Université de Lille

Mémoire de Master 1 mathématiques,
parcours Recherche et Agrégation.

Groupes finis comme unions de sous-groupes propres

Cassian DUPONT-ROZÉ

Sous la direction de Olivier Serman

Université de Lille. Département de Mathématiques.

Année académique 2023-2024

Dernière modification : 27 mai 2024.

Sommaire

Introduction

Les groupes finis sont une structure fondamentale en algèbre abstraite, offrant une richesse de propriétés et d'applications dans divers domaines des mathématiques et de la science. Ce mémoire, réalisé dans le cadre d'un Travail Encadré de Recherche (TER), se concentre sur l'étude des groupes finis, avec un accent particulier sur leurs sous-groupes propres. L'objectif principal de cette recherche est de comprendre comment un groupe fini peut être écrit comme une union de ses sous-groupes propres.

Contexte et motivation

L'étude des groupes et de leurs sous-groupes est au cœur de la théorie des groupes, un domaine central de l'algèbre moderne. Les groupes finis, en particulier, apparaissent naturellement dans de nombreux contextes, allant des symétries géométriques aux solutions d'équations polynomiales. La capacité à décomposer un groupe en termes de ses sous-groupes propres enrichit non seulement notre compréhension de sa structure interne, mais offre également des perspectives nouvelles pour l'analyse et la classification des groupes finis.

La motivation de ce TER provient de l'intérêt mathématique et des applications potentielles de la décomposition des groupes finis en sous-groupes propres. Les résultats classiques, tels que les théorèmes de Lagrange, Sylow et autres, fournissent une base solide pour cette étude. En outre, explorer les conditions sous lesquelles un groupe fini peut être exprimé comme une union de ses sous-groupes propres pose des défis mathématiques captivants et peut conduire à de nouvelles découvertes dans la théorie des groupes.

Objectifs

1. Examiner les propriétés fondamentales des sous-groupes propres des groupes finis.
2. Étudier les conditions spécifiques permettant d'écrire un groupe fini comme une union de ses sous-groupes propres.
3. Identifier et analyser des exemples de groupes satisfaisant cette propriété, ainsi que des contre-exemples.
4. Discuter les implications de ces décompositions dans le cadre plus large de la théorie des groupes finis.

Prérequis

Ce mémoire suppose une familiarité avec les notions de base en théorie des groupes, notamment :

- Les groupes et sous-groupes
- Les sous-groupes normaux
- Les morphismes de groupes
- Les théorèmes de base en théorie des groupes (Lagrange, Sylow, etc.)

Ces concepts sont essentiels pour comprendre les discussions et les résultats présentés dans ce travail, qui se concentrent exclusivement sur les groupes finis.

Méthodologie

La méthodologie adoptée dans ce TER combine des techniques algébriques classiques et des résultats contemporains en théorie des groupes. Nous utiliserons des théorèmes bien établis, ainsi que des démonstrations rigoureuses pour explorer et vérifier les conditions sous lesquelles un groupe fini peut être décomposé en union de ses sous-groupes propres. Des exemples concrets et des contre-exemples seront également présentés pour illustrer et approfondir les concepts discutés.

Notations

- e_G : élément neutre d'un groupe G, i.e. $\forall\, g \in G,\ g \cdot e_G = e_G \cdot g = e_G$;
- $|G|$: ordre ou cardinal d'un groupe G ;
- $< g >$: sous-groupe d'un groupe G, engendré par un élément $g \in G$;
- $[\![1, n]\!]$: tous les entiers compris entre 1 et $n \in \mathbb{N}^*$;
- S_n : groupe symétrique d'ordre $n!$, où $n \in \mathbb{N}^*$;
- A_n : groupe alterné d'ordre $n!/2$, où $n \in \mathbb{N}^*$;
- D_n : groupe diédral d'ordre $2n$, où $n \in \mathbb{N}^*$;
- $i(H)$: indice de H sous-groupe d'un groupe G, i.e. $i(H) = |G|/|H|$;
- HK : sous-groupe engendré par les sous-groupes H et K d'un groupe G, on a en fait $HK = \{hk \mid h \in H, k \in K\} \subset G$;
- G/N : groupe quotient où N est un sous-groupe distingué d'un groupe G, on a en fait $G/N = \{gN \mid g \in G\}$;
- C_n : groupe cyclique d'ordre $n \in \mathbb{N}^*$;
- $\mathrm{ord}(g)$: ordre d'un élément g d'un groupe G ;
- $N_G(H)$: le normalisateur d'un sous-groupe H d'un groupe G, i.e. $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$.

1 Cadre Théorique

1.1 Définitions

Commençons par revoir quelques définitions essentielles, elles seront indispensables à la compréhension ultérieure.

Définition 1.1.1. Soit G un groupe. Soit H un sous-groupe de G. On dit que H est un sous-groupe maximal si, pour tout sous-groupe K tel que $H \subset K \subset G$ on a $K = H$ ou $K = G$.

Définition 1.1.2. Soit G un groupe. Soit H un sous-groupe de G. On dit que H est un sous-groupe propre si $H \neq \{e_G\}$ et $H \neq G$.

Définition 1.1.3. Soient G et K deux groupes. On dit que G admet K pour quotient s'il existe $N \triangleleft G$ tel que $G/N \simeq K$. De façon équivalente, on dit que G admet K pour quotient s'il existe un morphisme surjectif $G \to K$.

Nous allons maintenant présenter l'élément clé de ce chapitre, $\sigma(G)$, défini pour un groupe G. Il est important de noter que cette notation n'est pas universelle.

Définition 1.1.4. Soit G un groupe. Notons $\sigma(G)$ le plus petit entier, s'il existe, tel que G soit union de $\sigma(G)$ sous-groupes propres.

