104 : Groupes finis. Exemples et applications

I Généralités et outils des groupes finis

A Vocabulaire des groupes finis X. G 1.2 Berhuy ou Ron 1.1 et 1.2

Définition 1 : Un élément $a \in G$ est dit d'ordre $p \in \mathbb{N}^*$ si $\langle a \rangle$ est fini d'ordre p. L'ordre de a est aussi le plus petit entier naturel non nul p tel que $a^p = e$ et on a $\langle a \rangle = \{e, a, \dots, a^{p-1}\}$.

Exemple 2 : $\bar{1}$ est d'ordre n dans $(\mathbb{Z}/n\mathbb{Z}, +)$, $n \geq 2$.
Le neutre d'un groupe est d'ordre 1.

Théorème 3 (Lagrange) : Soit G un groupe fini. L'ordre de tout sous groupe H de G divise l'ordre de G.

Corollaire 4 : Si G est fini d'ordre n, alors l'ordre de tout élément de G divise n. En particulier tout élément $a \in G$ vérifie $a^n = e$.

Application 5 : Si l'ordre de G est un nombre premier p, tout élément de G différent du neutre est d'ordre p.

Définition 6 : On appelle exposant de G, noté $\exp(G)$ le plus petit entier $m \in \mathbb{N}^*$ qui vérifie que pour tout $a \in G$, $a^m = e$.

Proposition 7 : On a $\exp(G) = \text{ppcm}\{\text{ord}(a), a \in G\}$

Application 8 : Si $x \in G$ est d'ordre a, $y \in G$ est d'ordre b et si $a \wedge b = 1$ alors xy est d'ordre ab.

Proposition 9 : Si G est un groupe abélien alors il admet un élément d'ordre $\exp(G)$

Exemple 10 : $\exp(\mathbb{Z}_p) = p$ avec $p \in \mathcal{P}$.

B Actions de groupes Rom 1.6 (et Per pour rem 12)

Définition 11 : On dit que le groupe G opère à gauche sur l'ensemble E si on a une application : $G \times E \to E$ $(g, x) \mapsto g.x$ telle que :
i) $\forall x \in E$, $1.x = x$ ii) $\forall (g, g', x) \in G^2 \times E$, $g.(g'.x) = (gg').x$

Remarque 12 : Il revient au même de se donner un homomorphisme $\varphi : G \to S(X)$
On pose alors $g.x = \varphi(g)(x)$.

Exemple 13 : G agit sur lui-même par translations à gauche : $(g, h) \mapsto g.h = gh$ ($G \times G$)
G agit sur lui-même par conjugaison $(g, h) \in G \times G \mapsto g.h = ghg^{-1}$
$S(E)$ agit sur E par $(\sigma, x) \in S(E) \times E \mapsto \sigma.x = \sigma(x) \in E$.

Application 14 (Théorème de Cayley) : G est isomorphe à un sous-groupe de $S(G)$

Définition 15 : Soit G un groupe opérant sur $E \neq \emptyset$ et soit $x \in E$. On définit :
i) $O(x) = G.x = \{g.x, g \in G\}$ l'orbite de x
ii) $G_x = \{g \in G, g.x = x\}$ le stabilisateur de x.

Proposition 16 : pour tout $x \in X$, G_x est un sous groupe de G.

Exemple 17 : pour l'action de G sur lui-même par conjugaison, les orbites sont appelées classes de conjugaison : $\forall h \in G$, $G.h = \{ghg^{-1}, g \in G\}$. Le groupe G est commutatif si et seulement si $G.h = \{h\}$ pour tout $h \in G$.

Théorème 18 (Equation des classes) : Soit $(G, .)$ un groupe fini opérant sur un ensemble fini E. En notant $G.x_1, \dots, G.x_n$ toutes les orbites deux à deux distinctes, on a $\text{card}(E) = \sum_{i=1}^{n} |O(x_i)| = \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|}$

Application 19 : pour tout p premier, le centre d'un p-groupe n'est pas trivial

Application 20 : Tout groupe d'ordre p^2 avec p premier est commutatif

II Exemples fondamentaux

A Sous groupes de Sylow Per 1.5

Définition 21 : Soit G un groupe fini de cardinal n et p un diviseur premier de n. Si $n = p^\alpha m$ avec $p \wedge m$, on appelle p-sous groupe de Sylow de G un sous groupe de cardinal p^α.

Remarque 22 : Dire que P est un p-sous groupe de Sylow de G signifie :
i) que P est un p-groupe ($|P| = p^k$, $k \in \mathbb{N}^*$)
ii) $p \wedge [G : P] = 1$ où $[G : P] = |G/P|$ est l'indice de P dans G.

