PREMIÈRE PARTIE : GROUPES

Cette partie est consacrée à l'étude des groupes, et plus particulièrement des groupes finis. La première section concerne les célèbres théorèmes de Sylow. On introduit ensuite la notion de produit semi-direct, qui apparaît naturellement dans l'étude de la structure des groupes, finis ou non. On termine cette partie par le cas particulier des groupes abéliens finis.

1. Théorèmes de Sylow

1.1. **Motivation.** D'après le théorème de Lagrange, l'ordre de tout sous-groupe H d'un groupe fini G divise l'ordre du groupe ; si G est fini, alors $H \subset G \Rightarrow |H|||G|$.

Question : qu'en est-il de la réciproque ? Autrement dit, étant donné un groupe fini G, et $d||G|$, existe-t-il un sous-groupe $H \subset G$ d'ordre d.

C'est le cas pour un groupe cyclique d'ordre n. Cependant, le groupe alterné A_4 est un groupe d'ordre 12 n'admettant aucun sous-groupe d'ordre 6. Mais le premier théorème de Sylow apporte une réciproque partielle au théorème de Lagrange : si $p^r||G|$ avec p premier, alors G admet un sous-groupe d'ordre p^r

1.2. **Lemme de Cauchy.** Avant de démontrer cet énoncé, commençons par établir le *lemme de Cauchy*. On peut l'obtenir comme application de la *formule des classes* qui est l'outil essentiel de la démonstration des théorèmes de Sylow. Rappelons ce dont il s'agit.

Soit G un groupe agissant sur un ensemble X fini. L'action de G sur X partitionne X en r orbites $\omega_1, \ldots, \omega_r$:

$$X = \bigsqcup_{i=1}^{r} \omega_i.$$

Choisissons pour tout i un élément $x_i \in \omega_i$. On a alors $\omega_i = G \cdot x_i$, et l'ensemble ω_i est en bijection avec G/G_{x_i} :

$$G/G_{x_i} \simeq \omega_i,$$

où G_{x_i} désigne le *stabilisateur* de x_i, aussi noté $\mathrm{Stab}(x_i)$:

$$G_{x_i} = \mathrm{Stab}(x_i) = \{g \in G, g \cdot x_i = x_i\}.$$

Le cardinal de ω_i est donc égal à celui de l'ensemble quotient G/G_{x_i}, qui est par définition l'*indice* $[G : G_{x_i}]$ du sous-groupe G_{x_i} dans G. De plus, lorsque G est **finie**, cet indice est égal à

$$\operatorname{card} \omega_i = \operatorname{card}(G/G_{x_i}) = \frac{|G|}{|G_{x_i}|}.$$

La formule des classes s'écrit alors simplement pour l'action d'un groupe G sur un ensemble fini X dont les orbites sont représentées par les éléments $x_1, \ldots, x_r$

$$\operatorname{card} X = \sum_{i=1}^{r} \operatorname{card} \omega_i = \sum_{i=1}^{r} \operatorname{card} G/G_{x_i} = \sum_{i=1}^{r} [G : G_{x_i}],$$

et, si G est également **finie**, elle devient

$$\operatorname{card} X = \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}.$$

Date: 9 mars 2021.

Théorème 1.2.1 (Lemme de Cauchy)**.** *Soit p un diviseur premier de l'ordre d'un groupe fini G. Alors G admet un élément d'ordre p.*

Démonstration. Notons $n = |G|$. Considérons l'ensemble

$$X = \{(g_1, \dots, g_p) \in G^p, g_1 g_2 \cdots g_p = e\}.$$

C'est un sous-ensemble du produit G^p de cardinal n^{p-1} (en effet, $G^{p-1} \to X, (g_1, \dots, g_{p-1}) \mapsto (g_1, \dots, g_{p-1}, g_{p-1}^{-1} g_{p-2}^{-1} \cdots g_1^{-1})$ est une bijection).

Considérons la permutation $(g_1, \dots, g_p) \mapsto (g_2, \dots, g_p, g_1)$ de G^p. Elle envoie X sur X, et définit ainsi une permutation σ de X, d'ordre p. Soit $H = \langle \sigma \rangle$ le sous-groupe cyclique de S_X d'ordre p engendré par σ (on note S_X le groupe des permutations (i.e. bijections) de X). Ce groupe agit naturellement sur X, et la formule des classes assure que, si $x_1, \dots, x_r$ est un système de représentants des orbites, alors

$$\operatorname{card} X = \sum_{i=1}^{r} \frac{|H|}{|H_{x_i}|}.$$

La situation ici est particulièrement simple : puisque H est d'ordre p premier, l'indice $\frac{|H|}{|H_{x_i}|} = [H : H_{x_i}]$ de H_{x_i} dans H vaut 1 ou p. Il vaut 1 si H_{x_i} est égal à H, et p si $H_{x_i} = \{e\}$.

Remarquons alors que $H_{x_i} = H$ signifie que x_i est fixé par tous les éléments de H, autrement dit ici que x_i est un p-uplet de la forme $(g, g, \dots, g)$.

Pour conclure, notons qu'il y a visiblement dans X une orbite à 1 élément, celle de $\{e, e, \dots, e\}$. On déduit de la formule des classes qu'il y en a au moins une autre (en fait au moins p) : en effet, en réduisant modulo p l'égalité

$$n^{p-1} = \operatorname{card} X = \sum_{i=1}^{r} \frac{|H|}{|H_{x_i}|}$$

et en rappelant que p divise n et que $\frac{|H|}{|H_{x_i}|}$ vaut 1 ou p, on obtient que

$$\operatorname{card}\{i, H = H_{x_i}\} \equiv 0 \mod p,$$

et, puisque cet ensemble contient au moins un élément, il doit en contenir au moins p.

Il existe donc $g \neq e$ dans G tel que $(g, \dots, g) \in X$, i.e. $g^p = e$. Un tel g est d'ordre p. □

1.3. p-groupes.

Définition 1.3.1 (p-groupe)**.** Soit p un nombre premier. Un p-groupe est un groupe fini dont le cardinal est une puissance de p.

Proposition 1.3.2. *Soit p un nombre premier. Un groupe fini est un p-groupe si et seulement si tous ses éléments sont d'ordre une puissance de p.*

Démonstration. D'après le théorème de Lagrange, l'ordre d'un élément d'un p-groupe P d'ordre p^r divise $|P| = p^r$, donc est lui-même une puissance de p.

Réciproquement, supposons que tout élément d'un groupe fini non trivial P a pour ordre une puissance de p. Soit q premier divisant $|P|$. D'après le lemme de Cauchy 1.2.1, P possède un élément d'ordre q. Par hypothèse, $q = p$. Ainsi p est l'unique diviseur premier de $|P|$, et P est donc un p-groupe. □

Les p-groupes jouissent de nombreuses propriétés remarquables. En voici une qui sera utilisée dans la démonstration des théorèmes de Sylow :

Lemme 1.3.3 (Points fixes sous l'action d'un p-groupe)**.** *Soit p un nombre premier. Soit P un p-groupe opérant sur un ensemble fini X. Notons $X^P = \{x | \forall g \in P, g \cdot x = x\}$ l'ensemble des* points fixes *de X sous l'action de P. Alors*

$$\operatorname{card} X^P \equiv \operatorname{card} X \mod p.$$

Démonstration. Décomposons X en réunion disjointe de ses orbites sous l'action de P : $X = \bigsqcup_i X_i$. Le cardinal d'une telle orbite $X_i = P \cdot x_i$ divise P (car $p \in P \mapsto p \cdot x_i$ réalise l'orbite X_i comme un quotient de P (par le stabilisateur P_{x_i}), d'où $\operatorname{card} P \cdot x_i = [P : P_{x_i}] | |P|$. Il est donc égal à 1 ou divisible par p.

De plus, $\operatorname{card} P \cdot x = 1 \Leftrightarrow x \in X^P$.

On a donc

$$\operatorname{card} X = \sum_i \operatorname{card} X_i = \sum_{i | \operatorname{card} X_i = 1} 1 + \sum_{i | \operatorname{card} X_i \neq 1} \operatorname{card} X_i \equiv \operatorname{card} X^P \mod p.$$

□

1.4. p-sous-groupe de Sylow ou p-Sylow, premier et deuxième théorèmes de Sylow.

Définition 1.4.1 (p-sous-groupe de Sylow ou p-Sylow)**.** Soient G un groupe fini d'ordre n et p un nombre premier. Soit r tel que $n = p^r m$ avec $p \not| n$. On appelle p-sous-groupe de Sylow ou p-Sylow de G un sous-groupe de cardinal p^r.

Ainsi, un p-Sylow d'un groupe fini G est un sous-groupe d'ordre la plus grande puissance de p divisant $|G|$.

Remarque 1.4.2. Soit S un sous-groupe de G fini, et soit p un nombre premier. Alors S est un p-Sylow si et seulement si S est un p-groupe d'indice $[G : S]$ premier à p.

Le premier théorème de Sylow assure l'existence de tels sous-groupes.

Théorème 1.4.3 (Premier et deuxième théorèmes de Sylow)**.** *Soit p premier. Tout groupe fini possède au moins un p-Sylow. Le nombre n_p des p-Sylow de G est congru à 1 modulo p :*

$$n_p \equiv 1 \mod p.$$

Plus généralement, tout groupe fini G d'ordre n admet des sous-groupes d'ordres p^s avec p premier et $p^s | n$, et le nombre de ces sous-groupes est congru à 1 modulo p.

Démonstration. Il existe de nombreuses démonstrations de ce théorème, mais qui sont toutes des variations sur le thème des actions de groupes et de la formule des classes. En voici une suivant Miller-Wielandt, avec une belle combinatoire. Pour plus de clarté, nous donnons d'abord la démonstration pour les p-Sylow, et esquissons les modifications pour le cas général.

Soit G un groupe d'ordre $n = p^r m$ avec m premier à p. On note X l'ensemble des parties de G à p^r éléments, et Y l'ensemble des p-Sylow de G.

Le groupe G opère sur X par translation à gauche : si $A \subset G$ est une partie à p^r éléments, $g \cdot A = gA = \{ga, a \in A\}$. L'orbite $G \cdot A$ d'un élément $A \in X$ a pour cardinal $[G : G_A]$.