La première question qui se pose est de savoir pour quels groupes G la notation $\sigma(G)$ est pertinente. Donnons une réponse immédiatement.

Proposition 1.1.5. Soit G un groupe. Alors $\sigma(G)$ existe si et seulement si G n'est pas cyclique.

Démonstration.
Commençons par démontrer le sens direct, nous allons utiliser la contraposée. Nous allons donc montrer que si G est cyclique alors $\sigma(G)$ ne peut pas exister. Notons $|G| = n \in \mathbb{N}^*$, alors puisque G est cyclique il possède un élément d'ordre n. Mais cet élément engendre G, et donc ne pourra jamais être contenu dans un sous-groupe propre, ainsi on ne pourra pas écrire G comme union de sous-groupes propres. Donc $\sigma(G)$ n'existe pas, le sens direct est démontré.
Regardons maintenant le sens indirect. Supposons que G n'est pas cyclique.
Notons $|G| = m \in \mathbb{N}^*$ et $G = \{a_1, a_2, ..., a_m\}$, où $a_1 = e_G$.
Posons maintenant $H_i = < a_i >$ pour tout $i \in [\![1, m]\!]$. Nous avons alors :

1. $\forall\ i \in [\![2, m]\!], H_i \neq \{e_G\}$, car $\forall\ i \in [\![2, m]\!], a_i \neq e_G$.
2. $\forall\ i \in [\![2, m]\!], H_i \neq G$, car G n'est pas cyclique.
3. $G = \bigcup_{i=2}^{m} H_i$, car $a_1 \in H_2$ et $\forall\ i \in [\![2, m]\!], a_i \in H_i$.

Ainsi, G est union de $m - 1$ sous-groupes propres, mais nous ne savons pas si $m - 1$ est le plus petit entier vérifiant cela. Donc $\sigma(G) \leq m - 1$.

■

Pour la suite, sauf indication contraire, lorsque nous évoquerons $\sigma(G) \in \mathbb{N}$, le groupe G sera considéré comme non cyclique. Si G est cyclique, nous poserons $\sigma(G) = +\infty$.

1.2 Exemples

Observons maintenant la valeur de $\sigma(G)$ pour divers groupes G, qui, par conséquent, ne seront pas cycliques.

Proposition 1.2.1. Voici les différentes valeurs de $\sigma(S_n)$ pour $n \in [\![1, 6]\!]$:

- $\sigma(S_1) = +\infty$
- $\sigma(S_2) = +\infty$
- $\sigma(S_3) = 4$
- $\sigma(S_4) = 4$
- $\sigma(S_5) = 16$
- $\sigma(S_6) = 13$

Démonstration.
Nous allons utiliser la même méthode pour démontrer les six points, exhiber tous les sous-groupes propres, et regarder la plus petite combinaison de ces sous-groupes qui recouvre le groupe tout entier.
- $S_1 = \{\mathrm{Id}\}$ est cyclique.
- $S_2 = \{\mathrm{Id}, (1\,2)\}$ est cyclique.
- $S_3 = \{\mathrm{Id}, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$ possède 4 sous-groupes propres, qui sont $\{\mathrm{Id}, (1\,2)\}$, $\{\mathrm{Id}, (1\,3)\}$, $\{\mathrm{Id}, (2\,3)\}$ et $\{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\}$. On remarque donc que pour recouvrir S_3 il faut forcément utiliser les 4 sous-groupes propres, ainsi $\sigma(S_3) = 4$.
- Nous utilisons la même méthode pour les trois autres groupes, on exhibe tous les sous-groupes propres et on calcule $\sigma(G)$ à la main.

■

Proposition 1.2.2. Voici les différentes valeurs de $\sigma(A_n)$ pour $n \in [\![1, 5]\!]$:

- $\sigma(A_1) = +\infty$
- $\sigma(A_2) = +\infty$
- $\sigma(A_3) = +\infty$
- $\sigma(A_4) = 5$
- $\sigma(A_5) = 10$

Démonstration.
Nous allons utiliser la même méthode pour démontrer les cinq points, exhiber tous les sous-groupes propres, et regarder la plus petite combinaison de ces sous-groupes qui recouvre le groupe tout entier.
- $A_1 = \{\mathrm{Id}\}$ est cyclique.
- $A_2 = \{\mathrm{Id}\}$ est cyclique.
- $A_3 = \{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\}$ est cyclique.
- Nous utilisons la même méthode pour les deux autres groupes, on exhibe tous les sous-groupes propres et on calcule $\sigma(G)$ à la main.

■

Dans la suite, pour un $n \in \mathbb{N}^*$, on notera D_n le groupe diédral d'ordre $2n$. On notera r (élément d'ordre n) et s (élément d'ordre 2) ses générateurs, on a donc $D_n =< r, s >= \{\mathrm{Id}, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$.

Proposition 1.2.3. Voici les différentes valeurs de $\sigma(D_n)$ pour $n \in [\![1, 5]\!]$:

- $\sigma(D_1) = +\infty$
- $\sigma(D_2) = 3$
- $\sigma(D_3) = 4$
- $\sigma(D_4) = 3$
- $\sigma(D_5) = 6$

Lorsque n est pair : $\sigma(D_n) = 3$,
Lorsque n est premier : $\sigma(D_n) = n + 1$

Démonstration.
Nous allons utiliser la même méthode pour démontrer les cinq points, exhiber tous les sous-groupes propres, et regarder la plus petite combinaison de ces sous-groupes qui recouvre le groupe tout entier.
• $D_1 = \{\mathrm{Id}, s\}$ est cyclique.
• $D_2 = \{\mathrm{Id}, r, s, sr\}$ possède 3 sous-groupes propres maximaux qui sont $\{\mathrm{Id}, s\}$, $\{\mathrm{Id}, r\}$, $\{\mathrm{Id}, sr\}$. On remarque donc que pour recouvrir S_3 il faut forcément utiliser les 3 sous-groupes propres, ainsi $\sigma(D_2) = 3$.
• $D_3 = \{\mathrm{Id}, r, r^2, s, sr, sr^2\}$ possède 3 sous-groupes propres maximaux qui sont $\{\mathrm{Id}, s\}$, $\{\mathrm{Id}, r, r^2\}$ et $\{\mathrm{Id}, s, sr, sr^2\}$. On remarque donc que pour recouvrir D_3 il faut forcément les utiliser les 3 sous-groupes propres, ainsi $\sigma(D_3) = 3$.
• Nous utilisons la même méthode pour les deux autres groupes, on exhibe tous les sous-groupes propres et on calcule $\sigma(G)$ à la main.

