Théorie des groupes
Classification des groupes de petit ordre

AFFALOU Étienne

Octobre 2023

Table des matières

On va classifier les groupes dont l'ordre est compris entre 1 et 31, hormis 16 et 24.
Soient p et q deux nombres premiers distincts. On suppose $p < q$.

1 Groupes d'ordre p, p^2, pq, p^3

1.1 Groupes d'ordre p, p^2

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 $G = \langle\{x\}\rangle$ ($\langle\{x\}\rangle \subset G$ 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.

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 :
$Z(G)$ est non trivial car G est un p-groupe.
Si $|Z(G)| = p$, alors $G/Z(G)$ est monogène car de cardinal p et donc G est abélien. Ainsi, G est abélien.
Distinguons deux cas :
- Si G admet un élément d'ordre p^2, alors $G \cong (\mathbb{Z}/p^2\mathbb{Z})$.
- Sinon, tous les éléments de G différents de l'élément neutre sont d'ordre p.
  Soit $x \in G \setminus \{e\}$. Notons $H = \langle\{x\}\rangle$. $H \cong \mathbb{Z}/p\mathbb{Z}$ (H d'ordre p).
  Soit $y \in G \setminus H$. Notons $K = \langle\{y\}\rangle$. $K \cong \mathbb{Z}/p\mathbb{Z}$ (K d'ordre p).
  G est abélien, $G = HK = KH$ et $H \cap K = \{e\}$. Ceci montre que $G \cong (\mathbb{Z}/p\mathbb{Z})^2$.

1.2 Groupes d'ordre pq

Lemme Soient H et N deux groupes, $\varphi : H \to \mathrm{Aut}(N)$ et $\alpha \in \mathrm{Aut}(H)$.
Soit ψ tel que le diagramme suivant soit commutatif ($\varphi = \psi \circ \alpha$).

$$\begin{array}{ccc} H & \xrightarrow{\varphi} & \mathrm{Aut}(N) \\ {\scriptstyle\alpha}\downarrow & \nearrow_{\psi} & \\ H & & \end{array}$$

Alors, $N \rtimes_\psi H \cong N \rtimes_\varphi H$.

Preuve :
On introduit l'application

$$\begin{array}{rccc} f & : & N \rtimes_\varphi H & \longrightarrow & N \rtimes_\psi H \\ & & (n,h) & \longmapsto & (n,\alpha(h)) \end{array}$$

C'est bien entendu une bijection (on peut donner son inverse). Montrons que c'est un morphisme.
Soient $(n,n') \in N^2$ et $(h,h') \in H^2$. On a d'une part

$$f((n,h)(n',h')) = f(n\varphi(h)(n'), hh') = (n\varphi(h)(n'), \alpha(hh'))$$

Et d'autre part,

$$f(n,h)f(n',h') = (n,\alpha(h))(n',\alpha(h')) = (n\psi(\alpha(h))(n'), \alpha(h)\alpha(h')) = (n\varphi(h)(n'), \alpha(hh'))$$

Donc f est bien un isomorphisme de groupes, et $N \rtimes_\psi H \cong N \rtimes_\varphi H$.

Proposition Soit G un groupe d'ordre pq.
- Si $p \mid q-1$, alors $G \cong \mathbb{Z}/pq\mathbb{Z}$ ou $G \cong (\mathbb{Z}/q\mathbb{Z}) \rtimes_\alpha (\mathbb{Z}/p\mathbb{Z})$ où $\alpha : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est non trivial.
- Sinon, $G \cong \mathbb{Z}/pq\mathbb{Z}$.

Preuve :
D'après le premier théorème de Sylow, G admet au moins un q-Sylow.
En utilisant le second théorème de Sylow, on obtient que le nombre n_q de q-Sylow de G vérifie

$$n_q \equiv 1 \ [q] \text{ et } n_q \mid p$$

Donc $n_q = 1$ et G a un unique q-Sylow, qui est donc distingué dans G. Notons le Q.
Q étant de cardinal premier, $Q \cong \mathbb{Z}/q\mathbb{Z}$. Or, $p \mid |G|$ donc G a un élément d'ordre p par le théorème de Cauchy.
Le sous-groupe N qu'il engendre est donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On a donc

- $Q \trianglelefteq G$.
- $Q \cap N = \{e\}$ car si $x \in Q \cap N$, son ordre divise q et p par le théorème de Lagrange, donc vaut 1.
- Montrons que $G = QN$. QN est un sous-groupe de G étant donné que $Q \trianglelefteq G$.
  De plus, le second théorème d'isomorphisme donne

  $$QN/Q \cong N/(Q \cap N)$$

  donc $|QN|/q = p/1$ puis $|QN| = pq$ ($NQ = QN$ car $Q \trianglelefteq G$). Ainsi, $G = QN$.