Remarquons que pour tout $A \in X$, $|G_A| \leqslant p^r$: en effet [1], si $a \in A$, alors l'application injective $g \in G_A \mapsto ga$ envoie G_A dans A de cardinal p^r.

On a donc deux cas :

— ou bien $|G_A| < p^r$, et $\operatorname{card} GA$ est divisible par p,

— ou bien $|G_A| = p^r$ (i.e. G_A est un p-Sylow), et $\operatorname{card} GA = m$.

1. On a mieux : $|G_A| | p^r$. En effet, G_A agit sur A librement, d'où $p^r = \operatorname{card} A = |G_A| \cdot \operatorname{card} A/G_A$.

Cela nous conduit à considérer $X' = \{A \in X | |G_A| = p^r\}$ et $X'' = \{A \in X | |G_A| < p^r\}$ qui sont stables par l'action de G (car de manière générale $G_{gx} = gG_xg^{-1}$) et vérifient $X = X' \bigsqcup X''$.

Les orbites de X'' sous l'action de G sont toutes de cardinal divisible par p, donc $p | \operatorname{card} X''$ (X'' est l'union disjointe de ces orbites).

On détermine le cardinal de X' en le décomposant non pas selon ses orbites sous l'action de G, mais en sous-ensembles de points ayant le même stabilisateur [2]. Par définition, $A \in X' \Leftrightarrow G_A \in Y$, de sorte que

$$X' = \bigsqcup_{S \in Y} \{A \in X' | G_A = S\}.$$

Montrons alors que, pour tout $S \in Y$, $\{A \in X' | G_A = S\}$ est de cardinal $[G : S] = m$. Soit donc $S \in Y$. Alors, pour tout $g \in G$, Sg a p^r éléments et son stabilisateur G_{Sg} est égal à S (ce stabilisateur contient visiblement S, et, puisque $|S| = p^r \geqslant |G_{Sg}|$, il lui est égal). Par ailleurs, si $A \in X'$ vérifie $G_A = S$, alors $SA (= \{sa | s \in S, a \in A\}) = A$, donc, si $a \in A$, on a $Sa \subset A$, puis, par égalité des cardinaux (finis), $Sa = A$. On a donc montré que $\{A \in X' | G_A = S\} = \{Sg, g \in G\}$. C'est exactement l'ensemble des classes (à droite !) relativement à S (ensemble noté $S\backslash G$) dont le cardinal est égal à $\frac{|G|}{|S|} = m$ (en effet, deux classes à droite Sg et Sg' sont disjointes ou confondues, et elles ont le même cardinal $|S|$; elles forment donc une partition de G en $\frac{|G|}{|S|}$ sous-ensembles de cardinal $|S|$).

On en déduit

$$\operatorname{card} X' = \sum_{S \in Y} \operatorname{card}\{A \in X' | G_A = S\} = \sum_{S \in Y} m = m \operatorname{card} Y,$$

puis

$$\binom{p^r m}{p^r} = \operatorname{card} X = \operatorname{card} X' + \operatorname{card} X'' \equiv m \operatorname{card} Y \mod p.$$

En particulier, puisque m est inversible modulo p, la classe de $\operatorname{card} Y$ modulo p ne dépend que de l'ordre n du groupe G, et pas du groupe lui-même.

On peut en particulier considérer $G = \mathbf{Z}/n\mathbf{Z}$. Ce groupe cyclique contient un unique p-Sylow (engendré par la classe de m modulo n) [3], ce qui montre que pour ce groupe, et donc pour tout groupe d'ordre n, $\operatorname{card} Y \equiv 1 \mod p$.

Voici les modifications (mineures) à apporter pour obtenir le résultat concernant les sous-groupes d'ordre p^s avec $s \leqslant r$. On note X_s l'ensemble des parties de G à p^s éléments, et Y_s l'ensemble des sous-groupes de G d'ordre p^s.

---

2. Voici un autre argument, peut-être plus clair, où on raisonne sur ces orbites sous G : revenons à la description des stabilisateurs. On remarque en fait que, pour chaque $A \in X$, l'orbite GA contient un unique A_0 tel que $e \in G$. De plus,

$$\operatorname{card}(GA) = m \Leftrightarrow |G_{A_0}| = p^r \Leftrightarrow G_{A_0} = A_0 \Leftrightarrow A_0 \text{ sous-groupe de } G.$$

En effet, la première équivalence résulte de ce qui précède puisque $GA = GA_0$. Pour la deuxième, il faut remarquer que, si $|G_{A_0}| = p^r$, alors pour tout $a_0 \in A_0$, l'application $g \in G_{A_0} \mapsto ga_0$ est bijective (on a déjà noté qu'elle était toujours injective, et par hypothèse les deux ensembles ont le même cardinal fini), et, puisque $e \in A_0$, on conclut en prenant $a_0 = e$. Pour la dernière, il faut montrer que si A_0 est un sous-groupe, alors $G_{A_0} = A_0$. Mais $A_0 \subset G_{A_0}$ et $\operatorname{card} A_0 = p^r \geqslant |G_{A_0}|$ (ou $e \in A_0$ entraîne $G_{A_0} = G_{A_0}e \subset G_{A_0}A_0 \subset A_0$) permettent de conclure.

L'ensemble X se décompose en orbites de cardinal divisible par p et en orbites de cardinal m, et chacune de ces orbites de cardinal m contient un et un seul sous-groupe d'ordre p^r. Autrement dit, le nombre $\operatorname{card} Y$ de sous-groupes d'ordre p^r est égal au nombre d'orbites de cardinal m, et $\operatorname{card} X \equiv m \operatorname{card} Y \mod p$.

3. On peut le montrer en se ramenant à l'étude des sous-groupes de $\mathbf{Z}$ en considérant l'image réciproque d'un sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ par la projection $\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ ou en constatant que pour tout entier positif d divisant n, $\mathbf{Z}/n\mathbf{Z}$ contient exactement d éléments d'ordre divisant d.

On fait agir G sur X_s par translations à gauche, le stabilisateur G_A de $A \in X_s$ est d'ordre $\geqslant p^s$, avec égalité si et seulement si $G_A \in Y_s$.

Écrivons $X_s = X'_s \bigsqcup X''_s$ avec $X's = \{A \in X_s || G_A| = p^s\}$ et $X''_s = \{A \in X_s || G_A| < p^s\}$ tous deux stables sous l'action de G. En décomposant X''_s en orbites sous l'action de G, on constate que $\operatorname{card} X''_s$ est divisible par p^{r-s+1}, et, en décomposant X'_s suivant les stabilisateurs de l'action de G, on obtient $\operatorname{card} X'_s = mp^{r-s} \operatorname{card} Y_s$.

On a alors $\binom{p^r m}{p^s} = \operatorname{card} X_s = \operatorname{card} X'_s + \operatorname{card} X''_s \equiv mp^{r-s} \operatorname{card} Y_s \mod p^{r-s+1}$. Pour conclure, remarquons à nouveau que cette formule est vraie pour le groupe cyclique d'ordre mp^r, qui admet un unique sous-groupe d'ordre p^s (le sous-groupe engendré par la classe de $p^{r_s}m$), ce qui entraîne la congruence $\binom{p^r m}{p^s} \equiv mp^{r-s} \mod p^{r-s+1}$. On a donc $p^{r-s}m(\operatorname{card} Y_s - 1) \equiv 0 \mod p^{r-s+1}$, d'où, encore avec m premier à p,

$$\operatorname{card} Y_s = 1 \mod p.$$

Le nombre de sous-groupes de G d'ordre p^s est donc congru à 1 modulo p. □

Remarque 1.4.4. La démonstration établit au passage le résultat non trivial

$$\text{si } p \not| m, \text{ alors } \binom{p^r m}{p^r} \equiv m \mod p$$

(et, plus généralement pour $s \leqslant r$ et $p \not| m$, $p^{r-s} | \binom{p^r m}{p^s}$ et $\frac{1}{p^{r-s}}\binom{p^r m}{p^s} \equiv m \mod p$).

Cette congruence peut se démontrer directement de plusieurs façons. On l'obtient par exemple rapidement en écrivant, dans l'algèbre $\mathbf{F}_p[X]$ des polynômes à une indéterminée sur le corps $\mathbf{F}_p$ à p éléments, $(1+X)^{p^r m} = ((1+X)^{p^r})^m = (1+X^{p^r})^m$. En considérant le coefficient de degré p^r, on obtient $\binom{p^r m}{p^r} = m$ dans $\mathbf{F}_p$, ce qui est exactement la congruence annoncée.

Cette congruence et sa généralisation s'obtiennent aussi simplement en écrivant

$$\binom{p^r m}{p^s} = \frac{(p^r m)!}{(p^s)!(p^r m - p^s)!} = \prod_{k=0}^{p^s-1} \frac{p^r m - k}{p^s - k} = p^{r-s} m \prod_{k=1}^{p^s-1} \frac{p^r m - k}{p^s - k}.$$

Le dernier facteur est un entier A (c'est $\binom{p^r m - 1}{p^s - 1}$) qui vérifie $A \prod_{k=1}^{p^s-1}(p^s - k) = \prod_{k=1}^{p^s-1}(p^r m - k)$. Pour montrer qu'il est congru à 1 modulo p, écrivons $1 \leqslant k \leqslant p^s - 1$ sous la forme $k = p^{t_k} l_k$ avec $0 \leqslant t_k < s$ et l_k premier à p. On a alors $\prod_{k=1}^{p^s-1}(p^r m - k) = \prod_{k=1}^{p^s-1}(p^r m - p^{t_k} l_k) = \prod_{k=1}^{p^s-1} p^{t_k}(p^{r-t_k} m - l_k)$, et $A \prod_{k=1}^{p^s-1}(p^s - k) = A \prod_{k=1}^{p^s-1}(p^s - p^{t_k} l_k) = A \prod_{k=1}^{p^s-1} p^{t_k}(p^{s-t_k} - l_k)$, d'où $A \prod_{k=1}^{p^s-1} p^{t_k}(p^{s-t_k} - l_k) = \prod_{k=1}^{p^s-1} p^{t_k}(p^{r-t_k} m - l_k)$, puis $A \prod_{k=1}^{p^s-1}(p^{s-t_k} - l_k) = \prod_{k=1}^{p^s-1}(p^{r-t_k} m - l_k)$. Enfin, puisque, pour tout k, $r - t_k \geqslant s - t_k \geqslant 1$, $p^{r-t_k} m - l_k$ et $p^{s-t_k} - l_k$ sont deux entiers congrus à l_k *inversible* modulo p. On en déduit $A \equiv 1 \mod p$, d'où la congruence annoncée.