■

1.3 Théorèmes et Lemmes Préparatoires

Nous constatons que le calcul de $\sigma(G)$, pour un groupe G, en énumérant tous les sous-groupes propres devient complexe lorsque l'ordre du groupe est élevé. L'objectif est donc de trouver des théorèmes "principaux" qui simplifient ce calcul. Avant cela, nous allons introduire, dans cette section, des lemmes et des théorèmes qui poseront les bases nécessaires pour démontrer ces théorèmes principaux.

Avant cela, nous allons introduire quelques notations. Lorsqu'on aura $\sigma(G) = n \in \mathbb{N}^*$ pour un groupe G, on écrira souvent $G = \bigcup_{k=1}^{n} H_k$, où H_1, H_2, …, H_n sont des sous-groupes propres de G. On notera $i_k = i(H_k)$ l'indice du sous-groupe H_k, et on les ordennera toujours (sauf mention contraire) dans l'ordre croissant i.e. $i_1 \leq i_2 \leq \ldots \leq i_n$ et donc $|H_1| \geq |H_2| \geq \ldots \geq |H_n|$.

De plus, quitte à les remplacer, on pourra supposer que tous les H_i sont des sous-groupes maximaux.

Théorème 1.3.1. Soit G un groupe tel que $\sigma(G) = n \in \mathbb{N}^*$. Notons H_1, H_2, … , H_n les n sous-groupes propres tels que $G = \bigcup_{k=1}^{n} H_k$. Alors $|G| \leq \sum_{k=2}^{n} |H_k|$, avec égalité si et seulement si $H_1 H_r = G$, $r \neq 1$ et $H_r \cap H_s \subset H_1$, $r \neq s$.

Démonstration.
On suppose que $\sigma(G) = n \in \mathbb{N}^*$. Pour tout $k \in [\![2, n]\!]$, regardons le nombre d'éléments dans H_k mais pas dans H_1 :

$$|H_k| - |H_1| \cap |H_k| = |H_k| - \frac{|H_1||H_k|}{|H_1 H_k|} \leq |H_k| - \frac{|H_1||H_k|}{|G|} = |H_k| \left(1 - \frac{|H_1|}{|G|}\right).$$

Nous avons donc :

$$\begin{aligned} |G| &\leq |H_1| + \sum_{k=2}^{n} \left(|H_k| - |H_1| \cap |H_k|\right) \\ &\leq |H_1| + \sum_{k=2}^{n} |H_k| \left(1 - \frac{|H_1|}{|G|}\right) \\ &\leq |H_1| + \left(1 - \frac{|H_1|}{|G|}\right) \sum_{k=2}^{n} |H_k| \end{aligned}$$

Ce qui donne finalement :

$$\begin{aligned} & |G| - |H_1| \leq \left(1 - \frac{|H_1|}{|G|}\right) \sum_{k=2}^{n} |H_k| \\ \implies \quad & |G| \times (|G| - |H_1|) \leq (|G| - |H_1|) \sum_{k=2}^{n} |H_k| \\ \implies \quad & |G| \leq \sum_{k=2}^{n} |H_k| \end{aligned}$$

De plus, l'égalité a lieu si et seulement si les inégalités utilisées ci-dessus sont en fait des égalités i.e. $H_1 H_r = G$ pour tout $r \neq 1$, et deux sous-groupes n'ont pas d'éléments en commun non contenu dans H_1 i.e. $H_r \cap H_s \subset H_1$ pour tout $r \neq s$.

■

Il convient de souligner l'importance du lemme suivant dans les démonstrations de la section à venir, car il permet de déterminer les indices des sous-groupes propres. Ce résultat joue un rôle fondamental dans l'analyse des propriétés structurelles des groupes considérés, en fournissant un moyen systématique de caractériser les sous-groupes et leur relation avec le groupe principal.

Lemme 1.3.2. Soit G un groupe tel que $\sigma(G) = n \in \mathbb{N}^*$. Notons H_1, H_2, ... , H_n les n sous-groupes propres tels que $G = \bigcup_{k=1}^{n} H_k$. Alors $i_2 \leq n - 1$.

Démonstration.
Avec le théorème précédent nous avons :

$$|G| \leq \sum_{k=2}^{n} |H_k| \ , \text{ ce qui donne : } \ \frac{|G|}{|H_2|} \leq \sum_{k=2}^{n} \frac{|H_k|}{|H_2|} = \sum_{k=2}^{n} \frac{|G|}{|H_2|} \frac{|H_k|}{|G|} \ .$$

Avec nos notations :

$$i_2 \leq \sum_{k=2}^{n} \frac{i_2}{i_k} \ , \text{ où } i_2 \leq i_3 \leq ... \leq i_n \text{ et donc : } \forall\ k \in [\![2, n]\!] \text{ on a } \frac{i_2}{i_k} \leq 1.$$

Ainsi,

$$i_2 \leq \sum_{k=2}^{n} \frac{i_2}{i_k} \leq \sum_{k=2}^{n} 1 \leq n-1.$$

■

De manière analogue au lemme précédent, le lemme à venir sera important dans les démonstrations de la section suivante pour majorer $\sigma(G)$. Cette étape est essentielle pour réduire autant que possible les cas à considérer, ce qui simplifie considérablement le calcul de $\sigma(G)$.

