Théorie des groupes
Classification des groupes d'ordre p, p^2 et $2p$

AFFALOU Étienne

Septembre 2023

Table des matières

L'objectif de ce court article est de trouver, à isomorphisme près, tous les groupes d'ordre p, p^2 et $2p$ où p est un nombre premier. À la fin, on trace les premiers termes de la suite $(u_n)_{n\in\mathbb{N}^*}$ telle que $\forall n \in \mathbb{N}^*$, u_n est la proportion d'entiers $k \leqslant n$ qui sont classifiés par les théorèmes de l'article.
Dans toute la suite, p est un nombre premier.

1 Groupes d'ordre p, groupes d'ordre p^2

1.1 Classification des groupes d'ordre p

La première proposition utilise le théorème de Lagrange et la classification des groupes monogènes.

> Proposition Soit G un groupe d'ordre p. Alors, $G \cong \mathbb{Z}/p\mathbb{Z}$.

Preuve :
Comme p est premier, G a au moins deux éléments. On peut donc prendre $x \in G$ différent du neutre.
L'ordre de x n'est pas égal à 1 (x n'est pas l'élément neutre par hypothèse) et divise p par le théorème de Lagrange.
Donc, l'ordre de x vaut p et donc $G =< \{x\} > (< \{x\} >\subset G$ et égalité des cardinaux).
G est cyclique de cardinal p donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$ par théorème de classification des groupes monogènes.

Avant de classifier les groupes d'ordre p^2, on redémontre que le centre d'un p-groupe n'est pas trivial.

1.2 Centre d'un p-groupe

Les deux preuves qui suivent se trouvent dans [**1**]. On prouve d'abord un lemme.

> Lemme Soit G un groupe d'ordre p^α avec $\alpha \in \mathbb{N}^*$. Soit X un ensemble fini. On suppose que G opère sur X. Notons $X^G = \{x \in X, \forall g \in G, g.x = x\}$ l'ensemble des points fixes sous G. Alors, $|X| \equiv |X^G|\ [p]$.

Preuve :
Un élément x de X est dans X^G si et seulement si l'orbite de x notée $\omega(x)$ est réduite à $\{x\}$.
Dans le cas où un élément x de X est dans X^G, on a donc $|\omega(x)| = 1$. Sinon, $|\omega(x)| > 1$ et on a $|\omega(x)| \mid |G|$.
G étant de cardinal p^α, $\forall x \in X \setminus X^G, p \mid |\omega(x)|$ et les éléments de X sont soit dans X^G, soit dans $X \setminus X^G$.
Ainsi, en notant $\mathcal{O}$ une partie de X dans laquelle il y a exactement un élément de chaque orbite, on a

$$|X| = |X^G| + \sum_{x\in\mathcal{O}\cap(X\setminus X^G)} |\omega(x)|$$

puis comme p divise $|\omega(x)|$ pour $x \in X \setminus X^G$, on obtient bien $|X| \equiv |X^G|\ [p]$.

> Proposition Soit G un groupe d'ordre p^α avec $\alpha \in \mathbb{N}^*$. Alors, $Z(G) \neq \{e\}$.

Preuve :
En faisant opérer G sur G par automorphisme intérieur, on trouve $|G| \equiv |Z(G)|\ [p]$ en utilisant le lemme.
Mais $Z(G)$ contient au moins l'élément neutre donc $|Z(G)| > 1$. Ainsi, $|Z(G)| \geqslant p$ et $Z(G)$ n'est pas trivial.

1.3 Classification des groupes d'ordre p^2

> Proposition Soit G un groupe d'ordre p^2. Alors, $G \cong \mathbb{Z}/p^2\mathbb{Z}$ ou $G \cong (\mathbb{Z}/p\mathbb{Z})^2$.