Remarque 1.4.5. Une autre très belle démonstration du premier théorème de Sylow est basée sur la remarque que le groupe linéaire $\mathbf{GL}_n(\mathbf{F}_p)$ sur le corps à p éléments possède un p-Sylow. Il suffit alors de rappeler que tout groupe fini d'ordre n se plonge comme sous-groupe de $\mathbf{GL}_n(\mathbf{F}_p)$ (pour p premier quelconque) : en effet, $g \in G \mapsto (h \mapsto gh) \in S_G$ est un morphisme de groupe injectif de G dans le groupe S_G des permutations de G, isomorphe au groupe symétrique S_n. Et le groupe symétrique S_n se plonge dans $\mathbf{GL}_n(\mathbf{F}_p)$, via le morphisme de groupes associant à $\sigma \in S_n$ la matrice de l'application envoyant e_i sur e_{σ_i}, où $e_1, \ldots, e_n$ est la base canonique de $\mathbf{F}_p^n$ (i.e. la matrice P_σ dont les coefficients sont définis par $(P_\sigma)_{ij} = 1$ si $i = \sigma(j)$, et 0 sinon). On conclut alors en montrant que si H est un sous-groupe de G et S un p-Sylow de G, alors il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.

Remarque 1.4.6. Le lemme de Cauchy est un corollaire du premier théorème de Sylow : si $p||G|$, alors G admet un p-Sylow S, qui n'est pas réduit à $\{e\}$ puisque $p||G|$. Soit donc g un élément non trivial de ce p-Sylow S. L'ordre de g divise $|S|$, donc est une puissance p^k de p avec $k \geqslant 1$ (puisque $g \neq e$). Alors $g^{p^{k-1}}$ est d'ordre p.

1.5. **Conjugaison des p-Sylow et troisième théorème de Sylow.** On considère maintenant l'action de G par conjugaison sur l'ensemble des p-Sylow. Rappelons que l'*action par conjugaison* de G sur lui-même est définie par $G \times G \to G, (g,h) \mapsto g \cdot h = ghg^{-1}$. Le conjugué gHg^{-1} d'un sous-groupe H est un sous-groupe de même ordre. En particulier, G agit par conjugaison sur l'ensemble de ses p-Sylow.

Les théorèmes de Sylow donnent de précieuses informations sur l'ensemble des p-Sylow.

Théorème 1.5.1 (Troisième théorème de Sylow)**.** *Soit G un groupe fini, et soit p un nombre premier.*

(1) Tout p-sous-groupe de G est contenu dans un p-Sylow.

(2) Les p-Sylow sont deux à deux conjugués.

(3) Le nombre n_p de p-Sylow de G est congru à 1 modulo p et divise n (donc divise m, où $|G| = p^r m$ avec m premier à p) :

$$n_p \equiv 1 \mod p \text{ et } n_p | m.$$

Démonstration. Soit S un p-Sylow de G (dont l'existence est assurée par 1.4.3) et P un p-sous-groupe de G.

Le p-sous-groupe P opère (par multiplication à gauche) sur l'ensemble $X = \{gS, g \in G\} = G/S$ des classes à gauche suivant S, ensemble de cardinal $m \not\equiv 0 \mod p$. D'après le lemme 1.3.3, $\operatorname{card} X^P \equiv \operatorname{card} X \equiv m \not\equiv 0 \mod p$. En particulier, $\operatorname{card} X^P$ est non nul, donc il existe donc une classe $x \in X$ fixée par P. Le stabilisateur G_x de x *sous l'action de G sur $X = G/S$* contient donc P, et est de plus un conjugué de S (car, si $x = gS$, alors $h \cdot x = x \Leftrightarrow hgS = gS \Leftrightarrow h \in gSg^{-1}$), autrement dit un p-Sylow. Cela établit *(1)*.

Remarquons qu'on a montré un peu plus : étant donné un p-Sylow S, alors tout p-sous-groupe P est contenu dans un conjugué de S.

En particulier, tout (autre) p-Sylow S' est contenu dans un conjugué de S : il existe $g \in G$ tel que $S' \subset gSg^{-1}$. Vu les ordres, on a égalité $S' = gSg^{-1}$. Cela prouve *(2)*.

La dernière assertion en découle facilement : le groupe G opère par conjugaison sur l'ensemble $\mathcal{S}_p$ des p-Sylow de G, et le point *(2)* assure que cette action possède une seule orbite. Le cardinal de cette orbite est donc égal à $\operatorname{card} \mathcal{S}_p = n_p$. Par ailleurs, le cardinal d'une orbite divise toujours l'ordre du groupe. On a donc $n_p | n$ et, si $n = mp^r$ avec m premier à p, la congruence $n_p \equiv 1 \mod p$ entraîne $n_p | m$. □

1.6. **Application à la (non) simplicité.** Les théorèmes de Sylow permettent d'obtenir des conditions numériques suffisantes à l'existence d'un sous-groupe distingué non trivial dans un groupe fini G.

Corollaire 1.6.1. *Soit S un p-Sylow de G. Alors S est distingué dans G si et seulement si S est l'unique p-Sylow.*

En particulier, si le nombre de p-Sylow est égal à 1, alors l'unique p-Sylow est un sous-groupe distingué.

Démonstration. En effet, les p-Sylow sont deux à deux conjugués. D'autre part, un sous-groupe est distingué si et seulement si il coïncide avec tous ses conjugués. □

Définition 1.6.2 (Groupe simple)**.** Un groupe G est *simple* s'il est non trivial et si ses seuls sous-groupes distingués sont le groupe trivial et le groupe G.

Les théorèmes de Sylow permettent d'obtenir la non simplicité dans de nombreux cas. Par exemple :

Proposition 1.6.3. *Soit G un groupe d'ordre pq avec p et q deux nombres premiers distincts. Alors G n'est pas simple.*

Démonstration. Supposons $p < q$. D'après les théorèmes de Sylow, le nombre n_q de q-Sylow est d'une part congru à 1 modulo q, et d'autre part divise p.

Puisque p est premier, la seconde condition signifie que n_q est égal à 1 ou p. Mais $p < q \Rightarrow p \not\equiv 1 \mod q$, et on a donc $n_q = 1$. Le groupe G admet un unique q-Sylow, et ce sous-groupe est donc distingué. Ainsi G n'est pas simple. □

Proposition 1.6.4. *Un groupe d'ordre* 63 *n'est pas simple.*

Démonstration. Puisque $63 = 3^2 \times 7$, le nombre de 7-Sylow est divise 9 et est congru à 1 modulo 7. Ce ne peut être que 1. Autrement dit G admet un unique 7-Sylow, nécessairement distingué. Le groupe G n'est donc pas simple. □

2. Produits directs et semi-directs

Un sous-groupe distingué $N \lhd G$ d'un groupe G définit un groupe quotient G/N. On a ainsi deux groupes N et G/N plus « petits »(si G est fini, on a deux groupes d'ordres inférieurs à l'ordre de G). Il est naturel de chercher à reconstituer G à partir de N et G/N.

2.1. Suites exactes, extensions.

Définition 2.1.1 (Suite exacte)**.** Une *suite exacte* (ou *suite exacte courte*)

$$1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$$

est la donnée de trois groupes N, G et H et de deux morphismes de groupes $i\colon N \to G$ et $p\colon G \to H$ tels que

— i injectif ;
— p surjectif ;
— $\ker p = \operatorname{im} i$.

Si G s'insère dans une telle suite exacte, on dit que G est une *extension* de H par N.

Remarque 2.1.2. Si la suite $1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$ est exacte, alors le sous-groupe $i(N)$ (isomorphe à N) est distingué, puisque que c'est le noyau du morphisme p, et la projection p induit un isomorphisme de groupes $G/N \xrightarrow{\sim} H$ (ou plutôt $G/i(N) \xrightarrow{\sim} H$).

Inversement, tout sous-groupe distingué $N \lhd G$ induit une suite exacte

$$1 \to N \subset G \xrightarrow{p} G/N \to 1.$$

Exemple 2.1.3. Le groupe symétrique S_n est une extension

$$1 \to A_n \to S_n \xrightarrow{\varepsilon} \{\pm 1\} \to 1,$$

où ε est la signature.

Le groupe linéaire $\mathbf{GL}_n(k)$ s'insère dans une suite exacte

$$1 \to \mathbf{SL}_n(k) \to \mathbf{GL}_n(k) \xrightarrow{\det} k^* \to 1.$$

2.2. Produits directs.

Proposition-Définition 2.2.1 (Produit direct)**.** *Le produit direct de deux groupes N et H, noté $N \times H$, est le produit cartésien*

$$N \times H = \{(n, h), n \in N, h \in H\}$$

muni de la loi de groupe définie par $(n, h)(n', h') = (nn', hh')$.

Démonstration. On vérifie sans difficulté que cela définit bien une loi de groupe sur le produit cartésien $N \times H$. □

Le produit direct $N \times H$ de deux groupes N et H vérifie de nombreuses propriétés :

— $\iota_N \colon N \to N \times H, n \mapsto (n, e_H)$ et $\iota_H \colon H \to N \times H, h \mapsto (e_N, h)$ sont deux morphismes de groupes injectifs, et on note souvent $N \times \{e_H\}$ ou $\overline{N}$ l'image de ι_N et $\{e_N\} \times H$ ou $\overline{H}$ l'image de ι_H ;
— les projections $p_N \colon N \times H \to N, (n, h) \mapsto n$ et $p_H \colon N \times H \to H, (n, h) \mapsto h$ sont deux morphismes de groupes surjectifs ;
— $\ker p_N = \overline{H}$ et $\ker p_H = \overline{N}$;
— $\overline{N}$ et $\overline{H}$ sont distingués dans $N \times H$, et, mieux, $\forall \bar{n} \in \overline{N}, \forall \bar{h} \in \overline{H}, \bar{n}\bar{h} = \bar{h}\bar{n}$;
— $\overline{N} \cap \overline{H} = \{e\}$ et $\overline{N}\,\overline{H} = N \times H$ (où $\overline{N}\,\overline{H} = \{\bar{n}\bar{h}, \bar{n} \in \overline{N}, \bar{h} \in \overline{H}\}$) ;
— la restriction de $p_H \colon G \to H$ à $\overline{H}$ induit un isomorphisme de $\overline{H} \xrightarrow{\sim} H$ (et la restriction de p_N à $\overline{N}$ induit un isomorphisme $\overline{N} \xrightarrow{\sim} N$).