Lemme 1.3.3. Soit G un groupe. Si $N \triangleleft G$, alors $\sigma(G) \leq \sigma(G/N)$.

Démonstration.
Posons $\sigma(G/N) = n \in \mathbb{N}^*$, et notons H_1, H_2, ... , H_n les n sous-groupes propres tels que $G/N = H_1 \cup \ldots \cup H_n$.
Notons $\pi : G \to G/N$, $g \mapsto gN$ la surjection canonique.
Posons maintenant $K_i = \pi^{-1}(H_i)$ pour tout $i \in [\![1, n]\!]$. Nous avons alors :

1. $\forall\, i \in [\![1, n]\!], K_i \neq \{e_G\}$, sinon on aurait $H_i = \{e_G\}$.
2. $\forall\, i \in [\![1, n]\!], K_i \neq G$, sinon on aurait $H_i = G$.
3. $G = K_1 \cup \ldots \cup K_n$, car $G/N = H_1 \cup \ldots \cup H_n$ et π est surjective.

Ainsi, G est union de n sous-groupes propres, mais nous ne savons pas si n est le plus petit entier vérifiant cela. Donc $\sigma(G) \leq n = \sigma(G/N)$.

■

Dans le lemme 1.3.4 et le théorème 1.3.6 qui suivent, nous allons calculer les valeurs de $\sigma(G)$ pour deux types spécifiques de groupes G.

Lemme 1.3.4. Soit p un nombre premier. Nous avons : $\sigma(C_p \times C_p) = p + 1$.

Démonstration.
Notons $G = C_p \times C_p$, on a donc $|G| = |C_p \times C_p| = p^2$.
Nous allons d'abord montrer une première inégalité. Si H est un sous-groupe de G, alors d'après le théorème de Lagrange nous savons que l'ordre de H divise p^2. Ainsi, $|H| \in \{1, p, p^2\}$; donc si H est un sous-groupe propre on a forcément $|H| = p$ et donc $[G : H] = |G/H| = |G|/|H| = p$. En particulier, si nous reprenons les notations habituelles, on a $i_2 = p$. Le lemme 1.3.2 nous donnne alors $p \leq \sigma(G) - 1$, d'où $\sigma(G) \geq p + 1$.
Montrons maintenant la seconde inégalité. Soit $g \in G$ tel que $g \neq e_G$, alors d'après le théorème de Lagrange nous savons que l'ordre de g divise p^2, notons le $\text{ord}(g)$. Ainsi, $\text{ord}(g) \in \{p, p^2\}$; mais G n'est pas cyclique, donc $\text{ord}(g) = p$. Nous savons donc que chaque élément g va engendrer un sous-groupe d'ordre p. Prenons $p + 1$ sous-groupes deux à deux distincts comme ceci, notons les H_1, H_2, ... , H_{p+1}. On peut donc écrire $|H_1 \cup \ldots \cup H_{p+1}| = |H_1| + ... + |H_{p+1}| - p = (p + 1)(p - 1) + 1 = p^2 = |G|$. Ce qui nous donne : $G = H_1 \cup ... \cup H_{p+1}$. Ainsi, G est union de $p + 1$ sous-groupes propres, mais nous ne savons pas si $p + 1$ est le plus petit entier vérifiant cela, donc $\sigma(G) \leq p + 1$.

■

Définition 1.3.5. Soit G un groupe. Soit p un nombre premier. On dit que G est un p-groupe s'il existe $m \in \mathbb{N}^*$ tel que $|G| = p^m$.

Théorème 1.3.6. Soit G un p-groupe non cyclique. Alors : $\sigma(G) = p + 1$.

Démonstration.
Puisque G n'est pas cyclique nous savons avec la proposition 1.1.5 que $\sigma(G)$ existe, notons $\sigma(G) = n \in \mathbb{N}^*$. Posons $|G| = p^m$, où $m \in \mathbb{N}^*$, et H_1, H_2, ..., H_n les n sous-groupes propres tels que $G = H_1 \cup \ldots \cup H_n$.
Montrons une première inégalité. Si H est un sous-groupe de G, d'après le théorème de Lagrange, il existe $l \in [\![1, m]\!]$ tel que $|H| = p^l$. Donc si H est un sous-groupe propre, $l \in [\![2, m-1]\!]$, ainsi $|H| \leq p^{m-1}$. En particulier, $|H_2| \leq p^{m-1}$ et donc $i_2 \geq \frac{p^m}{p^{m-1}} = p$, ainsi en utilisant le lemme 1.3.2 nous avons $\sigma(G) \geq p + 1$.
Motrons maintenant la seconde inégalité. Comme G est un p-groupe non cyclique (abélien), il possède un quotient isomorphe à $C_p \times C_p$, ainsi il existe $N \triangleleft G$ tel que $G/N \simeq C_p \times C_p$. On peut donc utiliser les lemmes 1.3.3 et 1.3.4, ce qui donne : $\sigma(G) \leq \sigma(G/N) = \sigma(C_p \times C_p) = p + 1$.

■

Lemme 1.3.7. Soit G un groupe. Soit H un sous-groupe maximal de G. Alors, soit H possède $i(H)$ conjugués dans G, soit $H \triangleleft G$ et $i(H)$ est premier.

Démonstration.
Notons $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ le normalisateur de H dans G. Nous savons alors que $N_G(H) \triangleleft G$ et $H \subset N_G(H) \subset G$. Or, H est un sous-groupe maximal de G, donc $N_G(H) = H$ ou $N_G(H) = G$. Distingons les deux cas.

