FRANCQUEVILLE Martin

104 : Groupes finis, exemples et applications.

réf : Risler, Perrin, Peryé

I Généralités (G sera un groupe fini dans toute cette partie, $n = |G|$)

1) Groupes distingués

déf 1 : Soit H un sous-groupe de G. On définit aH pour $a \in G$ la classe à gauche de a par rapport à H, et Ha la classe à droite.

Rem 2 : Les classes à gauche (resp à droite) forment une partition de G, et on note G/H (resp $H \backslash G$) l'ensemble des classes à gauche (resp à droite).

Thm 3 : (Lagrange) Soit H un sous-groupe de G, alors on a $|G| = |H|\,|G/H|$ donc $|H| \mid |G|$. En particulier, pour $a \in G$, l'ordre de a divise $|G|$.

déf 4 : Soit $A \subset G$, on définit $\langle A \rangle$ le sous-groupe engendré par A comme le plus petit sous-groupe de G contenant A, qui existe toujours.

déf 5 : H un sous-groupe de G. On dit que H est distingué dans G (noté $H \triangleleft G$) si $\forall a \in G$, $aH = Ha$

prop 6 : H un sous-groupe de G. Les propriétés suivantes sont équivalentes :

i) $\exists G'$ un groupe et $\varphi : G \to G'$ un morphisme de groupe tel que $H = \mathrm{Ker}(\varphi)$

ii) $H \triangleleft G$

iii) La structure de groupe de G induit une structure de groupe sur G/H

déf 7 : On dit que G est simple si pour $H \triangleleft G$ alors on a $H = \{1_G\}$ ou $H = G$ (où 1_G est le neutre de G)

ex 8 :
* $\mathbb{Z}/p\mathbb{Z}$ est simple $\Leftrightarrow$ p est premier
* le noyau d'un morphisme de groupe est toujours distingué

prop 9 : (propriété universelle) Soient $H \triangleleft G$ et $\varphi : G \to G_1$ (où G_1 un groupe) tel que $H \subset \mathrm{Ker}(\varphi)$. Alors il existe un unique morphisme $\overline{\varphi} : G/H \to G_1$ tel que $\overline{\varphi} \circ \pi = \varphi$ où π est la projection canonique de G dans G/H. Réciproquement, si un tel $\overline{\varphi}$ existe, alors $H \subset \mathrm{Ker}(\varphi)$, et on a : $\overline{\varphi}$ injectif $\Leftrightarrow H = \mathrm{Ker}(\varphi)$

2) Actions de groupes sur un ensemble

déf 10 : Soit X un ensemble. On dit que G opère sur X s'il existe une application (appelée action de G sur X) :
$$\begin{array}{rcl} G \times X & \to & X \\ (g, x) & \mapsto & g \cdot x \end{array}$$
telle que $\forall g, g' \in G, \forall x \in X$, $g \cdot (g' \cdot x) = gg' \cdot x$ et $\forall x \in X$ $1_G \cdot x = x$.

ex 11 : * $GL_n(\mathbb{R})$ opère sur $\mathbb{R}^n$

* G peut opérer sur lui-même de plusieurs façons, par exemple par conjugaison ou par translation.

* S_n agit sur $\{1, \dots, n\}$

prop 12 G est isomorphe à un sous-groupe de $S_{|G|}$ (thm de Cayley)

déf 13 : Soit G qui opère sur X. Pour $x \in X$, on définit $\omega(x)$ l'orbite de x formée des éléments $g \cdot x$ pour $g \in G$, et $Stab_x = \{g \in G \mid g \cdot x = x\}$ le stabilisateur de x, qui est un sous-groupe de G.

ex 14 : * Si G opère sur G par conjugaison, les orbites sont les classes de conjugaison

* Pour $n \in \mathbb{N}^*$, S_n agit sur $\{1, \dots, n\}$, $Stab_1$ est isomorphe à S_{n-1}.

prop 15 : Soit G opérant sur X. Pour $x \in X$, $\varphi_x : G \to \omega(x)$, $g \mapsto g \cdot x$ se factorise en $\Phi_x : G/Stab_x \to X$ qui est une bijection.

prop 16 : (formule des classes) On a : $|G| = |Z(G)| + \sum |\omega_i|$ où $\{\omega_i\}_i$ est l'ensemble des classes de conjugaison de G non réduites à un élément.

app 17 : Si $|G| = p^k$ pour p un nombre premier et $k \geq 1$, alors $Z(G) \neq \{1_G\}$. De plus si $|G| = p^2$, G est abélien.