Notons que les trois premières propriétés signifient exactement qu'on a deux suites exactes $1 \to N \to N \times H \to H \to 1$ et $1 \to H \to N \times H \to N \to 1$.

Dans les questions de classification, une notion fondamentale est celle de produit direct de sous-groupes :

Définition 2.2.2 (Produit direct de sous-groupes)**.** Soit G un groupe. Soient H et K deux sous-groupes de G. On dit que G est *produit direct des sous-groupes* H et K (et on note $G = H \times K$) si l'application

$$\begin{array}{ccc} H \times K & \longrightarrow & G \\ (h, k) & \longmapsto & hk \end{array}$$

est un isomorphisme de groupes.

Remarque 2.2.3. Le produit direct de deux groupes N et H est le produit direct de ses sous-groupes $\overline{N} = \mathrm{im}(n \to (n, e_H))$ et $\overline{H} = im(h \mapsto (e_N, h))$.

En conséquence, dire qu'un groupe G est isomorphe au produit direct de deux groupes G_1 et G_2 revient à dire que G est produit direct de deux sous-groupes $H_1 \subset G$ et $H_2 \subset G$ respectivement isomorphes à G_1 et G_2.

Voici un exemple bien connu de produit direct :

Proposition 2.2.4 (Lemme chinois)**.** *Soient m et n des entiers premiers entre eux. On a un isomorphisme (de groupes)*

$$\mathbf{Z}/mn\mathbf{Z} \simeq \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}.$$

Démonstration. On vérifie que l'application

$$k \in \mathbf{Z} \mapsto (k \mod m, k \mod n) \in \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$$

est un morphisme de groupes dont le noyau est exactement $mn\mathbf{Z}$ (en effet, k appartient au noyau si et seulement si m et n divisent k, donc si et seulement si leur produit mn divise k, puisqu'ils sont premiers entre eux). Elle induit donc un morphisme injectif $\mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$. Vu que les deux ensembles ont même cardinal mn, le morphisme est un isomorphisme de groupes. □

En termes de sous-groupes, le lemme chinois montre que si m et n sont premiers entre eux le groupe $\mathbf{Z}/mn\mathbf{Z}$ est le produit direct du groupe engendré par la classe de n et du groupe engendré par la classe de m : $\mathbf{Z}/mn\mathbf{Z} = \langle \bar{n} \rangle \times \langle \bar{m} \rangle$. On l'utilise rarement sous cette forme.

Donnons une condition nécessaire et suffisante pour reconnaître qu'un groupe est produit direct de deux sous-groupes (ou de deux groupes).

Proposition 2.2.5. *Soit G un groupe. Soient H et K deux sous-groupes de G. Alors G est produit direct de H et K si et seulement si*

(i) $\forall h \in H, \forall k \in K, hk = kh$,

(ii) $H \cap K = \{e\}$,

(iii) $HK = G$.

Si G est fini, on peut remplacer la dernière condition par $|G| = |H||K|$.

Démonstration. Considérons l'application

$$\begin{array}{rccc} \mu & : & H \times K & \longrightarrow & G \\ & & (h,k) & \longmapsto & hk. \end{array}$$

Pour $h, h' \in H$ et $k, k' \in K$, on a $\mu(h,k)\mu(h',k') = \mu((h,k)(h',k')) \Leftrightarrow hkh'k' = hh'kk' \Leftrightarrow kh' = h'k$, de sorte que μ est un morphisme de groupes si et seulement si $\forall h \in H, \forall k \in K, hk = kh$.

Supposons donc que μ est un morphisme. Alors $(h,k) \in \ker\mu \Leftrightarrow hk = e \Leftrightarrow k = h^{-1}$, de sorte que $\ker\mu = \{(h,h^{-1}), h \in H \cap K\}$ isomorphe à $H \cap K$ (par $h \mapsto (h,h^{-1})$). Ainsi μ injectif si et seulement si $H \cap K = \{e\}$.

Par définition, μ surjectif si et seulement si $HK = G$.

Cela montre l'équivalence annoncée. □

Voici un résultat un peu plus fort, où on affaiblit l'hypothèse (i) :

Proposition 2.2.6. *Un groupe G est produit direct des deux sous-groupes H et K si et seulement si H et K sont distingués, $H \cap K = \{e\}$ et $HK = G$.*

Démonstration. Les trois conditions sont évidemment nécessaires.

Pour montrer qu'elles sont suffisantes, il suffit en vertu du résultat précédent de montrer qu'elles assurent la condition (i). Soient donc $h \in H$ et $k \in K$. Considérons le *commutateur* $[h,k] = hkh^{-1}k^{-1}$ (qui est égal au neutre si et seulement si h et k commutent). Puisque $K \lhd G$, on a $hkh^{-1}k{-}1 = \underbrace{(hkh^{-1})}_{\in K}k^{-1} \in K$. De même, $H \lhd G$ assure $hkh^{-1}k{-}1 = h\underbrace{(kh^{-1}k^{-1})}_{\in H} \in H$. Ainsi $hkh^{-1}k^{-1} \in H \cap K = \{e\}$.

Alors la proposition précédente assure que G est le produit direct de ses sous-groupes H et K. □

2.3. **Produits semi-directs.**

2.3.1. *Motivation : point de vue description d'un groupe à partir de deux sous-groupes.* Supposons donnés un groupe G, et $N \lhd G$ un sous-groupe distingué. Supposons qu'il existe un sous-groupe H de G tel que $H \cap N = \{e\}$ et $NH = G$ (cf Proposition 2.2.5). Alors, l'application

$$\begin{array}{ccc} N \times H & \longrightarrow & G \\ (n,h) & \longmapsto & nh \end{array}$$

est une *bijection* du produit *ensembliste* $N \times H$ sur G (mais ce n'est pas en général un isomorphisme de groupes).

Cette bijection permet de munir l'ensemble $N \times H$ d'une nouvelle loi de groupe, déduite de celle de G : si on note $\mu\colon (n,h) \mapsto nh$ la bijection précédente, l'opération

$$(n,h) * (n',h') = \mu^{-1}(\mu(n,h)\mu(n',h')) = \mu^{-1}(nhn'h')$$

définit une loi de groupe sur l'ensemble $N \times H$ qui définit en général une structure de groupe différente de celle du groupe produit. On dit que cette multiplication est *tordue*.

On peut exprimer explicitement $\mu^{-1}(nhn'h')$ (et donc la loi $*$) en utilisant $N \lhd G$: en effet, $nhn'h' = n\underbrace{(hn'h^{-1})}_{\in N}hh'$ d'où on déduit

$$(n,h) * (n',h') = (nhn'h^{-1}, hh') = (n\varphi_h(n'), hh')$$

où $\varphi_h \colon n \in N \mapsto hnh^{-1}$ est la restriction à N de la conjugaison par h, bien définie car N distingué, qui est un automorphisme de groupes. Ainsi, la description précédente résulte du fait que, si N est distingué dans G, la conjugaison induit une opération par automorphismes de tout sous-groupe H sur N.

Cela conduit à la définition suivante :

Proposition-Définition 2.3.2 (Produit semi-direct)**.** *Soient N et H deux groupes. Soit $\varphi \colon H \to \mathrm{Aut}(N)$ un morphisme de groupes de H dans le groupe $\mathrm{Aut}(N)$ des automorphismes (de groupe) de N (autrement dit, une action de H sur N par automorphismes de groupe, donnée par $h \cdot n = \varphi_h(n)$, où $\varphi_h = \varphi(h)$).*

On définit sur l'ensemble produit $N \times H$ une loi de groupe par

$$(n,h) *_\varphi (n',h') = (n\varphi_h(n'), hh').$$

Le groupe $(N \times H, *_\varphi)$ est appelé produit semi-direct de N par H relativement à φ, *et est noté $N \rtimes_\varphi H$.*

Démonstration. C'est une vérification facile :

- élément neutre : l'élément neutre est (e_N, e_H), puisque $(e_N, e_H)*(n,h) = (\varphi_{e_H}(n), h) = (n,h)$ (en effet $\varphi_{e_H} = \mathrm{id}$) et $(n,h) * (e_N, e_H) = (n\varphi_h(e_H), h) = (n,h)$ (car φ_h automorphisme de groupe) ;
- inverse : l'inverse de (n,h) est $(\varphi_{h^{-1}}(n^{-1}), h^{-1})$: en effet, $(n,h)*(\varphi_{h^{-1}}(n^{-1}), h^{-1}) = (n\varphi_h(\varphi_{h^{-1}}(n^{-1})), hh^{-1}) = (nn^{-1}, e_H) = (e_N, e_H)$ car $\varphi_h \circ \varphi_{h^{-1}} = \varphi_{e_H} = \mathrm{id}_N$, et $(\varphi_{h^{-1}}(n^{-1}), h^{-1}) * (n,h) = (\varphi_{h^{-1}}(n^{-1})\varphi_{h^{-1}}(n), h^{-1}h)) = (\varphi_{h^{-1}}(n^{-1}n), e_H) = (e_N, e_H)$ car $\varphi_{h^{-1}}$ est un morphisme de groupe ;
- associativité : pour tous $(n,h), (n',h'), (n'',h'') \in N \times H$,

$$\begin{aligned}
(n,h) * \big((n',h') * (n'',h'')\big) &= (n,h) * (n'\varphi_{h'}(n''), h'h'') \\
&= (n\varphi_h(n'\varphi_{h'}(n'')), hh'h'') \\
&= (n\varphi_h(n')\varphi_{hh'}(n''), hh'h'') \\
&= (n\varphi_h(n'), hh') * (n'', h'') \\
&= \big((n,h) * (n',h')\big) * (n'',h'')
\end{aligned}$$

où on a utilisé plusieurs fois que $h \mapsto \varphi_h$ est un morphismes de groupes de H dans le groupe des automorphismes *de groupe* de N. □

Remarque 2.3.3. Si $\varphi \colon H \to \mathrm{Aut}(N)$ est le morphisme trivial, alors $N \rtimes_\varphi H$ est simplement le produit direct $N \times H$.