Preuve :
Montrons d'abord que G est abélien. Le centre de G est non trivial (voir **1.2**). Supposons que G n'est pas abélien.
Dans ce cas, $Z(G)$ est nécessairement d'ordre p par le théorème de Lagrange.
Le groupe $G/Z(G)$ est d'ordre p, donc monogène par la proposition précédente.
Notons $zZ(G)$ un générateur de $G/Z(G)$. Pour $(x, y) \in G^2$, on a

$$\exists (n, m) \in \mathbb{N}^2, xZ(G) = z^nZ(G) \text{ et } yZ(G) = z^mZ(G)$$

Mais l'élément neutre appartient à $Z(G)$ donc

$$\exists (h,h') \in (Z(G))^2, x = z^n h \text{ et } y = z^m h'$$

Ainsi, comme $(h,h') \in (Z(G))^2$,

$$xy = z^n h z^m h' = z^{n+m} hh' = z^{n+m} h'h = z^m h' z^n h = yx$$

Et donc G est abélien. D'où la contradiction avec l'hypothèse que G n'est pas abélien. G est donc abélien.
Maintenant, deux cas se présentent.

1. Si G admet un élément d'ordre p^2 alors G est cyclique donc isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ par théorème de classification des groupes monogènes.
2. Dans ce second cas, les éléments de G différents de l'élément neutre sont tous d'ordre p.
   Montrons que G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$.
   Soit $x \in G$. Notons $N =< \{x\} >$. N est de cardinal p donc $\exists y \in G \setminus N$. Soit $K =< \{y\} >$. On a alors
   — $N \cong \mathbb{Z}/p\mathbb{Z}$ et $K \cong \mathbb{Z}/p\mathbb{Z}$ par la proposition précédente.
   — G est abélien donc $\forall (n,k) \in N \times K, nk = kn$.
   — $G = NK$. En effet, $NK = KN$ car G est abélien donc NK est un groupe. NK est un sous-groupe de G qui contient au moins $p+1$ éléments (y et les puissances de x) donc c'est G par le théorème de Lagrange.
   — $N \cap K = \{e_G\}$ car $N \cap K$ est un sous-groupe de K donc est de cardinal p ou 1 par le théorème de Lagrange et ce n'est pas K car $y \notin N \cap K$ par exemple.
   Ces quatre conditions montrent que G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$.

2 Groupes d'ordre $2p$

Dans cette partie p est supposé impair (le cas où $p = 2$ a déjà été traité). Pour tout $n \in \mathbb{N}^*$, on note D_n le groupe diédral d'indice n (c'est le groupe des isométries du plan qui conservent un polygone régulier à n côtés).

> Proposition Soit G un groupe d'ordre $2p$. Alors, $G \cong \mathbb{Z}/2p\mathbb{Z}$ ou $G \cong D_p$.

Preuve :
2 est un diviseur premier de $|G|$ donc par le théorème de Cauchy, G admet un élément d'ordre 2.
Ici aussi, deux cas se présentent.

1. Dans le cas où G contient un unique élément g d'ordre 2, deux sous-cas se présentent.
   Si $\exists h \in G$ tel que h est d'ordre $2p$, alors $G \cong \mathbb{Z}/2p\mathbb{Z}$ (car cyclique d'ordre $2p$).
   Sinon, tous les éléments de G différents de g et de e sont d'ordre p. Soit h un élément d'ordre p de G.
   Dans ce cas, $< \{g,h\} >$ est d'ordre strictement plus grand que p et divise $2p$ donc vaut $2p$. Ainsi, $G =< \{g,h\} >$.
   Or, hgh^{-1} est d'ordre 2 (g est d'ordre 2). Donc, comme g est le seul élément d'ordre 2, $hgh^{-1} = g$ puis $hg = gh$.
   De plus, $2 \wedge p = 1$ car p est un nombre premier différent de 2. Donc l'ordre de gh est $2p$.
   D'où la contradiction avec l'hypothèse de ce second sous-cas. Ainsi, $G \cong \mathbb{Z}/2p\mathbb{Z}$ (G a un élément d'ordre $2p$).
2. Dans le second cas, G admet au moins deux éléments d'ordre 2.
   Soient g_1, g_2 deux éléments distincts de G qui sont d'ordre 2. Notons $H =< \{g_1, g_2\} >$.
   L'ordre de H est un multiple de 2 (car engendré par deux éléments d'ordre 2), et divise $2p$ par le théorème de Lagrange. Donc, $|H| = |G|$ puis comme $H \subset G$, $H = G$.
   Si G était abélien, alors $g_1 g_2$ serait aussi d'ordre 2 et donc $\{e, g_1, g_2, g_1 g_2\}$ serait un sous-groupe de G.
   Dans ce cas, on aurait $4|2p$. C'est impossible car p est impair.
   Donc, G n'est pas abélien et engendré par deux éléments d'ordre 2.
   Cela montre que $G \cong D_p$ (voir par exemple **[2]**).

