Théorème de Cauchy et application aux groupes d'ordre 2p

Noah

March 2026

Référence : Gourdon exo 11p 27 chapitre 1, et de tête pour l'application.

Théorème 1. *(Cauchy)*

Soit G un groupe fini, et soit p un diviseur premier de l'ordre de G. Il existe un élément d'ordre p.

Démonstration. Soit $S = \{(g_1, \dots, g_p) \in G^p, g_1 \dots g_p = e\}$. On commence par un lemme

Lemme 1. $|S| = |G|^{p-1}$

Démonstration. L'application

$$\begin{aligned} f : \quad S &\longrightarrow G^{p-1} \\ (g_1, \dots, g_p) &\longmapsto (g_1, \dots, g_{p-1}) \end{aligned}$$

est une bijection, en effet pour la surjectivité, si $(g_1, \dots, g_{p-1}) \in G^{p-1}$,

alors $(g_1, \dots, g_{p-1}, (g_1, \dots, g_{p-1})^{-1}))$ est un antécédent. □

Ensuite, considérons $\gamma \in \mathfrak{S}_p$ un p-cycle et faisons agir $< \gamma >$ sur S, par permutation cyclique, c'est à dire

$$\begin{aligned} < \gamma > \times \quad S &\longrightarrow S \\ (\sigma(= \gamma^k), \quad \underline{g}) &\longmapsto (g_{\sigma(1)}, \dots, g_{\sigma(p-1)}) \end{aligned}$$

Lemme 2. *Les orbites de cette action son de cardinal* 1 *ou* p.

Démonstration. Soit $\underline{x} \in S$. On a $\mathcal{O}_{\underline{x}} = \{\sigma \cdot x = (x_{\sigma(1)}, \dots, x_{\sigma(p)}), \quad \sigma \in < \gamma >\}$. On utilise le résultat fondamental suivant :

$$|\mathcal{O}_{\underline{x}}| \cdot |Stab_{<\gamma>}(x)| = | < \gamma > | = p$$

Donc, p étant premier, $|\mathcal{O}_{\underline{x}}|$ est d'ordre 1 ou p □

On peut désormais attaquer la preuve : Notons que si l'orbite d'un élément est de cardinal 1, cela signifie que le stabilisateur est lui d'ordre p, donc que tous les éléments du p-uplet sont les mêmes, donc $\underline{x} = (x, \dots, x)$ et par conséquent comme $\underline{x} \in S$, cela signifique que x est d'ordre p.

Soit Ω un ensemble contenant exactement un représentant de chaque orbite, et soit $A = \{\underline{x} \in S, |\mathcal{O}_{\underline{x}}| = 1\}$="$\{$*éléments d'ordre* $p\}$".

Par la formule des classes, on a

$$|S| = \sum_{\underline{x} \in \Omega} |\mathcal{O}_{\underline{x}}| = \sum_{\underline{x} \in A} |\mathcal{O}_{\underline{x}}| + \sum_{\underline{x} \in \Omega \setminus A} |\mathcal{O}_{\underline{x}}|$$

donc,

$$|G|^{p-1} = |A| + p \cdot |\Omega \backslash A|.$$

cela signifie que $|A| = |G|^{p-1} - p \cdot |\Omega \backslash A|$. p étant un diviseur de l'ordre de G, on voit que p divise $|A|$, mais A est non vide car le p-uplet formé du neutre est dedans, donc il existe $x \neq e$ tel que $x^p = e$, et comme p est premier, il n'existe pas de plus petite puissance, donc x est d'ordre p. □

Application : *Soit p premier et G un groupe d'ordre $2p$. Alors G est cyclique ou diédral.*

Démonstration. Par le théorème précédent, il existe un élément d'ordre 2 noté s et un élément d'ordre p noté r. On pose $H =< r >$. Alors H est un sosu groupe distingué de G car il est d'indice 2 (ne pas oublier de mettre cette propriété dans le plan) donc $\forall g \in G, \quad grg^{-1} = g^i, \quad i \in \mathbb{N}$.

En particulier, pour $g = s$ on a $srs = r^i$.
On obtient donc que

$$s(srs)s = r = sr^i s = r^{i^2}$$

, car $r^i = srs$ et $(srs)^i = sr^i s = (r^i)^i$. Par conséquent, $i^2 = 1 \mod p$, donc $i^2 = 1$ ou -1.

1. Si $i = 1$, alors $sr = rs$ et rs est d'ordre $2p$, en effet si k vérifie $(rs)^k = e$, alors $r^k s^k = e$, mais $s \notin H$ donc $r^k = e$ et $s^k = e$ donc $p|k$ et $2|k$ donc par primalité $k = 2p$.
2. Si i=-1, alors $G =< r, s >$ qui est le groupe diédral.

□