Remarque 2.3.4. Le produit semi-direct $G = N \rtimes_\varphi H$ contient deux sous-groupes isomorphes respectivement à N et H :

$$\overline{N} = \{(n, e_H), n \in N\} \text{ et } \overline{H} = \{(e_N, h), h \in H\}.$$

Le sous-groupe $\overline{N}$ est distingué dans $N \rtimes H$, mais en général $\overline{H}$ ne l'est pas. On a donc

$$\overline{N} \lhd N \rtimes_\varphi H$$

et la notation $N \rtimes H$ est faite pour rappeler que c'est (l'image de) N qui est distinguée dans le produit semi-direct.

On constate par ailleurs que $\overline{N} \cap \overline{H} = \{e\}$ et $\overline{N}\,\overline{H} = N \rtimes_\varphi H$.

L'action par conjugaison de $\overline{H}$ sur $\overline{N}$ permet de retrouver l'action de H sur N : si $h \in H$, φ_h est déterminé par $(e_N, h)(n, e_H)(e_N, h)^{-1} = (\varphi_h(n), e_H)$.

Enfin, les identifications naturelles de N et H à $\overline{N}$ et $\overline{H}$ identifient le produit semi-direct $N \rtimes_\varphi H$ au produit semi-direct $\overline{N} \rtimes_\psi \overline{H}$, où $\psi\colon \overline{H} \to \overline{N}$ est l'action par conjugaison de $\overline{H} \subset G$ sur le sous-groupe distingué $\overline{N}$: $\psi(\bar{h})(\bar{n}) = \bar{h}\bar{n}\bar{h}^{-1}$.

Le résultat suivant permet de reconnaître une situation de produit semi-direct :

Proposition 2.3.5 (Critère de décomposition en produit semi-direct de sous-groupes)**.** *Soit G un groupe. Soient N et H deux sous-groupes. Supposons que*

(i) $N \lhd G$,

(ii) $N \cap H = \{e\}$,

(iii) $G = NH$.

Alors, si $\varphi\colon H \to \mathrm{Aut}(N)$ désigne l'opération par conjugaison de H sur N, l'application

$$\begin{aligned} N \rtimes_\varphi H &\longrightarrow G \\ (n, h) &\longmapsto nh \end{aligned}$$

définit un isomorphisme de groupes

$$N \rtimes_\varphi H \xrightarrow{\sim} G.$$

On dit alors que G est le produit semi-direct interne de N par H*, ou tout simplement* le produit semi-direct des sous-groupes N et H*.*

Remarque 2.3.6. On peut remplacer l'hypothèse (iii) par : N et H engendrent G. Rappelons que le sous-groupe $\langle A \rangle$ engendré par une partie $A \subset G$ est le plus petit sous-groupe de G contenant A : comme d'habitude, on peut vérifier son existence en notant que c'est

$$\langle A \rangle = \bigcap_{K \text{ sous-groupe}, K \supset A} K,$$

qui est un sous-groupe car l'intersection de sous-groupes est un sous-groupe.

Par ailleurs, on vérifie sans peine que

$$\{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_r^{\varepsilon_r}, r \in \mathbf{N}, a_i \in A, \varepsilon_i = \pm 1\}$$

est un sous-groupe qui contient A, et que tout sous-groupe contenant A doit le contenir : c'est donc $\langle A \rangle$.

Si $\langle A \rangle = G$ on dit que A engendre G.

Montrons que, sous l'hypothèse $N \lhd G$, $G = NH$ si et seulement si $G = \langle N, H \rangle$ (on note $\langle N, H \rangle = \langle N \cup H \rangle$ le sous-groupe engendré par N et H). Il est clair (sans hypothèse sur N) que, si $G = NH$, alors N et H engendrent G. Réciproquement, constatons $\langle N, H \rangle = \{n_1^{a_1} h_1^{b_1} n_2^{a_2} h_2^{b_2} \cdots n_r^{a_r} h_r^{b_r}, r \in \mathbf{N}, n_i \in N, h_i \in H, a_i, b_i \in \{0, 1\}\}$. En utilisant que $hN = Nh$ pour tout $h \in H$, on vérifie que ce sous-groupe est inclus dans NH.

Par ailleurs, lorsque G est *fini*, on peut remplacer la condition (iii) par $|N||H| = |G|$ (ou (ii) par $|N||H| = |G|$).

Démonstation de 2.3.5. C'est une vérification facile :

— l'application $\mu\colon (n, h) \in N \rtimes_\varphi H \to G$ est un morphisme de groupes, puisque $\mu(n, h)\mu(n', h') = nhn'h'$ et $\mu((n, h)(n', h')) = \mu(n\varphi_h(n'), hh') = \mu(nhn'h^{-1}, hh') = nhn'h'$ coïncident ;

— soit $(n,h) \in \ker \mu$. Alors $nh = e_G$, d'où $n = h^{-1} \in N \cap H = \{e\}$. Donc $\ker \mu$ est trivial, et μ est injectif ;
— l'image de μ est exactement $NH = G$.

□

Remarque 2.3.7. Soient N et H deux groupes donnés. On peut caractériser les produits directs parmi les produits semi-directs de N par H relativement aux différents morphismes $\varphi\colon H \to \mathrm{Aut}(N)$: en effet, le produit est direct (au sens où la loi de groupe sur l'ensemble $N \times H$ est celle du produit direct) si et seulement si φ est le morphisme trivial, ou encore si et seulement si le sous-groupe $\overline{H} = \{(e_N, h), h \in H\}$ est distingué dans $N \rtimes_\varphi H$.

Remarque 2.3.8. Un produit direct peut être isomorphe à un produit semi-direct non trivial ! On a par exemple un isomorphisme

$$S_3 \times \mathbf{Z}/2\mathbf{Z} \simeq S_3 \rtimes \mathbf{Z}/2\mathbf{Z}$$

entre le produit direct et un produit semi-direct non trivial de S_3 par $\mathbf{Z}/2\mathbf{Z}$ (en effet, le produit direct $S_3 \times \mathbf{Z}/2\mathbf{Z}$ est produit semi-direct de ses sous-groupes $\overline{S_3} = \{(\sigma, 0), \sigma \in S_3\}$ et $\langle((12), 1)\rangle$, et ce produit n'est pas égal au produit direct puisque le sous-groupe à deux éléments $\langle((12), 1)\rangle$ n'est pas distingué).

Ce n'est en aucun cas en contradiction avec la remarque précédente !

Définition 2.3.9 (Section)**.** On appelle *section* d'un morphisme surjectif $p\colon G \to H$ tout morphisme de groupe $s\colon H \to G$ tel que $p \circ s = \mathrm{id}_H$. Lorsque dans une suite exacte $1 \to N \to G \xrightarrow{p} H \to 1$ la projection p admet une section, on dit que la suite exacte est *scindée*, ce qu'on représente ainsi :

$$1 \longrightarrow N \xrightarrow{i} G \underset{p}{\overset{s}{\rightleftarrows}} H \longrightarrow 1.$$

Remarque 2.3.10. L'existence d'une section pour une suite exacte $1 \to N \to G \xrightarrow{p} H \to 1$ équivaut à l'existence d'un sous-groupe H' tel que la restriction $p_{|H'}$ de p à H' induise un isomorphisme de H' sur H. On dit qu'une tel sous-groupe H' est un *relèvement* de H.

Soient N et H deux groupes, et $\varphi\colon H \to \mathrm{Aut}(N)$ un morphisme de groupes. Le produit semi-direct $N \rtimes_\varphi H$ s'insère dans une suite exacte scindée

$$1 \longrightarrow N \longrightarrow N \rtimes_\varphi H \underset{}{\overset{s}{\rightleftarrows}} H \longrightarrow 1$$

le relèvement du quotient H étant fourni par le sous-groupe $\overline{H} = \{(e_N, h), h \in H\}$. Réciproquement on a un critère pour qu'une extension soit produit semi-direct :

Proposition 2.3.11. *Si une suite exacte*

$$1 \longrightarrow N \longrightarrow G \underset{}{\overset{}{\rightleftarrows}} H \longrightarrow 1$$

est scindée, alors G est isomorphe à un produit semi-direct $N \rtimes_\varphi H$.

Démonstration. Soit $\overline{H}$ le relèvement de H associé à la section s de la projection $p\colon G \to H$. La restriction à $\overline{H}$ de p définit un isomorphisme $q\colon \overline{H} \to H$. De même, l'inclusion $i\colon N \to G$ induit un isomorphisme $j\colon N \to \overline{N}$ de N sur son image.

Soit $\varphi\colon H \to \mathrm{Aut}\, N$ le morphisme induit par ces isomorphismes et la conjugaison de $\overline{H}$ sur $\overline{N}$. On vérifie (voir discussions précédentes) que G est isomorphe au produit semi-direct $N \rtimes_\varphi H$. □

3. Groupes abéliens finis

On étudie dans cette section les groupes abéliens finis, qui seront notés additivement.

Les produits de groupes finis cycliques sont évidemment des groupes abéliens finis. Nous allons voir que réciproquement tout groupe abélien fini est isomorphe à un produit de groupes cycliques (ou plus précisément produit de sous-groupes cycliques). Néanmoins, le lemme chinois montre qu'une telle décomposition ne peut être unique.

3.1. **Décomposition en composantes primaires.**

On appelle *groupe p-primaire* un p-groupe abélien (p étant un nombre premier). On dit qu'un groupe G est un groupe primaire s'il existe un premier p tel que G est p-primaire.