- Si $N_G(H) = H$, alors H possède $i(N_G(H)) = i(H)$ conjugués dans G.
- Si $N_G(H) = G$, alors $H \triangleleft G$, il reste à montrer que $i(H)$ est premier. Prenons $x \in G$ mais $x \notin H$. Comme H est un sous-groupe maximal de G, on a $H \subset < H, x > = G$, et puisque $H \triangleleft G$ on a également $Hx = xH$. Donc, pour tout élément $g \in G$, il existe $h \in H$ et $n \in \mathbb{N}$ tels que $y = hx^i$. Notons $k \in \mathbb{N}$ le plus petit entier tel que $x^k \in H$, alors $G = \bigcup_{n=1}^{k} Hx^n$ et $k = i(H)$. Supposons qu'il existe deux entiers différents $a, b \neq 1$ tels que $k = ab$, alors $x^a \notin H$ par la définition de k. On a donc $< H, x^a >$ qui est un sous-groupe propre de G tel que $H \subset < H, x^a >$, ce qui contredit la maximalité de H, $i(H) = k$ est donc premier.

■

Lemme 1.3.8. Soit G un groupe tel que $\sigma(G) = n \in \mathbb{N}^*$. Soit $m \in \mathbb{N}$ tel que $m < n$. Si G peut s'écrire $G = \left(\bigcup_{r=1}^{m} H_r\right) \cup \left(\bigcup_{r=m+1}^{n} K_r\right)$, où tous les sous-groupes sont maximaux et où les H_r ont des ordres distincts et sont distingués dans G, alors $|G| \leq \sum_{r=m+1}^{n} |K_r|$.

Démonstration.
Pour tout $r \in \{1, \ldots, m\}$, on a $H_r \triangleleft G$. Donc, d'après le Lemme 1.3.7, on peut poser $i(H_r) = p_r$, où les p_r sont des nombres premiers. Pour tout $r, s \in \{1, \ldots, m\}$ tels que $r \neq s$, les sous-groupes H_r et H_s sont distingés dans G et maximaux par hypothèse, ainsi $G = H_r H_s$ et donc

$$i(H_r \cap H_s) = \frac{|G||H_r H_s|}{|H_r||H_s|} = \frac{|G||G||H_r H_s|}{|H_r||H_s||G|} = i(H_r)i(H_s)$$

Posons $D = \bigcup_{r=1}^{m} H_r$. Nous pouvons alors calculer le nombre d'éléments dans D

$$\begin{aligned}
|D| &= \sum_{r=1}^{m} |H_r| - \sum_{r=1}^{m}\sum_{s=1}^{m} |H_r \cap H_s| + \sum_{r=1}^{m}\sum_{s=1}^{m}\sum_{t=1}^{m} |H_r \cap H_s \cap H_t| - \dots \\
&= |G| \left[\sum_{r=1}^{m} \frac{|H_r|}{|G|} - \sum_{r=1}^{m}\sum_{s=1}^{m} \frac{|H_r \cap H_s|}{|G|} + \sum_{r=1}^{m}\sum_{s=1}^{m}\sum_{t=1}^{m} \frac{|H_r \cap H_s \cap H_t|}{|G|} - \dots \right] \\
&= |G| \left[\sum_{r=1}^{m} \frac{1}{p_r} - \sum_{r=1}^{m}\sum_{s=1}^{m} \frac{1}{p_r p_s} + \sum_{r=1}^{m}\sum_{s=1}^{m}\sum_{t=1}^{m} \frac{1}{p_r p_s p_t} - \dots \right] \\
&= |G| \left[1 - \prod_{r=1}^{m} \left(1 - \frac{1}{p_r} \right) \right]
\end{aligned}$$

Posons, pour tout $r \in \{m+1, \dots, n\}$, $k_r = |K_r \backslash (D \cap K_r)|$. Nous savons que pour tout $s \in \{1, \dots, m\}$, $H_s \triangleleft G$ et K_r est maximal. Donc :

$$|H_s \cap K_r| = \frac{|H_s||K_r|}{|H_s K_r|} = \frac{|H_s||K_r|}{|G|} = \frac{|K_r|}{p_s}$$

De plus, pour tout $s, t \in \{1, \dots, m\}$, $H_s \cap H_t \cap K_r$ est un sous-groupe de $H_s \cap K_r$ et de $H_t \cap K_r$, donc divise $|K_r|/p_s$ et $|K_r|/p_t$, donc divise $|K_r|/p_s p_t$. Mais on a également

$$\begin{aligned}
|H_s \cap H_t \cap K_r| &= \frac{|K_r||H_s \cap H_t|}{|K_r(H_s \cap H_t)|} \\
&= \frac{|K_r||G|}{p_s p_t |K_r(H_s \cap H_t)|} \\
&\geq \frac{|K_r|}{p_s p_t}
\end{aligned}$$

et ainsi $|H_s \cap H_t \cap K_r| = |K_r|/p_s p_t$.

Nous pouvons étendre ces arguments, et on obtient

$$k_r = |K_r| \left(1 - \sum 1/p_s + \sum\sum 1/p_s p_t + \cdots \right) = |K_r| \left[\prod_{s=1}^{m} \left(1 - \frac{1}{p_s} \right) \right]$$

Par définition de D et des k_r, on a

$$\begin{aligned}
|G| &\leq |D| + \sum_{r=m+1}^{n} k_r \\
&= |G| \left[1 - \prod_{r=1}^{m} \left(1 - \frac{1}{p_r} \right) \right] + \sum_{r=m+1}^{n} |K_r| \left[\prod_{s=1}^{m} \left(1 - \frac{1}{p_s} \right) \right] \\
&= |G| - |G| \left[\prod_{r=1}^{m} \left(1 - \frac{1}{p_r} \right) \right] + \sum_{r=m+1}^{n} |K_r| \left[\prod_{s=1}^{m} \left(1 - \frac{1}{p_s} \right) \right]
\end{aligned}$$

