

Centre d'un p-groupe: Fraulinou 1p. 47 201-103-104

Jennemann p. 107

Soit G un groupe fini, soit $a \in G$. Alors:

1) En considérant l'action par conjugaison, $|Z(a)| = [G : C(a)]$ où $C(a)$ est le centralisateur de a et $Z(a)$ est l'orbite de a .

Si $|G| = p^m$, p premier, $m \geq 1$, on a:

2) $|Z(G)| = p^k$, $0 < k \leq m$ où $Z(G)$ est le centre de G .

3) Si $m = 2$, G est abélien.

Démonstration:

1) On considère l'action $g \cdot a = gag^{-1}$; $a, g \in G$.

On a: $C(a) = \{g \in G \mid ga = ag\} = \{g \in G \mid gag^{-1} = a\}$

Donc $C(a)$ est le stabilisateur de a pour l'action par conjugaison.

Comme $|G| = |Z(a)| \underbrace{|Stab(a)|}_{= |C(a)|}$ on a alors $|Z(a)| = \frac{|G|}{|C(a)|} = [G : C(a)]$

2) $Z(G) = \{a \in G \mid \forall g \in G, ag = ga\}$

Soit $a \in G$.

Alors $a \in Z(G) \iff \forall g \in G, gag^{-1} = a \iff Z(a) = \{a\}$

G est réunion disjointe de ses classes de conjugaison². La question 1)

assure que le cardinal d'une classe de conjugaison est un diviseur de $|G| = p^m$.

Si elle n'est pas réduite à un singleton, son cardinal est de la forme p^k avec $k \geq 1$ donc en nul modulo p . Soit T un hpt de

Ainsi: $|G| = \sum_{x \in T} |Orb(x)| = \sum_{x \in Z(G)} |Orb(x)| + \sum_{x \in T, x \notin Z(G)} |Orb(x)|$ après des orbites distinctes de l'action
Jennemann

$$= |Z(G)| + \sum_{x \in T, x \notin Z(G)} |Orb(x)|$$

Modulo p : $0 \equiv |G| \equiv |Z(G)|$ donc $p \mid |Z(G)|$

et $Z(G) < G$ donc par le théorème de Lagrange: $|Z(G)| = p^k$ où

³

$0 \leq h \leq m$. Comme $p \mid Z(h)$, $h \geq 1$.

3) Soit S_G le groupe des permutations de G . $S_G = \{ \text{bij de } G \text{ dans } G \}$

Soit $\varphi: G \rightarrow S_G$ où $\varphi_g: G \rightarrow G$ est le morphisme de conjugaison $(\varphi_g)^{-1} = \varphi_{g^{-1}}$
 $g \mapsto \varphi_g$ $a \mapsto g a g^{-1}$

Alors $\forall g, g' \in G$, $\varphi_{gg'} = \varphi_g \circ \varphi_{g'}$ et φ est un morphisme de G sur un sous groupe de S_G , noté $\text{Int}(G) = \{ \text{automorphismes intérieurs de } G \}$

$\ker(\varphi) = Z(G)$, or $Z(G) \neq \{e\}$ d'après 2) donc $|G| = |\text{Im}(\varphi)| |\ker(\varphi)|$
 donne $|\text{Int}(G)| = 1$ ou p $p \nmid \dots$ $|\text{Int}(G)| \mid \underbrace{|Z(G)|}_{=p \text{ ou } p^2}$

Comme p est premier, $\text{Int}(G)$ est cyclique dans les 2 cas

Il existe alors $g_0 \in G$ / $\forall g \in G$, $\exists h \in \mathbb{Z}$ / $\varphi_g = \varphi_{g_0}^h$ i.e. $\forall x \in G$,
 $g x g^{-1} = g_0^h x g_0^{-h}$.

pour $x = g_0$, on a:

Mais alors $g_0 \in Z(G)$ car $g g_0 g^{-1} = g_0^h g_0 g_0^{-h} = g_0$ et $g g_0 = g_0 g$

Donc $\varphi_{g_0} = \text{id}$ et $|\text{Int}(G)| = 1$. Donc $Z(G) = G$ i.e. G est abélien $\square$
 $\uparrow$ car $|G| = Z(G)$ donc $g_0 \in Z(G) \Rightarrow \varphi_{g_0} = \text{id}$