Dans un groupe abélien fini G, on appelle *composante p-primaire* l'ensemble G_p des éléments dont l'ordre est une puissance de p : $G_p = \{x \in G, \exists m \in \mathbf{N}, p^m x = 0\}$. C'est un sous-groupe. Plus précisément :

Lemme 3.1.1. *Soit G un groupe abélien fini. Pour tout premier p, la composante p-primaire de G est l'unique p-Sylow de G.*

Démonstration. Les théorèmes de Sylow assurent qu'il existe un unique sous-groupe de Sylow S_p : en effet, le groupe G étant abélien, tout sous-groupe est distingué. De plus, tout élément de S_p est d'ordre une puissance de p, donc $S_p \subset G_p$.

Par ailleurs, tout élément x d'ordre une puissance de p est contenu dans S_p : en effet, le sous-groupe $\langle x \rangle$ est un p-groupe, donc contenu dans le p-Sylow S_p. Ainsi $G_p \subset S_p$. □

Si G est d'ordre $n = p_1^{r_1} \cdots p_s^{r_s}$ (où les p_i sont des premiers deux à deux distincts) on a donc pour tout i une composante p_i-primaire G_{p_i} d'ordre $p_i^{r_i}$. Le groupe G est égal au produit direct de ces sous-groupes :

Théorème 3.1.2 (Décomposition en composantes p-primaires d'un groupe abélien fini)**.** *Soit G un groupe abélien fini. Alors G est isomorphe à un produit de groupes p-primaires.*

Plus précisément, si $|G| = p_1^{r_1} \cdots p_s^{r_s}$ (avec $p_1, \ldots, p_s$ diviseurs premiers deux à deux distincts), alors G est égal au produit de ses sous-groupes de Sylow, qui sont ses composantes p-primaires :

$$G_{p_1} \times \cdots \times G_{p_s} \xrightarrow{\sim} G.$$

Démonstration. Soit donc G_{p_i} le p_i-Sylow de G. Montrons que

$$\begin{array}{ccc} G_{p_1} \times \cdots \times G_{p_s} & \longrightarrow & G \\ (g_1, \ldots, g_s) & \longmapsto & g_1 + \cdots + g_s \end{array}$$

est un isomorphisme de groupes, ce qu'on note souvent $G = G_{p_1} \oplus \cdots \oplus G_{p_s}$.

Cela résulte du résultat suivant :

Soit G un groupe abélien d'ordre mn avec m et n premiers entre eux. Si $H = \{x \in G, mx = 0\}$ et $K = \{x \in G, nx = 0\}$, alors $(x, y) \in H \times K \mapsto x + y \in G$ est un isomorphisme.

En effet, d'après le théorème de Bézout il existe des entiers u et v tels que $um + vn = 1$, de sorte que $x \in H \cap K$ vérifie $x = (um + vn)x = 0$. De plus, tout $x \in G$ comme $x = (vn + um)x = \underbrace{vnx}_{\in H} + \underbrace{umx}_{\in K}$, de sorte que $G = H + K$. Puisque tous les éléments commutent, on reconnaît un produit direct : l'application $(x, y) \in H \times K \mapsto x + y$ est un isomorphisme de $H \times K$ sur G. □

3.2. **Décomposition en produits de sous-groupes cycliques.** Nous donnons ici un théorème de structure des groupes abéliens finis :

Tout groupe abélien fini G est produit de sous-groupes cycliques non nuls $H_1, \dots, H_s$ d'ordres d_i vérifiant $d_s|d_{s-1}|\cdots|d_2|d_1$. De plus, les entiers $d_1, \dots, d_s$ sont uniques, et sont appelés *diviseurs élémentaires* ou *facteurs invariants*. En revanche, les sous-groupes H_i ne sont pas du tout uniques (voir $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$).

C'est un cas particulier d'un résultat beaucoup plus général concernant la structure des modules de type fini sur un anneau principal. Nous en donnons ici une démonstration courte.

Lemme 3.2.1. *Soit G abélien fini. Soit x un élément d'ordre* maximal*, $C = \langle x \rangle$. Alors tout élément de G/C peut se relever en un élément de G de même ordre.*

Démonstration. Soit $\bar{y} \in G/C$ l'image par $p\colon G \to G/C$ d'un élément $y \in G$. L'ordre de tout relevé de $\bar{y}$ est divisible par l'ordre $o(\bar{y})$, et il s'agit donc de trouver un relevé y' de $\bar{y}$ dont l'ordre divise $o(\bar{y})$.

Supposons d'abord que G est un p-groupe. Écrivons $o(x) = p^r$ et $o(\bar{y}) = p^s$, avec $s \leqslant r$. Si y relève $\bar{y}$, on a $p^s y \in C = \langle x \rangle$, i.e. $p^s y = kx$ pour $k \in \mathbf{N}$. Écrivons $k = p^l m$ avec m premier à p. Alors $o(kx) = o(mp^l x) = p^{r-l}$. Donc $p^s y = kx$ est d'ordre p^{r-l}, et y est donc d'ordre p^{r-l+s}. Puisque p^r est l'ordre maximal d'un élément de G, on a $l \geqslant s$.

Alors $p^s y = kx = p^l m x$ entraîne $p^s(y - p^{l-s} m x) = 0$. Ainsi $y' = y - p^{l-s} m x$ s'envoie sur $\bar{y}$ dans G/C, et son ordre divise $p^s = o(\bar{y})$.

Dans le cas d'un groupe abélien fini de cardinal quelconque $n = p_1^{r_1} \cdots p_s^{r_s}$, considérons la décomposition de G en composantes primaires $G = G_{p_1} \oplus \cdots \oplus G_{p_s}$. Alors $x = (x_1, \dots, x_s)$ et $C = \langle x_1 \rangle \oplus \cdots \oplus \langle x_s \rangle$ (car les p_i sont des premiers deux à deux distincts !). On en déduit un isomorphisme entre G/C et $\prod_i G_{p_i}/\langle x_i \rangle$., ce qui permet d'écrire $\bar{y} = (\bar{y_1}, \dots, \bar{y_s})$ avec $\bar{y_i} \in G_{p_i}/\langle x_i \rangle$.

Les ordres des G_{p_i} étant deux à deux premiers entre eux, l'ordre d'un élément $(z_1, \dots, z_s)$ est le produit des ordres des z_i. Ainsi, chaque x_i est d'ordre maximal dans G_{p_i}, et le cas des p-groupes abéliens assure que pour tout i il existe un relèvement $y_i \in G_{p_i}$ de $\bar{y}_i$ de même ordre. Alors $y = (y_1, \dots, y_s)$ est un relèvement de $\bar{y}$ d'ordre $\prod_i o(y_i) = \prod_i o(\bar{y}_i) = o(\bar{y})$. □

Théorème 3.2.2 (Théorème de structure des groupes abéliens finis)**.** *Soit G un groupe abélien fini. Il existe alors un entier $s \in \mathbf{N}$, des entiers $d_i \geqslant 2$ vérifiant $d_s|d_{s-1}|\cdots|d_2|d_1$ et un isomorphisme de groupes*

$$G \simeq \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z}.$$

Plus précisément, G se décompose en produit de sous-groupes cycliques non nuls d'ordres $d_s|d_{s-1}|\cdots|d_2|d_1$.

De plus les entiers s et $d_1, \dots, d_s$ sont uniquement déterminés.

Démonstration.

Existence : démontrons l'existence par récurrence sur l'ordre du groupe.

Soit G un groupe abélien fini non nul, et x_1 un élément d'ordre maximal d_1. Rappelons que l'ordre de tout élément divise alors d_1 : en effet [4], soit y un élément d'ordre m. Si p premier, écrivons $d_1 = p^r k$ et $m = p^s l$, avec k et l premiers à p. Il suffit de

4. Rappelons au passage qu'on appelle *exposant du groupe G* le plus petit entier e tel que $g^e = 1$ pour tout $g \in G$. On a ainsi,

Proposition. *L'exposant d'un groupe abélien fini est le plus grand des ordres de ses éléments.*

Autrement dit, dans un groupe abélien fini, l'exposant est atteint.

remarquer que $p^r x_1$ est d'ordre k et ly d'ordre p^s. Le produit de ces deux éléments d'ordres premiers entre eux est d'ordre kp^s, inférieur à $d_1 = kp^r$. On a donc $s \leqslant r$. On a ainsi montré que, pour tout premier p, $p^s | o(y) \Rightarrow p^s | d_1$, ce qui signifie exactement que l'ordre de y divise d_1.

Si $G = \langle x_1 \rangle$ l'existence est établie. Sinon, par récurrence, le groupe quotient $G/\langle x_1 \rangle$ se décompose en produit de sous-groupes cycliques $\langle \bar{x}_2 \rangle \times \cdots \times \langle \bar{x}_s \rangle$ où les $\bar{x}_i$ sont d'ordres $d_s | \cdots | d_2$. D'après le lemme, on peut relever tout $\bar{x}_i$ en $x_i \in G$ d'ordre d_i. En particulier, on a $d_2 | d_1$.

Vérifions alors que le morphisme

$$\langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \langle x_s \rangle \longrightarrow G$$

défini par $(y_1, \ldots, y_s) \longmapsto y_1 + \cdots + y_s$ est un isomorphisme de groupes. La surjectivité est immédiate. Soient donc $k_1, \ldots, k_s \in \mathbf{N}$ tels que $k_1 x_1 + k_2 x_2 + \cdots + k_s x_s = 0$. En projetant dans $G/\langle x_1 \rangle$ on obtient $k_2 \bar{x}_2 + \cdots + k_s \bar{x}_s = 0$, ce qui signifie que, pour tout $i \geqslant 2$, $d_i | k_i$. On a donc $k_i x_i = 0$ pour tout $i \geqslant 2$, puis $k_1 x_1 = -k_2 x_2 - \cdots - k_s x_s = 0$. Le morphisme précédent établit donc bien un isomorphisme entre G et un produit de sous-groupes cycliques dont les ordres vérifient la condition attendue.

Unicité des d_i : soient s, $s' \in \mathbf{N}$, $d_s | d_{s-1} | \cdots d_1$ et $d'_{s'} | \cdots | d'_1$ tels qu'il existe un isomorphisme

$$\mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z} \simeq \mathbf{Z}/d'_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d'_{s'}\mathbf{Z}.$$

Soit $i_0 \geqslant 1$. Supposons que pour tout $i \leqslant i_0 - 1$, $d_i = d'_i$.