Et donc finalement

$$\begin{aligned}
0 &\leq -|G| \left[\prod_{r=1}^{m}\left(1-\frac{1}{p_r}\right)\right] + \sum_{r=m+1}^{n} |K_r| \left[\prod_{s=1}^{m}\left(1-\frac{1}{p_s}\right)\right] \\
&\Rightarrow |G| \left[\prod_{r=1}^{m}\left(1-\frac{1}{p_r}\right)\right] \leq \sum_{r=m+1}^{n} |K_r| \left[\prod_{s=1}^{m}\left(1-\frac{1}{p_s}\right)\right] \\
&\Rightarrow |G| \leq \sum_{r=m+1}^{n} |K_r|
\end{aligned}$$

■

2 Théorèmes Principaux

Dans ce chapitre, nous examinerons des théorèmes qui nous permettront de déterminer $\sigma(G)$ pour un groupe G sans avoir à exhiber tous les sous-groupes propres. Nous établirons une équivalence entre la valeur de $\sigma(G)$ et l'existence d'un morphisme surjectif lorsque $\sigma(G)$ prend les valeurs de 2 à 7. Il est évident que $\sigma(G)$ ne peut jamais être égal à 1, car, par définition, un sous-groupe propre ne peut pas être égal au groupe tout entier.

2.1 Cas 2 et 3

Dans cette section nous traiterons les cas $\sigma(G) = 2$ et 3. Dans un premier temps, remarquons que $\sigma(G)$ ne peut jamais être égal à 2.

Théorème 2.1.1. Il n'existe pas de groupe G tel que $\sigma(G) = 2$.

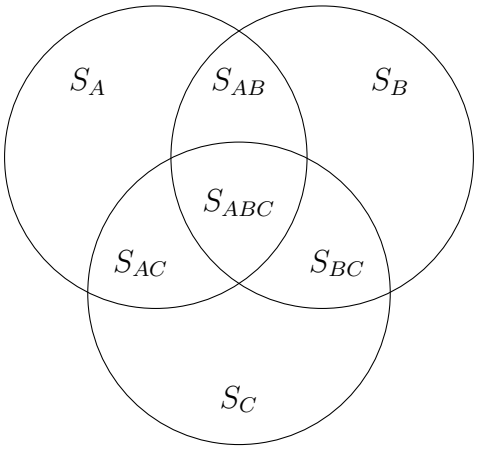
Démonstration.
Supposons que $\sigma(G) = 2$, donc G est union de deux sous-groupes propres. Notons ces deux sous-groupes A et B, alors $G = A \cup B$ et $A \neq G$, $B \neq G$. Prenons un élément $a \in A$ qui n'est pas dans B (existe sinon $A \subset B$ et donc $A \cup B = B \neq G$), et un élément $b \in B$ qui n'est pas dans A (existe sinon $B \subset A$ et donc $A \cup B = A \neq G$). Regardons le produit ab, si $ab \in A$ alors $a^{-1}ab \in A$ ($a^{-1} \in A$), or $a^{-1}ab = b$ et b n'est pas dans A, donc ab n'est pas dans A. Si $ab \in B$ alors $abb^{-1} \in B$ ($b^{-1} \in B$), or $abb^{-1} = a$ et a n'est pas dans B, donc ab n'est pas dans B. Ceci est absurde puisque $ab \in G$ ($a \in G, b \in G$), $G = A \cup B$, mais $ab \notin A$ et $ab \notin B$.

■

Pour le cas $\sigma(G) = 3$, cela se complique légèrement, Scorza à démontré le théorème suivant en 1926.

Théorème 2.1.2 (Scorza, 1926)**.** Soit G un groupe. Alors $\sigma(G) = 3$ si et seulement si G admet $C_2 \times C_2$ comme quotient.

Démonstration.
Commençons par démontrer le sens direct, pour cela nous avons deux démonstrations, une première plus élémentaire et une seconde plus rapide. Voici la première.



$$\begin{cases} S_A = A\backslash(A \cap (B \cup C)) \\ S_B = B\backslash(B \cap (A \cup C)) \\ S_C = C\backslash(C \cap (A \cup B)) \\ S_{AB} = (A \cup B)\backslash((A \cup B) \cap C) \\ S_{AC} = (A \cup C)\backslash((A \cup C) \cap B) \\ S_{BC} = (B \cup C)\backslash((B \cup C) \cap A) \\ S_{ABC} = A \cap B \cap C \end{cases}$$

Supposons que $\sigma(G) = 3$, donc G est union de trois sous-groupes propres. Notons ces trois sous-groupes A, B et C, alors $G = A \cup B \cup C$ et $A \neq G, B \neq G, C \neq G$ et $A \neq \{e_G\}, B \neq \{e_G\}, C \neq \{e_G\}$.
Nous voulons alors montrer que G admet $C_2 \times C_2$ commme quotient, pour cela il suffit de trouver un sous-groupe $N \triangleleft G$ tel que le quotient G/N soit isomorphe à $C_2 \times C_2$. Il se trouve que ce sous-groupe sera S_{ABC}, notre objectif va donc être de montrer que G/S_{ABC} est isomorphe à $C_2 \times C_2$.