① Goursat p. 22 Si $|G| < \infty$, $\forall x \in X$, $|G| = |Gx| \cdot |S_x|$

en effet: soit $n \in X$ soit R_n le rel d'éq sur G def par: $s R_n t \Leftrightarrow$

$s \cdot n = t \cdot n$. Alors $s R_n t \Leftrightarrow t^{-1} \cdot s \cdot n = n \Leftrightarrow t^{-1} \cdot s \in S_n \Leftrightarrow s \in t S_n$ $\checkmark$ (Stab(n))

les classes d'éq sont alors de la forme $t S_n$, $t \in G$ donc de haut de

cardinal $|S_n|$. Il y a autant de classes d'éq que de valeurs prises par

$s \cdot n$, $s \in G$ et il y a $|Gx|$ classes d'éq.

Donc $|G| = |Gx| |S_x|$.

② Spinglas p. 245. Les orbites de X sous l'action de G forment une

partition de X et il existe une bijection $G / (\text{Stab}(u)) \rightarrow \text{Orb}(u)$

$g \text{ Stab}(u) \mapsto g \cdot u$

③ Théorème de Lagrange: Soit G un groupe fini. L'ordre de tout sous-gp H de G divise $|G|$.

En effet: $x \in H \Leftrightarrow xg^{-1} \in H$ et inverse de g . Si on note à la place de $a \in G$, on a: $\bar{x} = Hx = \{zx, z \in H\}$ (en effet: $y \in \bar{x} \Leftrightarrow y \in Hx \Leftrightarrow yx^{-1} \in H \Leftrightarrow y \in Hx$.)

$\forall x \in G, H \rightarrow Hx$ est une bijection donc $|H| = |Hx|$
 $y \mapsto yx$

Ainsi, toutes les classes ont $|H|$ éléments. Comme les classes de g forment une partition de G , $|G| = n|H|$ où $n = |G/H|$ est le nb de classes de g .
 $= [G:H]$ indice

④ $\varphi: G \rightarrow S_G$ morphisme? $\varphi(g_1 g_2) = \varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2} = \varphi(g_1) \circ \varphi(g_2)$
 $g \mapsto \varphi_g$
 $\uparrow$
 φ_g morphisme

⑤ $\text{Ker}(\varphi) = \{g \in G \mid \varphi(g) = \text{id}\} = \{g \in G \mid \varphi_g = \text{id}\}$
 $= \{g \in G \mid \forall x \in G, \varphi_g(x) = x\} = \{g \in G \mid \forall x \in G, gxg^{-1} = x\}$
 $= Z(G)$

⑥ Frobenius p. 39 $f: G \rightarrow G$ morphisme $\Rightarrow |G| = | \text{Im}(f) | | \text{Ker}(f) |$

Soit R la rel de g $a \sim b \Leftrightarrow f(a) = f(b)$. Donc:

$|G/H| = | \text{Im}(f) |$ et $|H| = |K| \Leftrightarrow f(x^{-1}y) = 1$ car f est un morphisme donc $x^{-1}y \in \text{Ker}(f)$ $x \sim y \Leftrightarrow y \in x \text{Ker}(f)$

La classe $\bar{x}$ est donc la classe à gauche mod $\text{Ker}(f)$: $\bar{x} = x \text{Ker}(f)$

Ainsi, $| \bar{x} | = | \text{Ker}(f) |$ ($H \rightarrow gH$ est bijective
 $x \mapsto xg$)

Les classes ont donc $\bar{n}$ cardinal, celui de $\text{Ker}(f)$, donc $|G| = |G/H| | \text{Ker}(f) |$
 $= | \text{Im}(f) | | \text{Ker}(f) |$

$$\textcircled{7} \text{Int}(G) = \{ \varphi \in \text{Aut}(G) \mid \forall x \in G, \varphi(x) = g x g^{-1}, g \in G \}$$