Considérons le morphisme $\psi \colon x \mapsto d_{i_0} x = \underbrace{x + \cdots + x}_{d_{i_0} \text{ fois}}$ de multiplication par d_{i_0}, et particulièrement son image. Ce morphisme agit sur les produits directs facteur par facteur. Remarquons [5] que l'image $\psi_n(\mathbf{Z}/n\mathbf{Z})$ de $\psi_n \colon x \in \mathbf{Z}/n\mathbf{Z} \mapsto d_{i_0} x \in \mathbf{Z}/n\mathbf{Z}$ est nulle si et seulement si n divise d_{i_0}.

L'image de $\mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z}$ par la multiplication par d_{i_0} est donc

$$\psi_{d_1}(\mathbf{Z}/d_1\mathbf{Z}) \times \cdots \times \psi_{d_{i_0-1}}(\mathbf{Z}/d_{i_0-1}\mathbf{Z}) \times \{0\} \times \cdots \times \{0\}.$$

Celle de $\mathbf{Z}/d'_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d'_{s'}\mathbf{Z}$ est

$$\psi_{d'_1}(\mathbf{Z}/d'_1\mathbf{Z}) \times \cdots \times \psi_{d'_{i_0-1}}(\mathbf{Z}/d'_{i_0-1}\mathbf{Z}) \times \psi_{d'_{i_0}}(\mathbf{Z}/d'_{i_0}\mathbf{Z}) \times \cdots \times \psi_{d'_{s'}}(\mathbf{Z}/d'_{s'}\mathbf{Z}).$$

Puisque $d'_i = d_i$ pour $i \leqslant i_0 - 1$, les $i_0 - 1$ premiers facteurs sont isomorphes. Et en considérant les cardinalités, on obtient que l'image $\psi_{d'_{i_0}}(\mathbf{Z}/d'_{i_0}\mathbf{Z})$ de la multiplication $\mathbf{Z}/d'_{i_0}\mathbf{Z} \to \mathbf{Z}/d'_{i_0}\mathbf{Z}, x \mapsto d_{i_0} x$ est nulle. Autrement dit, d'_{i_0} divise d_{i_0}.

En considérant la multiplication par d'_{i_0}, on obtient de même $d_{i_0} | d'_{i_0}$.

Finalement, $d_{i_0} = d'_{i_0}$.

On en déduit l'unicité de la famille $d_1, \ldots, d_s$. □

Ce théorème a une conséquence importante :

Corollaire 3.2.3. *Deux groupes abéliens finis sont isomorphes si et seulement si ils ont les mêmes diviseurs élémentaires.*

5. En fait, l'image de la multiplication $x \in \mathbf{Z}/n\mathbf{Z} \mapsto dx \in \mathbf{Z}/n\mathbf{Z}$ est $(d,n)\mathbf{Z}/n\mathbf{Z}$ (i.e. le sous-groupe engendré par (n,d), et est de cardinal $\frac{n}{(n,d)}$: en effet, l'image réciproque par la projection canonique $\pi \colon \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ de l'image de la multiplication par d est $d\mathbf{Z} + n\mathbf{Z} = (d,n)\mathbf{Z}$. Cela nous permettrait d'écrire les images par la multiplication par d_{i_0} de $\mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z}$ et $\mathbf{Z}/d'_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d'_{s'}\mathbf{Z}$ comme

$$(d_{i_0}\mathbf{Z}/d_1\mathbf{Z}) \times \cdots \times (d_{i_0}\mathbf{Z}/d_{i_0-1}\mathbf{Z}) \times \{0\} \times \cdots \times \{0\}$$

et

$$(d_{i_0}\mathbf{Z}/d'_1\mathbf{Z}) \times \cdots \times (d_{i_0}\mathbf{Z}/d'_{i_0-1}\mathbf{Z}) \times ((d_{i_0}, d'_{i_0})\mathbf{Z}/d'_{i_0}\mathbf{Z}) \times \cdots \times ((d_{i_0}, d'_{s'})\mathbf{Z}/d'_{s'}\mathbf{Z}),$$

d'où on conclurait que $(d_{i_0}, d'_{i_0})\mathbf{Z}/d'_{i_0}\mathbf{Z}$ est trivial, i.e. $d'_{i_0} | d_{i_0}$.

Remarque 3.2.4. Ce corollaire permet de compter les classes d'isomorphismes de groupes abéliens d'ordre n donné.

Citons enfin pour terminer la décomposition en groupes cycliques primaires, qui résulte par exemple de la précédente à l'aide du lemme chinois, ou de la décomposition en composantes primaires et du théorème précédent :

Théorème 3.2.5. *Tout groupe abélien fini G est isomorphe à un produit de groupes cycliques primaires*

$$\left(\mathbf{Z}/p_1^{r_{11}}\mathbf{Z}\times\cdots\times\mathbf{Z}/p_1^{r_{1n_1}}\mathbf{Z}\right)\times\cdots\times\left(\mathbf{Z}/p_s^{r_{s1}}\mathbf{Z}\times\cdots\times\mathbf{Z}/p_s^{r_{sn_s}}\mathbf{Z}\right)$$

où $p_1,\ldots,p_s$ sont les diviseurs premiers de $|G|$ et, pour tout i, $r_{i1}\geqslant r_{i2}\geqslant\cdots\geqslant r_{in_i}$.

3.3. **Structure du groupe $(\mathbf{Z}/n\mathbf{Z})^\times$.**

L'étude de la structure du groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ des éléments inversibles dans l'anneau $\mathbf{Z}/n\mathbf{Z}$ est primordiale.

Rappelons que, pour tout entier relatif k, les propriétés suivantes sont équivalentes :
— k et n sont premiers entre eux.
— la classe $\bar{k}$ de k dans $\mathbf{Z}/n\mathbf{Z}$ définit un élément inversible,
— $\bar{k}$ engendre le groupe $(\mathbf{Z}/n\mathbf{Z},+)$.

On appelle *indicatrice d'Euler* ou *fonction d'Euler* comme la fonction $\varphi\colon\mathbf{N}^*\to\mathbf{N}$, $\varphi(n)=\mathrm{card}((\mathbf{Z}/n\mathbf{Z})^\times)=\mathrm{card}\{x|1\leqslant x\leqslant n,(n,x)=1\}$. On a, pour p premier et $\alpha\in\mathbf{N}^*$, $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$.

L'importance particulière de la compréhension du groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ vient du résultat suivant :

Proposition 3.3.1. *Le groupe des automorphismes de groupe de $\mathbf{Z}/n\mathbf{Z}$ (et donc, plus généralement, de tout groupe cyclique d'ordre n) est isomorphe à $(\mathbf{Z}/n\mathbf{Z})^\times$:*

$$\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})\xrightarrow{\sim}(\mathbf{Z}/n\mathbf{Z})^\times.$$

En particulier, $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$ est un groupe abélien, de cardinal $\varphi(n)$.

Démonstration. Si $u\in\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$, alors $u(\bar{1})$ est un générateur de $\mathbf{Z}/n\mathbf{Z}$ (en effet, u étant surjectif, tout élément de $\mathbf{Z}/n\mathbf{Z}$ est égal à $u(\bar{k})$ pour un entier $k\in\mathbf{N}$, et $u(\bar{k})=u(k\bar{1})=ku(\bar{1})$), donc appartient à $(\mathbf{Z}/n\mathbf{Z})^\times$. On obtient ainsi une application $\tau\colon u\mapsto u(\bar{1})$ de $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$ dans $(\mathbf{Z}/n\mathbf{Z})^\times$. C'est un morphisme de groupes : en effet, si $u(\bar{1})=\bar{k}$ avec $k\in\mathbf{N}$, alors $v\circ u(\bar{1})=v(\bar{k})=v(k\bar{1})=kv(\bar{1})=\bar{k}v(\bar{1})=u(\bar{(1)})v(\bar{(1)})$.

Inversement, si $s\in(\mathbf{Z}/n\mathbf{Z})^\times$, $x\mapsto sx$ définit un morphisme de groupe $\sigma(s)$ de $\mathbf{Z}/n\mathbf{Z}$ dans lui-même, qui est un isomorphisme, de réciproque $\sigma(s^{-1})$. On définit ainsi un morphisme $\sigma\colon s\mapsto\sigma(s)$ de $(\mathbf{Z}/n\mathbf{Z})^\times$ dans $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$, et on vérifie que les morphismes σ et τ sont réciproques l'un de l'autre. □

Remarque 3.3.2. Ainsi, la description de $(\mathbf{Z}/n\mathbf{Z})^\times$ intervient-elle naturellement lorsque l'on cherche à écrire un groupe comme produit semi-direct : si on identifie dans un groupe G un sous-groupe distingué cyclique $\langle x_n\rangle$ d'ordre n et un sous-groupe H d'indice n tels que $\langle x_n\rangle\cap H$ soit trivial, alors G est produit semi-direct de $\langle x_n\rangle$ et H, et ce produit semi-direct est donné par un morphisme $H\to\mathrm{Aut}(\langle x_n\rangle)$. D'après la proposition précédente, comprendre quels groupes on peut ainsi obtenir se ramène à déterminer les morphismes $H\to(\mathbf{Z}/n\mathbf{Z})^\times$.

Décrivons donc ce groupe $(\mathbf{Z}/n\mathbf{Z})^\times$. Remarquons que, si $(m,n)=1$, l'isomorphisme (de groupes) $\mathbf{Z}/(mn)\mathbf{Z}\xrightarrow{\sim}\mathbf{Z}/m\mathbf{Z}\times\mathbf{Z}/n\mathbf{Z}$ est un isomorphisme d'anneaux. On déduit alors de l'isomorphisme de groupes $(A\times B)^\times\simeq A^\times\times B^\times$ pour tous anneaux A et B le résultat suivant :

Proposition 3.3.3. *Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec p_i premiers deux à deux distincts et $\alpha_i \in \mathbf{N}^*$, on a un isomorphisme de groupes*

$$(\mathbf{Z}/n\mathbf{Z})^\times \simeq \prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times.$$

En particulier, $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$.

Cette proposition ramène l'étude de $(\mathbf{Z}/n\mathbf{Z})^\times$ à celle de $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$, p premier.
Le point de départ est le cas $\alpha = 1$, fondamental.