Exemple 23 : $|GL_n(\mathbb{F}_p)| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = p^{n\frac{n-1}{2}}\cdot m$
$P = \{ A=(a_{ij}) \,.\, a_{ij}=0 \text{ si } i>j \text{ et } a_{ii}=1 \}$ est un p Sylow de $GL_n(\mathbb{F}_p)$.

Développement (premier théorème de Sylow) Soit G un groupe fini et p un diviseur premier de $|G|$, alors G contient au moins un p sous groupe de Sylow.

Lemme 24 : Soit G un groupe avec $|G| = m = p^\alpha m$ avec $p \nmid m$ 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.

Théorème 25 (Sylow 2) : Soit G un groupe tel que $|G| = p^\alpha m$, $p \nmid m$.
i) Si H est un sous groupe de G qui est un p groupe, il existe un p Sylow S tel que $H \subset S$.
ii) Les p Sylow sont tous conjugués (et donc leur nombre k divise m).
iii) On a $k \equiv 1 \ [p]$ (donc $k \mid m$)

Remarque 26 : L'assertion $k \mid n$ résulte du fait que les p Sylows forment une orbite sous G.

Corollaire 27 : Si S est un p Sylow de G, on a :
$S \lhd G \iff S$ est l'unique p-Sylow de $G \iff k = 1$.

Application 28 : Un groupe d'ordre 63 n'est pas simple.

B Le groupe $\mathbb{Z}/m\mathbb{Z}$ Rom 1.6 10.1

Définition 29 : Soient m un entier naturel et a, b deux entiers relatifs. On dit que a est congru à b modulo m si $m \mid b-a$. On note alors $a \equiv b \ [m]$.
C'est une relation d'équivalence dont l'ensemble des classes d'équivalence modulo m est noté $\mathbb{Z}/m\mathbb{Z}$.

Théorème 30 : $\mathbb{Z}/m\mathbb{Z}$ est cyclique d'ordre m engendré par $\bar{1}$.

Proposition 31 : Soit G un groupe monogène. S'il est infini, il est alors isomorphe à $(\mathbb{Z}, +)$, s'il est cyclique d'ordre m, il est alors isomorphe à $(\mathbb{Z}/m\mathbb{Z}, +)$.

Exemple 32 : Le groupe multiplicatif Γ_m des racines m ièmes de l'unité qui est cyclique d'ordre m est isomorphe à $\mathbb{Z}/m\mathbb{Z}$ par l'application $\bar{k} \mapsto e^{\frac{2ik\pi}{m}}$

Application 33 : Un groupe de cardinal premier est cyclique.

Lemme 34 : Soit $x \in (\mathbb{Z}/m\mathbb{Z})^\times$, l'application $\sigma(x)$ définie sur $\mathbb{Z}/m\mathbb{Z}$ par :
$\forall y \in \mathbb{Z}/m\mathbb{Z}, \ \sigma(x)(y) = xy$
est un automorphisme du groupe additif $\mathbb{Z}/m\mathbb{Z}$.

Théorème 35 : L'application σ réalise un isomorphisme $(\mathbb{Z}/m^\times, \cdot)$ sur $(Aut(\mathbb{Z}/m), \circ)$
En particulier $Aut(\mathbb{Z}/m)$ est abélien de cardinal $\varphi(m)$.

C Le groupe S_n. X. G 1.2.3 Per

Définition 36 : Pour tout entier naturel n non nul, on note S_n le groupe des permutations de $\{1, \dots, n\}$ (muni de la loi de composition). Le groupe S_n est appelé groupe symétrique d'indice n. Si $\sigma \in S_n$ on note $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$.

Remarque 37 : $|S_n| = n!$

Définition 38 : Si $i \neq j$ on appelle transposition i, j la permutation notée $\tau_{i,j}$ qui permute les éléments i et j.

Théorème 39 : Tout élément de S_n se décompose en produit de transpositions.
Les transpositions engendrent S_n.

Définition 40 : Si $\sigma \in S_n$ et $a \in \{1, \dots, n\}$ on appelle orbite de a suivant σ l'ensemble
$O_\sigma(a) = \{ \sigma^k(a), \ k \in \mathbb{Z} \}$

Définition 41 : Soit $\gamma \in S_n$. On dit que γ est un cycle si parmi les $O_\gamma(a)$, $1 \leq a \leq n$, il n'existe qu'une seule orbite non réduite à un élément. L'orbite $O_\gamma(a)$ est appelée support du cycle, son cardinal la longueur du cycle et on note $\gamma = (a, \gamma(a), \dots, \gamma^{m-1}(a))$

Exemple 42 : Une transposition est un cycle de longueur 2.