Cela conclut la preuve.

On peut tout à fait démontrer l'existence d'un élément d'ordre 2 dans un groupe fini d'ordre pair sans utiliser le théorème de Cauchy (en considérant par exemple les $\{g, g^{-1}\}$ pour $g \in G$).

3 Combien ?

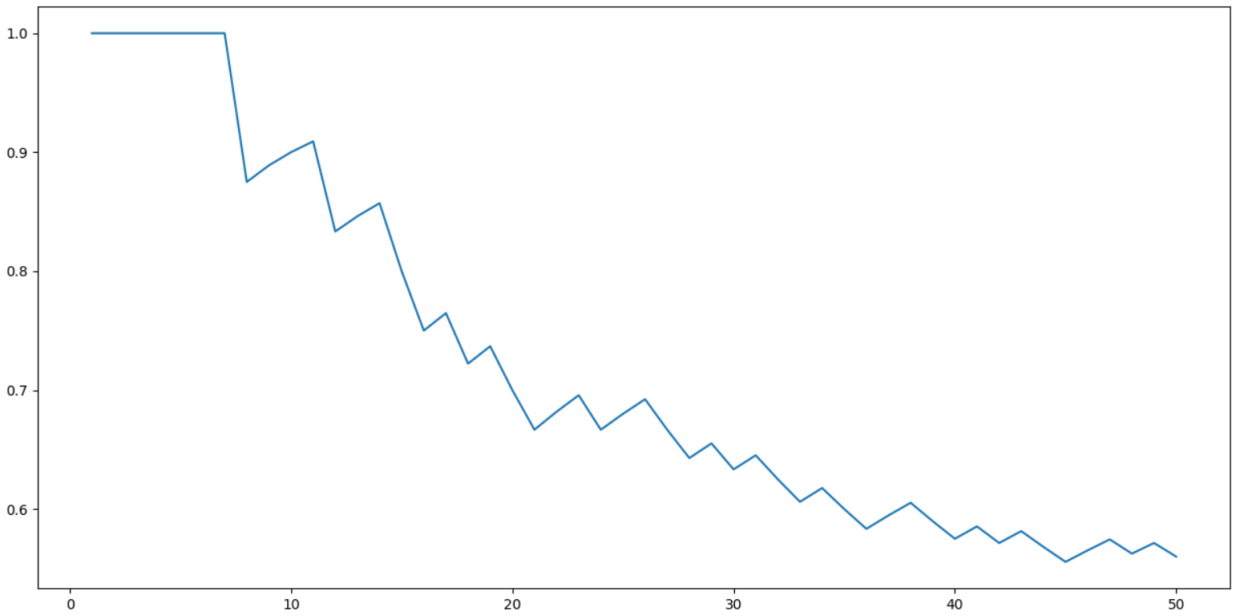
Les trois théorèmes de classification que l'on vient de montrer sont ils efficaces pour classifier tous les groupes finis d'ordre plus petit que $n \in \mathbb{N}^*$? Bien entendu, certains groupes finis échappent à nos théorèmes. Même si c'est faux,

on considère que les théorèmes démontrés précédemment permettent de classifier tous les groupes d'ordre 1 (il n'y en a qu'un). Dans le tableau suivant, on donne les premiers ordres que l'on a réussi à classifier.