Théorème 3.3.4. *Soit p un nombre premier. Alors le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique :*

$$(\mathbf{Z}/p\mathbf{Z})^\times \simeq \mathbf{Z}/(p-1)\mathbf{Z}.$$

Démonstration. Nous donnerons trois démonstrations (ou plutôt deux, avec deux variantes de la seconde) de ce résultat important. On démontre de la même manière que tout sous-groupe *fini* du groupe multiplicatif K^* d'un corps commutatif K est cyclique. Tous ces arguments reposent sur le fait qu'un polynôme de degré $d > 0$ à coefficients dans un corps commutatif possède au plus d racines.
Argument classique : on utilise la relation $n = \sum_{d|n} \varphi(d)$ (que l'on obtient en décomposant $\mathbf{Z}/n\mathbf{Z}$ en ses sous-ensembles d'éléments d'ordre d, pour $d|n$: en effet, il y a exactement $\varphi(d)$ éléments d'ordre d, qui sont exactement les générateurs de l'unique sous-groupe d'ordre d). Soit $N(d)$ le nombre d'éléments d'ordre $d \in \mathbf{N}^*$ dans $(\mathbf{Z}/p\mathbf{Z})^\times$ (ou dans un sous-groupe fini G de groupe multiplicatif K^* d'un corps commutatif K).

Soit $d \in \mathbf{N}^*$ tel que $N(d) > 0$. Il existe alors un élément x d'ordre d, et le sous-groupe cyclique $H_x = \langle x \rangle$ engendré par x contient exactement d éléments, qui vérifient tous $y^d = 1$. Mais le polynôme $Y^d - 1$ a au plus d racines dans le corps $\mathbf{Z}/p\mathbf{Z}$. Tous les éléments d'ordre d de $\mathbf{Z}/p\mathbf{Z}$ sont donc dans H_x, qui en contient exactement $\varphi(d)$. Ainsi, $N(d)$ est égal à 0 ou à $\varphi(d)$.

Puisque tout élément a un ordre qui est nécessairement un diviseur de $p-1$, on a $p - 1 = \sum_{d|n} N(d)$. Avec $p - 1 = \sum_{d|n} \varphi(d)$ et $N(d) \leqslant \varphi(d)$ pour tout d, on obtient $N(d) = \varphi(d)$ pour tout $d|n$. En particulier, $N(p-1) = \varphi(p-1) > 0$, donc $(\mathbf{Z}/p\mathbf{Z})^\times$ contient un élément d'ordre $p-1$, donc est cyclique.
Avec le théorème de structure des groupes abéliens finis : comme groupe abélien fini, $(\mathbf{Z}/n\mathbf{Z})^\times$ est isomorphe à un produit de groupe cyclique $\mathbf{Z}/d_1\mathbf{Z} \times \mathbf{Z}/d_2\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z}$ avec $d_s | \cdots | d_1$. Alors tous les éléments sont d'ordre divisant d_1, i.e. vérifient $x^{d_1} = 1$. Mais $X^{d_1} - 1$ a au plus d_1 racines dans le corps $\mathbf{Z}/p\mathbf{Z}$. Il n'y a donc qu'un seul facteur : $(\mathbf{Z}/n\mathbf{Z})^\times \simeq \mathbf{Z}/d_1\mathbf{Z}$.
Avec le lemme sur l'exposant d'un groupe abélien fini : on a vu que, dans un groupe abélien fini, si x est un élément d'ordre d maximal, alors l'ordre de tout élément divise d. Soit donc $x \in (\mathbf{Z}/p\mathbf{Z})^\times$ un élément d'ordre maximal d. Tous les éléments y vérifient alors $y^d = 1$. Mais $Y^d - 1$ a au plus d racines dans le corps $\mathbf{Z}/p\mathbf{Z}$. Ainsi $p - 1 \leqslant d | p - 1$. Donc $d = p - 1$, et $(\mathbf{Z}/p\mathbf{Z})^\times$ est engendré par x. □

Il faut ensuite distinguer les cas p impair et $p = 2$. Commençons par le cas impair.

Théorème 3.3.5. *Soient p premier impair, $\alpha \in \mathbf{N}^*$. Alors $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ est cyclique :*

$$(\mathbf{Z}/p^\alpha\mathbf{Z})^\times \simeq \mathbf{Z}/p^{\alpha-1}(p-1)\mathbf{Z}.$$

Démonstration. Supposons $\alpha \geqslant 2$ (le cas $\alpha = 1$ est exactement le théorème précédent). Le principe de la preuve est le suivant : la projection canonique $\mathbf{Z}/p^\alpha\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ induit un morphisme de groupes surjectif (vu la description des inversibles de ces deux anneaux)

$$(\mathbf{Z}/p^\alpha\mathbf{Z})^\times \longrightarrow (\mathbf{Z}/p\mathbf{Z})^\times.$$

D'après le théorème précédent, le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ admet un générateur, qu'on cherche à relever en un générateur de $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$. Soit $x \in (\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ un relèvement d'un générateur de $(\mathbf{Z}/p\mathbf{Z})^\times$. L'ordre de x est alors un multiple de $p-1$, donc égal à $m(p-1)$, et $y = x^m$ est alors d'ordre $p-1$.

Par ailleurs, le lemme ci-dessous montre que $(1+p)$ est d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ (en effet, on a d'une part $(1+p)^{p^{\alpha-1}} \equiv 1 + p^\alpha \mod p^{\alpha+1} \equiv 1 \mod p^\alpha$, et d'autre part $(1+p)^{p^{\alpha-2}} \equiv 1 + p^{\alpha-1} \mod p^\alpha \not\equiv 1 \mod p^\alpha$). Puisque les ordres $p-1$ et $p^{\alpha-1}$ de y et $1+p$ sont premiers entre eux (et que ces éléments commutent), le produit $y(1+p)$ est d'ordre [6] $(p-1)p^\alpha - 1$, i.e. engendre $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$. □

Lemme 3.3.6. *Soit p premier impair. Pour tout $k \in \mathbf{N}$, $(1+p)^{p^k} \equiv 1+p^{k+1} \mod p^{k+2}$.*

Démonstration. Montrons-le par récurrence sur k. Pour $k = 0$, la congruence est triviale. Soit donc $k \geqslant 1$ et supposons $(1+p)^{p^{k-1}} = 1 + p^k + ap^{k+1}$. On a $(1+p)^{p^{k+1}} = (1 + (p^k + ap^{k+1}))^p = 1 + p(p^k + ap^{k+1}) + \sum_{i=2}^{p} \binom{p}{i}(p^k + ap^{k+1})^i$. Comme $p|\binom{p}{i}$ pour $1 \leqslant i \leqslant p-1$, on a $p^{k+2}|\binom{p}{i}(p^k + ap^{k+1})^i = \binom{p}{i}p^{ki}(1+ap)^i$ pour $2 \leqslant i \leqslant p-1$, d'où $(1+p)^{p^{k+1}} \equiv 1 + p^{k+1} + p^{pk}(1+ap)^p \mod p^{k+2}$. Comme $p \geqslant 3$, $pk \geqslant k+2$, et $(1+p)^{p^{k+1}} \equiv 1 + p^{k+1} \mod p^{k+2}$. □

Reste à traiter le cas $p = 2$.

Théorème 3.3.7. *On a $(\mathbf{Z}/2\mathbf{Z})^\times = \{1\}$, $(\mathbf{Z}/4\mathbf{Z})^\times = \{\pm 1\} \simeq \mathbf{Z}/2\mathbf{Z}$, et, pour $\alpha \geqslant 3$, $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$.*

Démonstration. Supposons $\alpha \geqslant 3$ (les cas $\alpha = 1$ et $\alpha = 2$ sont immédiats). On considère le morphisme surjectif $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times \to (\mathbf{Z}/4\mathbf{Z})^\times = \{1, -1\} \simeq \mathbf{Z}/2\mathbf{Z}$.

Son noyau contient (la classe de) 5 et est d'ordre $2^{\alpha-2}$. Montrons que 5 est d'ordre $2^{\alpha-2}$.

Pour ce faire, montrons par récurrence sur k que $5^{2^k} = 1 + a2^{k+2}$ avec a impair. C'est trivial pour $k = 0$. Supposons, pour $k \geqslant 1$, $5^{2^{k-1}} = 1 + a2^{k+1}$ avec a impair. Alors $5^{2^k} = (1 + a2^{k+1})^2 = 1 + a2^{k+2} + a^2 2^{2k+2} = 1 + (a + a^2 2^k)2^{2k+2}$. Ce qui prouve l'égalité annoncée. On a alors $5^{2^{\alpha-2}} = 1 + a2^\alpha \equiv 1 \mod 2^\alpha$ et $5^{2^{\alpha-3}} = 1 + b2^{\alpha-1} \equiv 1 + 2^{\alpha-1} \mod 2^\alpha \not\equiv 1 \mod 2^\alpha$.

Ainsi le noyau de $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times \to (\mathbf{Z}/4\mathbf{Z})^\times = \{1, -1\} \simeq \mathbf{Z}/2\mathbf{Z}$ est cyclique, engendré par 5. Par ailleurs, la classe de -1 s'envoie sur -1 et est d'ordre 2. On reconnaît un produit direct : $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$ est produit direct de ses sous-groupes $\langle\bar{5}\rangle \simeq \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$ et $\langle\bar{-1}\rangle \simeq \mathbf{Z}/2\mathbf{Z}$. □

Remarque 3.3.8. Les résultats précédents montrent que le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique si et seulement si $n = 2$, 4, p^α, ou $2p^\alpha$, avec p premier impair. En effet, dans tous les autres cas, il contient au moins trois éléments d'ordre 2, alors qu'un groupe cyclique en contient exactement un.

---

6. En effet, si a et b commutent et sont d'ordres m et n premiers entre eux, alors ab est d'ordre mn : puisque $(ab)^m n = a^{mn}b^{mn} = e$, l'ordre de ab divise mn. Par ailleurs, si $(ab)^k = e$ alors, en élevant à la puissance n on a $e = a^{kn}b^{kn} = a^{kn}$, d'où $m|kn$ puis, puisque $(m,n) = 1$, $m|k$. En élevant à la puissance m on obtient de même $n|k$, d'où, en utilisant encore $(m,n) = 1$, $mn|k$. Ainsi mn est l'ordre de ab.