Ces trois points assurent que G s'écrit comme un produit semi-direct

$$G \cong Q \rtimes_\alpha N$$

où $\alpha : N \to \mathrm{Aut}(Q)$ est un morphisme de groupes, avec $N \cong \mathbb{Z}/p\mathbb{Z}$ et $\mathrm{Aut}(Q) \cong \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$.
Les deux sous-cas de la proposition apparaissent naturellement :

1. Si p ne divise pas $q-1$, alors pour tout $x \in N$, l'ordre de $\alpha(x)$ divise $q-1$.
   Or, l'ordre de x étant égal à p, l'ordre de $\alpha(x)$ vaut 1 ou p. Donc l'ordre de $\alpha(x)$ vaut 1 et α est trivial.
   Le produit est donc direct, et

   $$G \cong (\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/pq\mathbb{Z}$$

   par le théorème chinois.
2. Dans le second cas, $p \mid q-1$ et comme $\mathbb{Z}/(q-1)\mathbb{Z}$ est cyclique, il admet un unique sous-groupe d'ordre p.
   On a donc toujours la possibilité où α est trivial, mais α peut également être non trivial, ce qui donne des produits semi-directs isomorphes par le lemme démontré juste avant. Ainsi, on a bien

   $$G \cong \mathbb{Z}/pq\mathbb{Z} \text{ ou } G \cong (\mathbb{Z}/q\mathbb{Z}) \rtimes_\alpha (\mathbb{Z}/p\mathbb{Z})$$

   avec $\alpha : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ non trivial.

D'où le résultat annoncé.

Proposition Soit G un groupe fini d'ordre $2p$.

- Si $p = 2$, alors $G \cong \mathbb{Z}/4\mathbb{Z}$ ou $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
- Si p est impair, $G \cong \mathbb{Z}/2p\mathbb{Z}$ ou $G \cong D_p$.

Preuve :
Traitons d'abord le cas $p = 2$.

1. Si $p = 2$, alors G est d'ordre 4. Si G a un élément d'ordre 4, alors G est cyclique donc

   $$G \cong \mathbb{Z}/4\mathbb{Z}$$

   d'après le théorème de classification des groupes monogènes.
   Sinon, les trois éléments de G différents du neutre sont d'ordre 2.
   Donc $\forall (x,y) \in G^2$, $e = (xy)^2 = xyxy$ donc $xy = y^{-1}x^{-1} = yx$ car $y^{-1} = y$ et $x^{-1} = x$ ($x^2 = y^2 = e$).
   Cela montre que G est abélien donc

   $$G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

   d'après le théorème de structure des groupes abéliens finis.
2. Si p est impair, alors $p > 2$ et notre classification s'applique. Comme p est impair, $2 \mid q-1$.
   D_p est un groupe non abélien d'ordre $2p$, donc il n'est pas isomorphe à $\mathbb{Z}/2p\mathbb{Z}$.
   Il est donc nécessairement isomorphe à $G \cong (\mathbb{Z}/p\mathbb{Z}) \rtimes_\alpha (\mathbb{Z}/2\mathbb{Z})$ où $\alpha : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ est non trivial.
   Finalement,

   $$G \cong \mathbb{Z}/2p\mathbb{Z} \text{ ou } G \cong D_p$$

   en utilisant ce qui précède.

1.3 Groupes d'ordre p^3

PROPOSITION Un groupe abélien d'ordre 8 est isomorphe à l'un des groupes suivants

$$\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ ou } (\mathbb{Z}/2\mathbb{Z})^3$$

PREUVE : Le théorème de structure des groupes abéliens finis nous donne le résultat ($8 = 2^3 = 2^2 \times 2$).

C'est plus délicat pour les groupes non abéliens d'ordre 8.

PROPOSITION Soit G un groupe non abélien d'ordre 8. Alors, $G \cong Q_8$ ou $G \cong D_4$.

PREUVE : Raisonnons sur l'ordre des éléments de G.
Si G admet un élément d'ordre 8, G est cyclique donc abélien. C'est impossible par hypothèse.
Si tous les éléments de G sont d'ordre 2 alors en particulier,

$$\forall (x,y) \in G^2, xyxy = (xy)^2 = e = x^2y^2 \text{ et donc } yx = x^{-1}x^2y^2y^{-1} = xy$$

et G est abélien. C'est impossible par hypothèse. On a donc l'existence dans G d'un élément h d'ordre 4.
Notons $H =< \{h\} >$. Si on prend $g \in G \setminus H$, on obtient $G = H \cup gH$ car $|H| = |gH|$ et $gH \neq H$ car $g \notin H$. Ainsi,

$$G = \{e, h, h^2, h^3, g, gh, gh^2, gh^3\}$$

H est un sous-groupe de G d'indice 2 donc il est distingué dans G. En effet,

$$G = H \cup gH \text{ et aussi } G = H \cup Hg$$

donc $H \cup gH = H \cup Hg$ puis $Hg = gH$. On a donc $ghg^{-1} \in H$.
Si $ghg^{-1} = e$, alors $gh = g$ puis $h = e$. C'est impossible puisque h est d'ordre 4.
Si $ghg^{-1} = h^2$, comme h^2 est d'ordre 2, ghg^{-1} est d'ordre 2 (donc h aussi). C'est impossible car h est d'ordre 4.
Si $ghg^{-1} = h$, alors $gh = hg$ et G est abélien. C'est impossible par hypothèse.
Ainsi, $ghg^{-1} = h^{-1}$. On distingue (c'est le cas de le dire !) deux cas :