Dans un premier temps nous allons montrer que $S_{AB} = S_{BC} = S_{AC} = \emptyset$.
Prenons $a \in S_A$ et $x \in S_{BC}$. Si $ax \in A$, alors $a^{-1}ax \in A$ ($a^{-1} \in A$), or $a^{-1}ax = x$ et x n'est pas dans A, donc $ax \notin A$. Si $ax \in B \cup C$, alors $axx^{-1} \in B \cup C$ ($x^{-1} \in B \cup C$), or $axx^{-1} = a$ et a n'est pas dans $B \cup C$, donc ax n'est pas dans $B \cup C$. Ceci est absurde puisque $ax \in G$ ($a \in G, x \in G$), $G = A \cup B \cup C$, mais $ax \notin A$, $ax \notin B \cup C$. Contradiction : x n'existe pas (a existe toujours, $S_A \neq \{e_G\}$ sinon $A \subset B \cup C \Rightarrow B \cup C = G \Rightarrow \sigma(G) = 2$), ainsi $S_{BC} = \emptyset$. Par un raisonnement symétrique nous obtient également $S_{AB} = S_{AC} = \emptyset$. Nous avons donc $G = S_A \cup S_B \cup S_C \cup S_{ABC}$.

Soit $a \in S_A$, $b \in S_B$. Regardons le produit ab, si $ab \in A$ alors $a^{-1}ab \in A$ ($a^{-1} \in A$), or $a^{-1}ab = b$ et b n'est pas dans A, donc ab n'est pas dans A. Si $ab \in B$ alors $abb^{-1} \in B$ ($b^{-1} \in B$), or $abb^{-1} = a$ et a n'est pas dans B, donc ab n'est pas dans B. Donc $ab \in S_C$, ce qui nous donne $S_A S_B \subset S_C$ (de la même façon nous obtenons $S_B S_A \subset S_C$, $S_A S_C \subset S_B$, $S_C S_A \subset S_B$, $S_B S_C \subset S_A$, $S_C S_B \subset S_A$).
Prenons $c \in S_C$, alors pour tout $b \in S_B$, on a $a = cb^{-1} \in S_C S_B \subset S_A$ et donc $c = ab \in S_A S_B$. Ainsi nous avons $S_C \subset S_A S_B$ (de la même façon nous obtenons $S_C \subset S_B S_A$, $S_A \subset S_B S_C$, $S_A \subset S_C S_B$, $S_B \subset S_A S_C$, $S_B \subset S_C S_A$). Nous avons donc les égalités suivantes : $S_C = S_A S_B = S_B S_A$, $S_A = S_B S_C = S_C S_B$, $S_B = S_A S_C = S_C S_A$. Avec les mêmes arguments nous obtenons également : ${S_A}^2 = {S_B}^2 = {S_C}^2 = S_A S_B S_C = S_{ABC}$.

De plus, prenons $a \in S_A$, $b \in S_B$, $c \in S_C$, alors $a \cdot S_{ABC} = S_{ABC} \cdot a = S_A$, $b \cdot S_{ABC} = S_{ABC} \cdot b = S_B$, $c \cdot S_{ABC} = S_{ABC} \cdot c = S_C$.

Nous avons donc : $G/S_{ABC} = \{g \cdot S_{ABC};\ g \in G\} = \{S_{ABC}, S_A, S_B, S_C\}$.

Notons $C_2 \times C_2 = < a > \times < b > = \{e, a\} \times \{e, b\} = \{e, a, b, ab\}$.
Posons $\phi : G/S_{ABC} \to C_2 \times C_2$, où $\phi(S_{ABC}) = e$, $\phi(S_A) = a$, $\phi(S_B) = b$, $\phi(S_C) = ab$.
Alors, par toutes les relations demontrées ci-dessus, nous pouvons affirmer que ϕ est un isomorphisme. Ainsi, G admet $C_2 \times C_2$ comme quotient.

Regardons maintenant la deuxième démonstration, nous allons utiliser la stratégie suivante :

$$\begin{aligned}[\sigma(G) = 3] &\Rightarrow [\exists\ A, B < G \text{ tels que } |G/A| = |G/B| = 2] \\ &\Rightarrow [\exists\ N \triangleleft G \text{ tel que } G/N \simeq C_2 \times C_2]\end{aligned}$$

Notons $G = H_1 \cup H_2 \cup H_3$ où H_1, H_2, H_3 sont 3 sous-groupes propres tels que $|H_1| \geq |H_2| \geq |H_3|$, et donc tels que $i_1 \leq i_2 \leq i_3$.

En utilisant le lemme 1.3.2, nous avons $i_2 \leq \sigma(G) - 1 = 3 - 1 = 2$. Or, $i_1 \leq i_2$, donc nous avons forcément $i_1 = i_2 = 2$. Ainsi la première implication est démontrée, il suffit de poser $A = H_1$ et $B = H_2$.

Nous savons que A et B sont deux sous-groupes d'indices 2 de G, ils sont donc distingués dans G. Nous pouvons alors regarder G/A et G/B comme deux groupes.

$$\begin{array}{rccc} \text{Notons } \pi : & G & \to & G/A \times G/B \\ & g & \mapsto & (gA, gB) \end{array}$$

Nous avons $|G/A| = |G/B| = 2$, donc $G/A \simeq C_2$ et $G/B \simeq C_2$.
Notons K le noyau de π, $K = \ker(\pi) \triangleleft G$. Nous avons $K \subset A \cap B$, en effet si $g \in K$, alors $(gA, gB) = (A, B)$ et donc $g \in A \cap B$. Avec le premier théorème d'isomorphisme, nous avons donc $G/K \simeq \mathrm{Im}(\pi)$. Le but va donc être de montrer que $\mathrm{Im}(\pi) \simeq C_2 \times C_2$. Nous savons déja que $\mathrm{Im}(\pi)$ est isomorphe à un sous-groupe de $C_2 \times C_2$, mais lequel ?

De plus, $|\mathrm{Im}(\pi)|$ divise $4 = |C_2 \times C_2|$, il reste à éliminer les cas 1 et 2.

