est basé sur le fait qu'Alice et Bob partagent le secret $(\gamma^a)^k = (\gamma^k)^a$.

Rq 67. La sécurité du système réside dans la difficulté de résoudre le problème du "logarithme discret", c'est à dire, la difficulté de trouve a en connaissant γ^a

Ex 68. Considérons $f = X^7 + 2X + 2012 \in \mathbb{F}_{2017}[X]$, qui est irréductible. Le corps $K = \mathbb{F}_{2017}[X]/(f)$ possède 2017^7 éléments et $\gamma = \overline{X}$ est un générateur de K^* d'ordre $2017^7 - 1$. Alice choisit comme clef secrète $a = 20162017$, et rend public $\gamma^a = 1362z^6 + 554z^5 + 220z^4 + 468z^3 + 1038z^2 + 868z + 6$. Afin d'envoyer le message $\rho = 66z^6 + 55z^5 + 44z^4 + 33z^2 + 22z + 11z$ à Alice, Bob choisit un entier au hasard, disons $k = 7654321$, et calcule $(\gamma^k, \rho \cdot (\gamma^a)^k)$.

Bibliographie

[Odi23] Alain Ninet Odile Fleury Loic Foissy. *Algèbre et calcul formel*. 2eme edition. ellipses, 2023.

[Per96] Daniel Perrin. *Cours d'algèbre*. ellipses, 1996.

[Rom21] Jean-Étienne Rombaldi. *Mathématiques pour l'agrégation : Algèbre et géométrie*. 2e éd. De Boeck Supérieur, 2021.

[Ulm18] Felix Ulmer. *Anneaux, corps, résultants*. ellipses, 2018.

[Ulm21] Felix Ulmer. *Théorie des groupes*. 2021.