1. Dans le cas où $\exists k \in G \setminus H$ tel que k est d'ordre 2, alors $G =< \{h, k\} >$.
   Les relations $h^4 = e = k^2$ et $khk^{-1} = h^{-1}$ permettent de compléter la table du groupe G :

$\times$	e	h	h^2	h^{-1}	k	kh	kh^2	kh^{-1}
e	e	h	h^2	h^{-1}	k	kh	kh^2	kh^{-1}
h	h	h^2	h^{-1}	e	kh^{-1}	k	kh	kh^2
h^2	h^2	h^{-1}	e	h	kh^2	kh^{-1}	k	kh
h^{-1}	h^{-1}	e	h	h^2	kh	kh^2	kh^{-1}	k
k	k	kh	kh^2	kh^{-1}	e	h	h^2	h^{-1}
kh	kh	kh^2	kh^{-1}	k	h^{-1}	e	h	h^2
kh^2	kh^2	kh^{-1}	k	kh	h^2	h^{-1}	e	h
kh^{-1}	kh^{-1}	k	kh	kh^2	h	h^2	h^{-1}	e

   L'application qui envoie h sur r (rotation de D_4) et k sur s (symétrie de D_4) est alors un isomorphisme.
   D'où $G \cong D_4$.
2. Dans le second cas, tout élément de $G \setminus H$ est d'ordre 4 et h^2 est le seul élément d'ordre 2. Ainsi, $h^2 = g^2$.
   D'où $G =< \{h, g\} >$ avec $h^4 = e$, $g^2 = h^2$ et $ghg^{-1} = h^{-1}$. Cela permet de compléter la table de G :

$\times$	e	h	h^2	h^{-1}	g	gh	gh^2	gh^{-1}
e	e	h	h^2	h^{-1}	g	gh	gh^2	gh^{-1}
h	h	h^2	h^{-1}	e	gh^{-1}	g	gh	gh^2
h^2	h^2	h^{-1}	e	h	gh^2	gh^{-1}	g	gh
h^{-1}	h^{-1}	e	h	h^2	gh	gh^2	gh^{-1}	g
g	g	gh	gh^2	gh^{-1}	h^2	h^{-1}	e	h
gh	gh	gh^2	gh^{-1}	g	h	h^2	h^{-1}	e
gh^2	gh^2	gh^{-1}	g	gh	e	h	h^2	h^{-1}
gh^{-1}	gh^{-1}	g	gh	gh^2	h^{-1}	e	h	h^2

L'application qui à h associe I (élément de Q_8) et qui à g associe J (élément de Q_8) est alors un isomorphisme. D'où $G \cong Q_8$.

D'où le résultat recherché.

On a finalement la liste des groupes d'ordre 8 à isomorphisme près.

PROPOSITION Soit G un groupe d'ordre 8. Alors, G est isomorphe à l'un des groupes suivants

$$Q_8, D_4, \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ ou } (\mathbb{Z}/2\mathbb{Z})^3$$

PREUVE : Si G est abélien, il est isomorphe à $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou bien $(\mathbb{Z}/2\mathbb{Z})^3$. Sinon, $G \cong Q_8$ ou $G \cong D_4$.

On se place maintenant dans le cas où $p \neq 2$. Soit G un groupe d'ordre p^3.

PROPOSITION Si G est abélien, il est isomorphe à l'un des groupes suivants

$$\mathbb{Z}/p^3\mathbb{Z}, (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z}) \text{ ou } (\mathbb{Z}/p\mathbb{Z})^3$$

PREUVE : Le théorème de structure des groupes abéliens finis nous donne le résultat ($p^3 = p \times p^2 = p \times p \times p$).

Ici aussi, le cas des groupes non abéliens est plus délicat. La preuve provient de **[4]**.

PROPOSITION Si G n'est pas abélien, alors $G \cong (\mathbb{Z}/p\mathbb{Z})^2 \rtimes (\mathbb{Z}/p\mathbb{Z})$ ou $G \cong (\mathbb{Z}/p^2\mathbb{Z}) \rtimes (\mathbb{Z}/p\mathbb{Z})$.