Théorème 43 : Toute permutation $\sigma \neq id$ se décompose de manière unique à l'ordre près en un produit de cycles dont les supports sont deux à deux disjoints.

Exemple 44 : $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\,2)\cdot(3\,4)$

Définition 45 : Soit $\sigma \in S_n$. On appelle signature de σ le produit
$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j)-\sigma(i)}{j-i}$. On a $\varepsilon(\sigma) = \pm 1$. Si $\varepsilon(\sigma) = +1$ (resp $\varepsilon(\sigma) = -1$) σ est dite paire (resp impaire).

Définition 46 : On définit $A_n = \{\sigma \in S_n, \varepsilon(\sigma) = 1\} = \ker \varepsilon$ le groupe alterné.

Proposition 47 : Le groupe A_n est l'unique sous groupe de S_n d'indice 2.

Développement Pour $n \geq 5$, A_n est simple.

Application 48 : A isomorphisme près, A_5 est le seul groupe simple d'ordre 60.

III Groupes abéliens finis

A Cas des groupes cycliques Rom 1.4 1.5

On considère G un groupe.

Définition 49 : On dit que G est monogène s'il existe $g \in G$ tel que $G = \langle g \rangle$. Si de plus G est fini, on dit alors qu'il est cyclique.

Exemple 50 : $(\mathbb{Z}, +)$ est monogène engendré par 1.

Proposition 51 : Si G est cyclique alors G est abélien.

Théorème 52 : Si $G = \langle g \rangle$ est cyclique d'ordre n alors ses générateurs sont les g^k avec $k \in [\![1, n-1]\!]$ premier avec n.

Corollaire 53 : Le nombre de générateurs de G est égal à $\varphi(n)$.

Exemple 54 : Si $n \in \mathcal{P}$ alors le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$ est $n-1$.

Théorème 55 : Un groupe commutatif d'ordre pq où p et q sont deux nombres premiers distincts est cyclique.

Remarque 56 : Pour $p = q$ premiers le théorème devient faux. Par exemple $(\mathbb{Z}_p)^2$ qui est d'ordre p^2 n'est pas cyclique puisque tous ses éléments distincts de neutre sont d'ordre p.

Théorème 57 : Si $G = \langle g \rangle$ cyclique alors les sous groupes de G sont cycliques d'ordre diviseur de n et pour tout diviseur d de n il existe un unique sous groupe de G d'ordre d, il s'agit de $\langle g^{\frac{n}{d}} \rangle$

B Structure des groupes abéliens Rom 1.5 et 1.9

Théorème 58 (Cauchy) : Soit G un groupe commutatif fini d'ordre $n \geq 2$. Pour tout diviseur premier p de n il existe dans G un élément d'ordre p.

Remarque 59 : Pour G commutatif non cyclique et d diviseur quelconque de n, il n'existe pas nécessairement d'élément d'ordre d dans G. Par exemple pour G non cyclique et $d = n$, il n'existe pas d'élément d'ordre n.

Définition 60 : Exposant d'un gp, à mettre ici + exemple

Définition 61 : Un caractère d'un groupe G est un morphisme de groupes de G dans $\mathbb{C}^*$.

Exemple 62 : Le morphisme $g \in G \mapsto 1 \in \mathbb{C}^*$ est le caractère trivial.

Proposition 63 : Soit H un sous groupe de G. Tout caractère $\psi : H \to \mathbb{C}^*$ peut se prolonger en un caractère sur G.

Lemme 64 : Soit $g \in G$ d'ordre égale à l'exposant de G, soit :
$$m = \theta(g_0) = \max_{g \in G} \theta(g) = \operatorname{ppcm}\{\theta(g) \mid g \in G\} \quad \theta = \text{ord}()$$
et en supposant que $m \leq m-1$, on note $K = \langle g_0 \rangle$.
i) $\exists ! \varphi_0 : K \to \mathbb{C}^*$ tel que $\varphi_0(g_0) = \omega = e^{\frac{2i\pi}{m}}$.
ii) En prolongeant le caractère ψ en $\tilde{\psi}$ de G, l'application :
$\theta : \langle g_0 \rangle \times \ker \tilde{\psi} \to G$, $(g_0^k, h) \to g_0^k h$ est un isomorphisme de groupes.

Théorème 65 (Structure des groupes abéliens finis).
Il existe une suite d'entiers $(m_k)_{1 \le k \le n}$ telle que $m_k \geq 2$, $m_1 | m_2, \dots, m_{k-1} | m_k$ et $G \simeq \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$.

Références :

Rombaldi Mathématiques pour l'agrégation Rom

D. Perrin Cours d'Algèbre Per

X G Algèbre X G