Szpiro p. 237 Action d'un groupe G sur un ensemble X

Définition: On dit que G agit à gauche sur X si on a une application

$$\begin{aligned} G \times X &\rightarrow X \\ (g, x) &\mapsto g \cdot x \end{aligned} \quad \text{telle que : } \forall x \in X, 1 \cdot x = x$$

$$\forall g, g' \in G, \forall x \in X, (gg') \cdot x = g \cdot (g' \cdot x)$$

Dire que G agit à gauche sur X revient à demander qu'il existe un morphisme entre G et le groupe $S(X) = \{ \text{bijections de } X \}$ (muni de $\circ$)

Le morphisme est $\varphi: G \rightarrow S(X)$

$$g \mapsto \varphi_g: X \rightarrow X$$

$$x \mapsto g \cdot x$$

- Action fidèle: $\forall x \in X, g \cdot x = x \Rightarrow g = 1$
- Action transitive: $\forall x, y \in X, \exists g \in G \mid g \cdot x = y$

$$G \text{ agit fidèlement sur } X \Leftrightarrow \forall x \in X, \varphi_g(x) = x \Rightarrow g = 1$$

$$\Leftrightarrow \varphi_g = \text{id} \Rightarrow g = 1$$

$$\Leftrightarrow \varphi(g) = \text{id} \Rightarrow g = 1$$

$$\Leftrightarrow \varphi \text{ est injective}$$

On peut rendre une action fidèle en considérant le morphisme du groupe $G / \text{Ker}(\varphi)$ vers $S(X)$

Comme une action n'est pas toujours transitive, on introduit la relation d'éq: $x \sim y \Leftrightarrow \exists g \in G \mid y = g \cdot x$

les classes d'éq de cette rel sont appelées les orbites:

$$\begin{aligned} \text{Orb}(x) &= \{ y \in X \mid \exists g \in G \mid y = g \cdot x \} \\ &= \{ g \cdot x, g \in G \} \end{aligned}$$

l'action de G sur X induit une action de G sur $\text{Orb}(x)$,

qui est elle transitive.

Soit $x \in X$ d'orbite $\text{Orb}(x)$; $G \rightarrow \text{Orb}(x)$ est surjective :
 $g \mapsto g \cdot x$

Soit $y \in \text{Orb}(x)$, alors $\exists g \in G$ / $y = g \cdot x$

On introduit le stabilisateur de x pour rendre cette app. injective.

$$\text{Stab}(x) = \{ g \in G \mid g \cdot x = x \} \leq G$$

Soit $H \leq G$; $G \curvearrowright G/H$ par multiplication à gauche :

$$\begin{aligned} G \times G/H &\longrightarrow G/H \\ (g, g'H) &\longmapsto gg'H \end{aligned}$$

Cette action est transitive : si $gH, g'H \in G/H$ alors

$$(g'g^{-1})gH = g'H$$

Proposition : les orbites de X sous l'action de G forment une partition de

X et $f_x : G/\text{Stab}(x) \rightarrow \text{Orb}(x)$ est une bijection

$$g\text{Stab}(x) \mapsto g \cdot x$$

En effet : on a $X = \bigcup_{x \in X/\sim} \text{Orb}(x)$

① Soit $y \in X$, soit $x \in X$, comme $G \curvearrowright \text{Orb}(x)$ est transitive,

$\exists g \in G$ / $y = g \cdot x$ donc $y \in \text{Orb}(x)$

② Soit $y \in \bigcup_{x \in X/\sim} \text{Orb}(x)$ alors $\exists x \in X$ ($y \in \text{Orb}(x)$)

alors $\exists x \in X, \exists g \in G$ / $y = g \cdot x \in X$

On a vu précédemment que $f : G \rightarrow \text{Orb}(x)$ est surjective.
 $g \mapsto g \cdot x$

$$\begin{aligned} f(g) = f(g') &\Leftrightarrow g \cdot x = g' \cdot x \Leftrightarrow (g')^{-1}g \cdot x = x \Leftrightarrow (g')^{-1}g \in \text{Stab}(x) \\ &\Leftrightarrow g \in g' \text{Stab}(x) \Leftrightarrow \overline{g} = \overline{g'} \end{aligned}$$

Define $\bar{f} : G/\langle \text{stab}(a) \rangle \rightarrow \text{Orb}(a)$ or more bijection.

$$\bar{g} \mapsto g \cdot a$$

Claim: $|G| = |\text{stab}(a)| |\text{Orb}(a)|$ if $|G|, |X| < \infty$