PREUVE : Montrons que G admet un sous-groupe distingué d'ordre p.
Le centre de G est non trivial car G est un p-groupe, donc $|Z(G)| \geqslant p$. Trois cas se présentent par le théorème de Lagrange :

1. Si $|Z(G) = p^3$, G est abélien. Ce cas est donc impossible.
2. Si $|Z(G)| = p^2$, alors $G/Z(G)$ est d'ordre p donc monogène (on a $|G/Z(G)| = p$) puis G est abélien par le même argument que dans la classification des groupes d'ordre p^2. Ce cas est également impossible.
3. Si $|Z(G)| = p$, alors $G/Z(G)$ est un groupe d'ordre p^2 et $Z(G) \cong \mathbb{Z}/p\mathbb{Z}$.

On est donc dans le cas 3. et on dispose de $H = Z(G)$ tel que G/H est un groupe abélien car d'ordre p^2.
D'après la classification des groupes d'ordre p^2, deux cas se présentent à priori.

1. Si $G/H \cong \mathbb{Z}/p^2\mathbb{Z}$, alors $G/H = G/Z(G)$ est monogène et donc G est abélien. C'est impossible.
2. Sinon, $G/H \cong (\mathbb{Z}/p\mathbb{Z})^2$ et comme G/H est abélien, $\forall (g, g') \in G^2$, $(gg')H = (g'g)H$ et donc $g^{-1}g'^{-1}gg' \in H$. Ainsi, tous les commutateurs de G sont dans H.

On est donc dans le cas 2. et on peut définir l'application

$$\begin{array}{rccc} f & : & G & \longrightarrow & G \\ & & g & \longmapsto & g^p \end{array}$$

Montrons que f est un morphisme de groupes dont l'image est incluse dans H. Soient $g, g' \in G$. On a

$$g'g = gg'(g'^{-1}g^{-1}g'g)$$

Donc en posant $h = g'^{-1}g^{-1}g'g$, on a bien $h \in H = Z(G)$ (c'est un commutateur) donc

$$(gg')^p = g(g'g)^{p-1}g' = g(gg'h)^{p-1}g' = g^2(g'g)^{p-2}g'^2h^{p-1} = \cdots = g^p g'^p h^{p(p-1)/2}$$

en faisant une récurrence. Ainsi,

$$f(gg') = (gg')^p = g^p g'^p h^{p(p-1)/2}$$

Mais $h^p = e$ et p est impair donc $(p-1)/2$ est entier et

$$f(gg') = g^p g'^p (h^p)^{(p-1)/2} = g^p g'^p e^{(p-1)/2} = g^p g'^p = f(g)f(g')$$

Cela montre que f est un morphisme de groupes. De plus,

$$f(g)g' = g^p g' = g^{p-1}gg' = g^{p-1}g'gh^{-1} = \cdots = g'g^p(h^{-1})^p = g'g^p = g'f(g)$$

donc $f(g) \in Z(G) = H$ et l'image de f est bien incluse dans H.
Le noyau de ce morphisme est l'ensemble $\{g \in G, g^p = e\}$. Son cardinal vaut soit 1, soit p, soit p^2, soit p^3 (Lagrange).

1. On a H qui est de cardinal p et tous ses éléments différents du neutre sont d'ordre p donc $H \subset \ker(f)$ et comme p est impair, le cas $|\ker(f)| = 1$ est impossible ($\ker(f)$ a au moins $p-1$ éléments).
2. Si $|\ker(f)| = p$, alors le premier théorème d'isomorphisme affirme que $G/\ker(f) \cong \mathrm{Im}(f)$ et donc

$$p^2 = p^3/p = |G/\ker(f)| = |\mathrm{Im}(f)| \leqslant |H| = p$$

car $\mathrm{Im}(f) \subset H$. C'est impossible.

On est donc dans l'un des deux cas suivants.

1. Si $|\ker(f)| = |G|$, alors tout élément de G est d'ordre p. Soit $h \in H$.
Si $k \in G \setminus H$, on pose $H' =< \{h, k\} >$. Montrons que $H' \cong (\mathbb{Z}/p\mathbb{Z})^2$.
— $H_1 =< \{h\} > \cong (\mathbb{Z}/p\mathbb{Z})$ et $H_2 =< \{k\} > \cong (\mathbb{Z}/p\mathbb{Z})$. Ce sont bien entendu des sous-groupes de H'.
— Les éléments de H_1 sont dans le centre de G donc ils commutent en particulier avec les éléments de H_2.
— Tout élément de H' s'écrit sous la forme d'un produit d'éléments de H_1 et de H_2, possiblement "dans le désordre", mais comme les éléments de H_1 commutent avec ceux de H_2, on peut réécrire cet élément sous la forme d'un élément de H_1H_2. Inversement, on a bien entendu $H_1H_2 \subset H'$ et donc $H' = H_1H_2$.
— $H_1 \cap H_2 = \{e\}$ car $H_1 \cap H_2$ est en particulier un sous-groupe de H_1, donc son cardinal vaut soit 1, soit p. Or, on a pris $k \in G \setminus H$ donc l'ordre de $H_1 \cap H_2$ vaut nécessairement 1.
Maintenant, en prenant $k' \in G \setminus H'$, le sous-groupe $K' =< \{k'\} >$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
Montrons que G est isomorphe à un produit semi-direct $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes (\mathbb{Z}/p\mathbb{Z})$.
— $H' \cong (\mathbb{Z}/p\mathbb{Z})^2$ et $K' \cong (\mathbb{Z}/p\mathbb{Z})$.
— L'indice de H' dans G vaut p et p est le plus petit diviseur premier de $|G|$ dont par un théorème de Frobenius, $H' \trianglelefteq G$ (voir [**4**]).
— $H' \cap K'$ est un sous-groupe de K', différent de K' car K' n'est pas inclus dans $H' \cap K'$ (par exemple, $k' \notin H'$) donc $H' \cap K' = \{e\}$ par le théorème de Lagrange.
— $G = H'K'$ car par le second théorème d'isomorphisme,