Ordre du groupe	Classifiés ?	Si oui, justification
1	Oui	$\{e\}$
2	Oui	Ordre p
3	Oui	Ordre p
4	Oui	Ordre p^2
5	Oui	Ordre p
6	Oui	Ordre $2p$
7	Oui	Ordre p
8	Non	
9	Oui	Ordre p^2
10	Oui	Ordre $2p$
11	Oui	Ordre p
12	Non	
13	Oui	Ordre p
14	Oui	Ordre $2p$

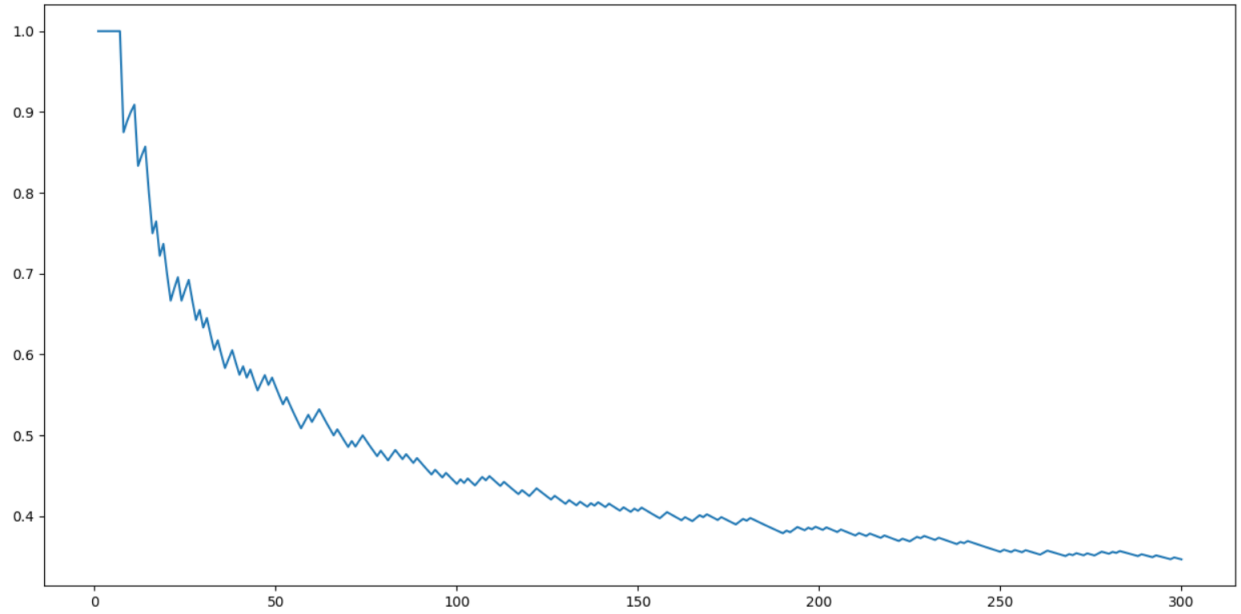
Application de nos théorèmes aux 14 *pemiers entiers naturels non nuls.*

Nous avons donc classifié une bonne partie des groupes de petit ordre à isomorphisme près. Ci dessous, on trace la proportion des ordres classifiés par notre test pour les groupes d'ordre plus petit que 50.



Parmi les 10 *permiers entiers naturels non nuls,* 90% *d'entre eux sont classifiés.*

On a réussi à classifier 54% des **ordres** entre 1 et 50. Par contre, nous n'avons absolument **pas** classifié 54% des **groupes** d'ordre plus petit que 50. Par exemple, il y a 51 groupes d'ordre 32 à isomorphisme près (voir [**3**]), alors que nos théorèmes nous donnent au plus deux groupes différents à chaque ordre compatible. On se doute que classifier les groupes d'ordre 32 est autrement plus compliqué que ce que l'on a pu montrer ici... Le lecteur intéressé par le nombre de groupes d'ordre n à isomorphisme près pour $n \in \mathbb{N}$ peut consulter `https://oeis.org/A000001`.
Ci-dessous, on trace la proportion d'ordres classifiés par nos théorèmes pour $n \leqslant 300$. On voit que ces derniers sont de moins en moins "efficaces" pour des ordres plus grands.



Pour améliorer cette proportion, on pourrait montrer un théorème qui classifie les groupes d'ordre pq où p et q sont deux nombres premiers...

Références :

— [**1**] Cours d'algèbre, *Daniel Perrin*
— [**2**] Théorie des groupes, *Felix Ulmer*
— [**3**] Groupes finis et treillis de leurs sous-groupes, *Alain Debreil*