Théorème de Cauchy pour les groupes

Christian V. Nguembou Tagne

9 août 2021

D'après le théorème de Lagrange, si G est un groupe fini d'ordre n, alors l'ordre de tout élément de G est un diviseur de n. Est-ce qu'en général, pour tout diviseur p de n, le groupe fini G admet un élément d'ordre p ? Pour les diviseurs premiers, Augustin Louis Cauchy répondit à cette question par l'affirmative.

Théorème (Cauchy).

Soit G un groupe fini d'ordre n et p un diviseur premier de n. Alors, G admet au moins un élément d'ordre p.

Dans cette note, nous démontrons ce théorème. Précisément, nous proposons une démonstration pour le cas abélien et une autre pour le cas non-abélien.

1. Démonstration du cas abélien

Soit G un groupe *abélien* fini d'ordre n et p un diviseur premier de n. Alors, $p \leq n$. Nous allons raisonner par induction sur l'ordre n de G.

Tout d'abord, soit $n = p$. Alors, G est cyclique et tout élément de G, distinct de l'élément neutre e, est un générateur de G. En effet, si a est un élément de G différent de e, alors, selon le théorème de Lagrange, le sous-groupe $\langle a \rangle$ engendré par a est d'ordre 1 ou p. Puisque $\{e, a\} \subset \langle a \rangle$, il en résulte que $\langle a \rangle$ est d'ordre p. D'où $G = \langle a \rangle$. Ainsi, tout élément de G, distinct de l'élément neutre, est d'ordre p.

Maintenant, nous supposons que tout groupe abélien fini, d'ordre strictement inférieur à n et divisible par le nombre premier p, admet un élément d'ordre p. Soit a un élément de G, distinct de l'élément neutre, d'ordre m. Alors, $m \geq 2$.

Premier cas : Soit m divisible par p. Alors, l'élément $a^{\frac{m}{p}}$ de G est d'ordre p. En effet,

$$\left(a^{\frac{m}{p}}\right)^p = a^m = e;$$

et si i et j sont des éléments de l'ensemble $\{0, \ldots, p-1\}$ satisfaisant $\left(a^{\frac{m}{p}}\right)^i = \left(a^{\frac{m}{p}}\right)^j$, alors $\frac{mi}{p} \equiv \frac{mj}{p} \, [\operatorname{mod} m]$, puis $i \equiv j \, [\operatorname{mod} p]$, et donc $i = j$.

Second cas : Soit m non divisible par p. Nous désignons par H le sous-groupe $\langle a\rangle$ engendré par a. Alors, H est un sous-groupe distingué de G, car G est abélien. Du reste,

$$\operatorname{card}(G/H) = \frac{\operatorname{card}(G)}{\operatorname{card}(H)} = \frac{n}{m}.$$

Clairement, p est un diviseur de $\frac{n}{m}$, puisque p divise n, mais pas m. Du reste, $\frac{n}{m} < n$, car $m \geq 2$. Ainsi, G/H est un groupe abélien fini, d'ordre strictement inférieur à n et divisible par le nombre premier p. De ce fait, selon l'hypothèse d'induction, il existe élément b de G tel que bH soit d'ordre p dans G/H. Soit k l'ordre b. Alors, $(bH)^k = b^kH = eH = H$. Il en résulte que k est un multiple de l'ordre p de bH. Par conséquent, l'élément $b^{\frac{k}{p}}$ de G est d'ordre p (voir le premier cas). Ceci conclut la démonstration du théorème de Cauchy pour les groupes abéliens.

2. Démonstration du cas non-abélien

Soit G un groupe *non-abélien* fini d'ordre n et p un diviseur premier de n. Alors, $p \leq n$.

Nous supposons que l'ordre de chaque sous-groupe propre de G n'est pas divisible par p. Alors, l'indice $[G : H]$ de tout sous-groupe non-trivial H dans G est divisible par p, car $n = \operatorname{card}(H) \times [G : H]$ d'après le théorème de Lagrange. Soit $Z(G)$ le centre du groupe G et $Z(g)$ le centralisateur de chaque $g \in G$; autrement dit,

$$Z(G) = \Big\{x \in G \ : \ (\forall g \in G)\ gx = xg\Big\} \qquad \text{et} \qquad Z(g) = \Big\{x \in G \ : \ gx = xg\Big\}.$$

L'application $G \times G \to G,\ (g, x) \mapsto gxg^{-1}$ est une action du groupe G sur lui-même. Pour cette action, l'orbite O_x d'un élément x de G est le singleton $\{x\}$ si, et seulement si, $x \in Z(G)$. Soient $x_1, \ldots, x_k$ les représentants des différentes orbites ayant plus d'un élément. Alors, le stabilisateur de chaque x_j est le centralisateur $Z(x_j)$ de x_j. D'où

$$\operatorname{card}(O_{x_j}) = \frac{\operatorname{card}(G)}{\operatorname{card}\left(Z(x_j)\right)} = [G : Z(x_j)].$$

En vertu de la *formule des classes*, il en résulte que

$$n = \operatorname{card}(G) = \sum_{x \in Z(G)} \operatorname{card}(O_x) + \sum_{j=1}^{k} \operatorname{card}(O_{x_j}) = \operatorname{card}\Big(Z(G)\Big) + \sum_{j=1}^{k} [G : Z(x_j)],$$

et donc

$$\operatorname{card}\Big(Z(G)\Big) = n - \sum_{j=1}^{k} [G : Z(x_j)].$$

Cependant, pour chaque $j \in \{1, \ldots, k\}$, nous avons $1 < [G : Z(x_j)] < m$ car $x_j \notin Z(G)$. De ce fait, $Z(x_j)$ est un sous-groupe non-trivial de G. Ceci induit que p divise $[G : Z(x_j)]$ pour tout $j \in \{1, \ldots, k\}$. Par conséquent, p divise $\operatorname{card}\Big(Z(G)\Big)$. Il en découle que $Z(G) = G$: une contradiction, car G est non-abélien. De ce fait, la supposition initiale est fausse.

✍

Il existe donc un sous-groupe non-trivial de G dont l'ordre est divisible par p.

Maintenant, comme dans le cas abélien, nous allons raisonner par induction sur l'ordre n de G.

Pour $n = p$, le groupe G est cyclique et tout élément de G, distinct de l'élément neutre e, est d'ordre p.

À présent, nous prenons pour hypothèse que tout groupe fini, d'ordre strictement inférieur à n et divisible par le nombre premier p, admet un élément d'ordre p. Le groupe G possède un sous-groupe non-trivial H dont l'ordre est divisible par p. En vertu de l'hypothèse d'induction, il en résulte que H, et donc G, admet un élément d'ordre p. Le théorème de Cauchy, pour les groupes non-abéliens, est ainsi démontré.