$$H'K'/H' \cong K'/K' \cap H'$$

et donc $|H'K'| = |K'| \times |H'|/1$ d'où $|G| = |H'K'|$ et $H'K' \subset G$.
Ainsi, on a bien $G \cong (\mathbb{Z}/p\mathbb{Z})^2 \rtimes (\mathbb{Z}/p\mathbb{Z})$.
L'objectif est maintenant de démontrer que tous les produits semi-directs obtenus sont isomorphes entre eux.
Soit $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2)$ un morphisme. On peut montrer que $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2) \cong \mathrm{GL}_2(\mathbb{F}_p)$ (voir [**5**]).
L'ordre de $\mathrm{GL}_2(\mathbb{F}_p)$ est $(p^2-1)(p^2-p) = p(p^2-1)(p^2+1)$ (compter les bases de $(\mathbb{F}_p)^2$).
Donc, les sous-groupes d'ordre p sont les p-Sylow qui sont deux à deux conjugués.
Ainsi si $\psi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2)$ est un morphisme, φ et ψ décrivent le même produit semi-direct car les morphismes sont conjugués.
On a donc bien un seul produit semi-direct à isomorphisme près.
2. Sinon, $|\ker(f)| = p^2$. Dans ce cas, G a un élément c d'ordre p^2 (G a un élément d'ordre plus grand que p et cet ordre divise p^3, donc vaut p^2 car p^3 donne que G est cyclique donc abélien). c^p est un élément de H donc $c^p = h^l$ où l n'est pas multiple de p. On montre de la même manière que précédemment que G est isomorphe à $(\mathbb{Z}/p^2\mathbb{Z}) \rtimes (\mathbb{Z}/p\mathbb{Z})$, et que ce produit semi-direct est unique à isomorphisme près.

D'où le résultat annoncé.

On a terminé la classification des groupes d'ordre p^3 pour p premier impair.

PROPOSITION Soit G un groupe d'ordre p^3. Alors, G est isomorphe à l'un des groupes suivants

$$(\mathbb{Z}/p\mathbb{Z})^2 \rtimes (\mathbb{Z}/p\mathbb{Z}), (\mathbb{Z}/p^2\mathbb{Z}) \rtimes (\mathbb{Z}/p\mathbb{Z}), \mathbb{Z}/p^3\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \text{ ou } (\mathbb{Z}/p\mathbb{Z})^3$$

PREUVE : C'est un corollaire des deux propositions précédentes.

2 Les récalcitrants

Quels ordres avons nous classifié ?

Ordres	Justification
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$	ordre p
$4, 6, 9, 10, 14, 15, 21, 22, 25, 26$	ordre p^2 ou pq
$8, 27$	ordre p^3

Sans compter 16 et 24, il ne reste donc plus que les ordres $12, 18, 20, 28$ et 30.

2.1 L'ordre 12

Soit G un groupe d'ordre 12. Montrons que $n_2 = 1$ ou $n_3 = 1$. Par le second théorème de Sylow, $n_2 \mid 3$ donc $n_2 \in \{1, 3\}$.
Le même théorème fournit $n_3 \mid 4$ et $n_3 \equiv 1\ [3]$ donc $n_3 \in \{1, 4\}$.
Si $n_3 = 1$, c'est gagné. Sinon, $n_3 = 4$ et les 3-Sylow sont conjugués. Ainsi, G a 8 éléments d'ordre 3 et donc $n_2 = 1$.
G est donc le produit semi-direct d'un sous-groupe d'ordre 4 et d'un sous-groupe d'ordre 3 (ou dans l'autre sens).
On s'intéresse donc aux groupes des automorphismes de

$$\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, V_4 = (\mathbb{Z}/2\mathbb{Z})^2$$