II Groupes et sous-groupes remarquables

1) Théorèmes de Sylow

déf 18 : Soit p premier, $p \mid |G| = p^\alpha m$ où m premier avec p. On appelle p-Sylow de G tout sous-groupe de G de cardinal p^α.

ex : 19 : p premier, $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$

$$= m\, p^{n(n-1)/2} \text{ où } m \wedge p = 1.$$

$H = \{M \text{ tq } \forall i,\ m_{i,i} = 1 \text{ et } \forall i > j,\ m_{i,j} = 0\}$ est un p-Sylow de $GL_n(\mathbb{F}_p)$.

lemme 20 : $|G| = p^\alpha m$, $\alpha \geq 1$, $m \wedge p = 1$, H sous-groupe de G tel que $p \mid |H|$, et S un p-Sylow de G. Alors, il existe $a \in G$ tel que aSa^{-1} soit un p-Sylow de H.

thm 21 : Soit $p \mid |G|$, p premier, alors G contient un p-Sylow.

cor 22 : $|G| = p^\alpha m$, $m \wedge p = 1$ où p premier. Alors $\forall i \leq \alpha$, G contient un sous-groupe de cardinal p^i.

thm 23 : $|G| = p^\alpha m$, $\alpha \geq 1$ et $p \wedge m = 1$.

* si H est un sous-groupe de G et un p-groupe, alors il existe S un p-Sylow de G tel que $H \subset S$

* les p-Sylow de G sont tous conjugués entre eux

* si k le nombre de p-Sylow de G vérifie $k \equiv 1\ (p)$ et $k \mid m$

cor 24 : S un p-Sylow de G, alors :

$S \trianglelefteq G \iff S$ est l'unique p-Sylow de G

2) Groupe symétrique ($n \in \mathbb{N}^*$ ici)

déf 25 : Soit $\{i_1, \dots, i_k\} \subset [\![1, n]\!]$, (i_k) tous distincts. $(i_1 \dots i_k)$ est appelé un cycle de longueur k de support $\{i_1, \dots, i_k\}$

prop 26 : $\forall \sigma \in \mathfrak{S}_n$, σ est produit de cycles à support disjoints, de manière unique à ordre des cycles près.

cor 27 : $\mathfrak{S}_n$ est engendré par les transpositions

prop 28 : On définit $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$, $\sigma \mapsto \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$ la signature

ε est un morphisme de groupes et on note $A_n = \ker(\varepsilon)$

prop 29 : A_n est engendré par les cycles de longueur 3, et deux cycles de longueur 3 sont conjugués dans A_n pour $n \geq 5$.

th 30 : A_n est simple pour $n \neq 4$.

th 31 (DVLP 1) : A_5 est l'unique groupe simple d'ordre 60 à isomorphisme près.

3) Caractères et structure des groupes abéliens finis

(G est désormais supposé abélien)

déf 32 : Un morphisme de groupe $\chi : G \to \mathbb{C}^*$ est appelé caractère, l'ensemble des caractères $\widehat{G}$ est appelé dual de G et c'est un groupe abélien.

prop 33 : On a en fait $\widehat{G} = \{\chi : G \to \mu_{|G|}$ où χ morphisme de groupe$\}$ où $\mu_k = \{$racines k-ième de l'unité dans $\mathbb{C}^*\}$

lemme 34 : Soit H sous-groupe de G. Tout caractère de H peut être prolongé en un caractère de G.

lemme 35 : Si $g \in G$ est tel que $\forall \chi \in \widehat{G}$, $\chi(g) = 1$, alors $g = 1_G$.

déf 36 : Soit $N = \mathrm{ppcm}\{|g|$ où $g \in G\}$. On dit que N est l'exposant de G.

lemme 37 : G et $\widehat{G}$ ont même exposant

th 38 : Il existe $r \in \mathbb{N}^*$ et $d_1, \dots, d_r \in \mathbb{N}$ tels que $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$ et $\forall i$, $d_{i+1} \mid d_i$

[DVLP 2 : lemme 37 + th 38]

th 39 : La décomposition du th 38 est unique

app 40 : Soit K un corps commutatif, H un sous-groupe fini de K^*. Alors H est cyclique.