$\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong (\mathbb{Z}/4\mathbb{Z})^*$ et $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^*$ donc $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ ($\varphi(4) = \varphi(3) = 2$).
$\mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2) \cong \mathrm{GL}_2(\mathbb{F}_2)$ donc $|\mathrm{Aut}(V_4)| = (2^2 - 1)(2^2 - 2) = 6$.
On montre par l'absurde que $\mathrm{Aut}(V_4)$ n'est pas cyclique. Ainsi, $\mathrm{Aut}(V_4) \cong \mathfrak{S}_3$ ($6 = 2 \times 3$).
On considère donc les produits semi-directs suivants :

$$V_4 \rtimes (\mathbb{Z}/3\mathbb{Z}), (\mathbb{Z}/4\mathbb{Z}) \rtimes (\mathbb{Z}/3\mathbb{Z}), (\mathbb{Z}/3\mathbb{Z}) \rtimes (\mathbb{Z}/4\mathbb{Z}) \text{ et } (\mathbb{Z}/3\mathbb{Z}) \rtimes V_4$$

Pour $V_4 \rtimes (\mathbb{Z}/3\mathbb{Z})$, on prend $\varphi : \mathbb{Z}/3\mathbb{Z} \to \mathfrak{S}_3$ un morphisme.
$\to$ Dans ce cas, $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$ (si $\mathrm{Im}(\varphi) = \{e\}$) ou $G \cong \mathfrak{A}_4$ (si $\mathrm{Im}(\varphi) \neq \{e\}$ car φ envoie un générateur de $\mathbb{Z}/3\mathbb{Z}$ sur un générateur de $\mathfrak{A}_3$). Voir **[5]** pour plus de détails.
Pour $(\mathbb{Z}/4\mathbb{Z}) \rtimes (\mathbb{Z}/3\mathbb{Z})$, soit $\varphi : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ un morphisme.
$\to$ φ est nécessairement trivial et $G \cong \mathbb{Z}/12\mathbb{Z}$ (considérer les images de 1 et de 2 par φ).
Pour $(\mathbb{Z}/3\mathbb{Z}) \rtimes (\mathbb{Z}/4\mathbb{Z})$, soit $\varphi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ un morphisme.
$\to$ On obtient $G \cong \mathbb{Z}/12\mathbb{Z}$ (si $\mathrm{Im}(\varphi) = \{e\}$) ou $G \cong (\mathbb{Z}/3\mathbb{Z}) \rtimes_\varphi (\mathbb{Z}/4\mathbb{Z})$ (c'est ni $\mathfrak{A}_4$, ni D_6).
Pour $(\mathbb{Z}/3\mathbb{Z}) \rtimes V_4$, soit $\varphi : V_4 \to \mathbb{Z}/3\mathbb{Z}$ un morphisme.
$\to$ Dans ce cas, $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$ (si $\mathrm{Im}(\varphi) = \{e\}$) ou $G \cong D_6$ (D_6 a un 2-Sylow isomorphe à V_4 : voir **[5]**).

2.2 L'ordre 18

Soit G un groupe d'ordre $18 = 2 \times 3^2$. Par le second théorème de Sylow, $n_3 = 1$ et $n_2 \in \{1, 3, 9\}$.
En notant H le 3-Sylow de G, on a $H \trianglelefteq G$ et

$$G \cong H \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z})$$

H est d'ordre $9 = 3^2$ donc $H \cong (\mathbb{Z}/9\mathbb{Z})$ ou $H \cong (\mathbb{Z}/3\mathbb{Z})^2$. On sait que $\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z}) \cong (\mathbb{Z}/9\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$.
De plus, $\mathrm{Aut}((\mathbb{Z}/3\mathbb{Z})^2) \cong \mathrm{GL}_2(\mathbb{F}_3)$. On recherche donc des morphismes $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ et $\psi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{GL}_2(\mathbb{F}_3)$ pour construire nos produits semi-directs.
Pour $H = \mathbb{Z}/9\mathbb{Z}$, soit $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$.
$\to$ Dans ce cas, $G \cong \mathbb{Z}/18\mathbb{Z}$ (si $\mathrm{Im}(\varphi) = \{e\}$) ou $G \cong D_9$ (G a un sous-groupe distingué cyclique d'ordre 9 et D_6 aussi).
Pour $H = (\mathbb{Z}/3\mathbb{Z})^2$, soit $\psi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{GL}_2(\mathbb{F}_3)$.
$\to$ Dans ce cas, l'ordre de $\psi(1)$ vaut 1 ou 2. Si c'est 1, alors $G \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$. Sinon, on doit trouver les valeurs de $\psi(1)$ d'ordre 2 à changement de base près (automorphismes intérieurs !). Le polynôme minimal de $\psi(1)$ divise nécessairement $X^2 - 1 = (X + 1)(X - 1)$. Deux possibilités :

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ et } \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

On a donc $G \cong (\mathbb{Z}/3\mathbb{Z}) \times \mathfrak{S}_3$ ou $G \cong (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes_\psi (\mathbb{Z}/2\mathbb{Z})$.

2.3 L'ordre 20

Soit G un groupe d'ordre $20 = 2^2 \times 5$. D'après le second théorème de Sylow, $n_5 \equiv 1\ [5]$ et $n_5 \mid 4$.
Donc $n_5 = 1$ et G a un sous-groupe normal d'ordre 5. Ainsi,

$$G \cong (\mathbb{Z}/5\mathbb{Z}) \rtimes_\varphi H$$

où H est $\mathbb{Z}/4\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$. On sait que $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$. On considère donc des morphismes $H \to \mathbb{Z}/4\mathbb{Z}$.
Pour $H = \mathbb{Z}/4\mathbb{Z}$, soit $\varphi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$.
$\to$ Dans ce cas, $G \cong \mathbb{Z}/20\mathbb{Z}$ (si $\mathrm{Im}(\varphi) = \{e\}$) ou $G \cong (\mathbb{Z}/5\mathbb{Z}) \rtimes_{\varphi_1} (\mathbb{Z}/4\mathbb{Z})$ ou $G \cong (\mathbb{Z}/5\mathbb{Z}) \rtimes_{\varphi_2} (\mathbb{Z}/4\mathbb{Z})$ (voir **[5]**).
Pour $H = (\mathbb{Z}/2\mathbb{Z})^2$, soit $\varphi : (\mathbb{Z}/2\mathbb{Z})^2 \to \mathbb{Z}/4\mathbb{Z}$.
$\to$ Dans ce cas, $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/10\mathbb{Z})$ (si $\mathrm{Im}(\varphi) = \{e\}$) ou $G \cong D_{10}$ (D_{10} a un 2-Sylow isomorphe à V_4).

2.4 L'ordre 28

Soit G un groupe d'ordre $28 = 2^2 \times 7$. Le second théorème de Sylow fournit $n_7 \equiv 1\ [7]$ et $n_7 \mid 4$.
Donc $n_7 = 1$ et G a un sous-groupe normal d'ordre 7. Ainsi,

$$G \cong (\mathbb{Z}/7\mathbb{Z}) \rtimes_\varphi H$$

où H est $\mathbb{Z}/4\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$. On sait que $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z}$. On considère donc des morphismes $H \to \mathbb{Z}/6\mathbb{Z}$.
Pour $H = \mathbb{Z}/4\mathbb{Z}$, soit $\varphi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$.
$\to$ Dans ce cas, $G \cong (\mathbb{Z}/28\mathbb{Z})$ ou $G \cong (\mathbb{Z}/7\mathbb{Z}) \rtimes (\mathbb{Z}/4\mathbb{Z})$ (l'image de 1 par φ est soit 0 soit 3).
Pour $H = (\mathbb{Z}/2\mathbb{Z})^2$, soit $\varphi : (\mathbb{Z}/2\mathbb{Z})^2 \to \mathbb{Z}/6\mathbb{Z}$.
$\to$ Dans ce cas, $G \cong (\mathbb{Z}/14\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ ou $G \cong D_{14}$.

2.5 L'ordre 30

Soit G un groupe d'ordre $30 = 2 \times 3 \times 5$.
Montrons que $n_3 = 1$ ou $n_5 = 1$. Second théorème de Sylow :

$$n_3 \equiv 1\ [3] \text{ et } n_3 \mid 10$$

donc $n_3 = 1$ ou $n_3 = 10$. De même,

$$n_5 \equiv 1\ [5] \text{ et } n_3 \mid 6$$

donc $n_5 = 1$ ou $n_5 = 6$. On ne peut pas avoir

$$n_3 = 10 \text{ et } n_5 = 6$$

($10 \times (3-1) = 20$ elts d'ordre 3 et $6 \times (5-1) = 24$ elts d'ordre 5). Si G a un sous-groupe N distingué d'ordre 3 (resp. d'ordre 5) : Soit H un 5-Sylow (resp. 3-Sylow) de G. $N' = NH$ est un sous-groupe d'ordre 15.
N' est d'indice 2 dans G donc $N' \trianglelefteq G$. Soit H' un 2-Sylow.
On a $N' \cong \mathbb{Z}/15\mathbb{Z}$ (ordre pq) et $H' \cong \mathbb{Z}/2\mathbb{Z}$. Ainsi,

$$G \cong (\mathbb{Z}/15\mathbb{Z}) \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z})$$

où $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/15\mathbb{Z}) \cong (\mathbb{Z}/15\mathbb{Z})^* \cong \mathbb{Z}/8\mathbb{Z}$ morphisme.
On obtient 4 morphismes, donc au plus 4 groupes d'ordre 30 (il y a 4 générateurs de $\mathbb{Z}/8\mathbb{Z}$).
$\mathbb{Z}/30\mathbb{Z}$, D_{15}, $\mathfrak{S}_3 \times (\mathbb{Z}/5\mathbb{Z})$ et $D_5 \times (\mathbb{Z}/3\mathbb{Z})$ sont deux à deux non isomorphes (nombre d'éléments d'ordre 2 : 1, 15, 3 et 5). Donc on a classifié les groupes d'ordre 30.

3 Conclusion

Le tableau ci-dessous récapitule ce que l'on a démontré. On note $\mathbb{Z}_n$ le groupe additif $\mathbb{Z}/n\mathbb{Z}$ pour $n \in \mathbb{N}^*$.

Ordre	Nombre	Groupes	Pourquoi ?
1	1	$\{e\}$	:-)
2	1	$\mathbb{Z}_2$	ordre p
3	1	$\mathbb{Z}_3$	ordre p
4	2	$\mathbb{Z}_4, (\mathbb{Z}_2)^2$	ordre p^2
5	1	$\mathbb{Z}_5$	ordre p
6	2	$\mathbb{Z}_6, D_3$	ordre pq
7	1	$\mathbb{Z}_7$	ordre p
8	5	$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, (\mathbb{Z}_2)^3, Q_8, D_4$	ordre p^3
9	2	$\mathbb{Z}_9, (\mathbb{Z}_3)^2$	ordre p^2
10	2	$\mathbb{Z}_{10}, D_5$	ordre pq
11	1	$\mathbb{Z}_{11}$	ordre p
12	5	$\mathbb{Z}_{12}, \mathbb{Z}_6 \times \mathbb{Z}_2, D_6, \mathfrak{A}_4, \mathbb{Z}_3 \rtimes \mathbb{Z}_4$	récalcitrant
13	1	$\mathbb{Z}_{13}$	ordre p
14	2	$\mathbb{Z}_{14}, D_7$	ordre pq
15	1	$\mathbb{Z}_{15}$	ordre pq
16	14		
17	1	$\mathbb{Z}_{17}$	ordre p
18	5	$\mathbb{Z}_{18}, \mathbb{Z}_6 \times \mathbb{Z}_3, D_9, \mathbb{Z}_3 \times \mathfrak{S}_3, (\mathbb{Z}_3)^2 \rtimes \mathbb{Z}_2$	récalcitrant
19	1	$\mathbb{Z}_{19}$	ordre p
20	5	$\mathbb{Z}_{20}, \mathbb{Z}_{10} \times \mathbb{Z}_2, D_{10}, \mathbb{Z}_5 \rtimes_1 \mathbb{Z}_4, \mathbb{Z}_5 \rtimes_2 \mathbb{Z}_4$	récalcitrant
21	2	$\mathbb{Z}_{21}, \mathbb{Z}_7 \rtimes \mathbb{Z}_3$	ordre pq
22	2	$\mathbb{Z}_{22}, D_{11}$	ordre pq
23	1	$\mathbb{Z}_{23}$	ordre p
24	15		
25	2	$\mathbb{Z}_{25}, (\mathbb{Z}_5)^2$	ordre p^2
26	2	$\mathbb{Z}_{26}, D_{13}$	ordre pq
27	5	$\mathbb{Z}_{27}, \mathbb{Z}_9 \times \mathbb{Z}_3, (\mathbb{Z}_3)^3, \mathbb{Z}_9 \rtimes \mathbb{Z}_3, (\mathbb{Z}_3)^2 \rtimes \mathbb{Z}_3$	ordre p^3
28	4	$\mathbb{Z}_{28}, \mathbb{Z}_{14} \times \mathbb{Z}_2, D_{14}, \mathbb{Z}_7 \rtimes \mathbb{Z}_4$	récalcitrant
29	1	$\mathbb{Z}_{29}$	ordre p
30	4	$\mathbb{Z}_{30}, D_{15}, \mathfrak{S}_3 \times \mathbb{Z}_5, D_5 \times \mathbb{Z}_3$	récalcitrant
31	1	$\mathbb{Z}_{31}$	ordre p

Liste des groupes d'ordre plus petit que 31 *à isomorphisme près (sans* 16 *ni* 24*).*

Il reste à trouver les groupes d'ordre 24 à isomorphisme près et les groupes d'ordre 16 à isomorphisme près...

Bibliographie :

- [**1**] Cours d'algèbre, *Daniel Perrin*
- [**2**] Groupes finis et treillis de leurs sous-groupes, *Alain Debreil.*
- [**3**] Exercices d'algèbre, *Pascal Ortiz*
- [**4**] Outils de base pour la classification des groupes de petit cardinal, *Philippe Caldero.*
- [**5**] Théorie des groupes, *Felix Ulmer*
- [**6**] `https://oeis.org/A000001`
- [**7**] `https://web.archive.org/web/20190725032846/http://www.icm.tu-bs.de/ag_algebra/software/small/number.html`