- $|\mathrm{Im}(\pi)| = 1 \Rightarrow G = K \Rightarrow G \subset A \cap B$, absurde
- $|\mathrm{Im}(\pi)| = 2 \Rightarrow |G/K| = 2$, or $K \subset A$ et $K \subset B \Rightarrow K = A = B$, absurde

Donc nous avons forcément $|\mathrm{Im}(\pi)| = 4$. Et le seul sous-groupe de $C_2 \times C_2$ d'ordre 4, est $C_2 \times C_2$ lui-même. Donc, $\mathrm{Im}(\pi) \simeq C_2 \times C_2$, et ainsi $G/K \simeq C_2 \times C_2$.

Le sens direct est démontré, montrons le sens indirect.
Nous supposons que G admet $C_2 \times C_2$ comme quotient, donc il existe un sous-groupe $N \triangleleft G$ tel que G/N soit isomorphe à $C_2 \times C_2$, on a donc $\sigma(G/N) = \sigma(C_2 \times C_2)$.
En utilisant le lemme 1.3.4, nous savons que $\sigma(C_2 \times C_2) = 2 + 1 = 3$.
Ainsi, d'après le lemme 1.3.3, $\sigma(G) \leq \sigma(G/N) = \sigma(C_2 \times C_2) = 3$.
Mais, avec le théorème 2.1.1, il ne reste qu'une possibilité : $\sigma(G) = 3$.

■

2.2 Cas 4 et 5

Dans cette section nous traiterons les cas $\sigma(G) = 4$ et 5. Ces deux théorèmes ont été démontrés par Cohn en 1993. Ces deux cas sont plus compliqués que les précédents, mais nous utiliserons a peu près la même méthode pour démontrer ces deux résultats.

Théorème 2.2.1 (Cohn, 1993)**.** Soit G un groupe. Alors $\sigma(G) = 4$ si et seulement si $\sigma(G) \neq 3$ et G admet $C_3 \times C_3$ ou S_3 comme quotient

Démonstration.
Commençons par montrer le sens direct, nous allons utiliser la stratégie suivante :

$$\begin{aligned}[\sigma(G) = 4] &\Rightarrow [\exists\ A, B < G \text{ tels que } |G/A| = |G/B| = 3] \\ &\Rightarrow [\exists\ N \triangleleft G \text{ tel que } G/N \simeq C_3 \times C_3 \text{ ou } G/N \simeq S_3]\end{aligned}$$

Notons $G = H_1 \cup H_2 \cup H_3 \cup H_4$ où H_1, H_2, H_3, H_4 sont 4 sous-groupes propres tels que $|H_1| \geq |H_2| \geq |H_3| \geq |H_4|$, et donc tels que $i_1 \leq i_2 \leq i_3 \leq i_4$.

En utilisant le lemme 1.3.2, on a $i_2 \leq \sigma(G) - 1 = 4 - 1 = 3$. Or, si $i_2 = 2$ nous avons forcément $i_1 = i_2 = 2$, et nous nous retrouvons dans le cas de la démonstration du théorème 2.1.2 et on aurait donc $\sigma(G) = 3$, absurde. Ainsi, $i_2 = 3$.

Avec le théoreme 1.3.1, on a $|G| \leq |H_2| + |H_3| + |H_4|$ et donc $1 \leq \frac{1}{i_2} + \frac{1}{i_3} + \frac{1}{i_4}$. Or, $3 = i_2 \leq i_3 \leq i_4$, donc on a forcément $i_2 = i_3 = i_4 = 3$. On a donc démontré la première implication, il suffit de poser par exmple $A = H_2$ et $B = H_3$.

Pour montrer la deuxième implication, nous allons distinguer deux cas.

Cas n°1 : On suppose $A \triangleleft G$ et $B \triangleleft G$.

Notons $\pi : \begin{array}{ccc} G & \to & G/A \times G/B \\ g & \mapsto & (gA, gB) \end{array}$

Nous avons $|G/A| = |G/B| = 3$, donc $G/A \simeq C_3$ et $G/B \simeq C_3$.
Notons K le noyau de π, $K = \ker(\pi) \triangleleft G$. Nous avons $K \subset A \cap B$, en effet si $g \in K$, alors $(gA, gB) = (A, B)$ et donc $g \in A \cap B$. Avec le premier théorème d'isomorphisme, nous avons donc $G/K \simeq \mathrm{Im}(\pi)$. Le but va donc être de montrer que $\mathrm{Im}(\pi) \simeq C_3 \times C_3$. Nous savons déja que $\mathrm{Im}(\pi)$ est isomorphe à un sous-groupe de $C_3 \times C_3$, mais lequel ?

Nous savons que $|\mathrm{Im}(\pi)|$ divise $9 = |C_3 \times C_3|$.

- $|\mathrm{Im}(\pi)| = 1 \Rightarrow G = K \Rightarrow G \subset A \cap B$, absurde
- $|\mathrm{Im}(\pi)| = 3 \Rightarrow |G/K| = 3$, or $K \subset A$ et $K \subset B \Rightarrow K = A = B$, absurde

Donc nous avons forcément $|\mathrm{Im}(\pi)| = 9$. Et le seul sous-groupe de $C_3 \times C_3$ d'ordre 9, est $C_3 \times C_3$ lui-même. Donc, $\mathrm{Im}(\pi) \simeq C_3 \times C_3$, et ainsi $G/K \simeq C_3 \times C_3$.

Cas n°2 : On suppose $A \not\triangleleft G$ (ou $B \not\triangleleft G$, mais la démonstration sera la même). Notons $\pi : \begin{array}{ccc} G & \to & S_{G/A} \\ g & \mapsto & \pi_g : \end{array}$

Nous avons $|G/A| = 3$ donc $S_{G/A} \simeq S_3$.

Notons K le noyau de π, $K = \ker(\pi) \triangleleft G$. Nous avons $K \subset A$, ($g \in K \Rightarrow \forall\ h \in G,\ ghA = hA \Rightarrow$ pour $h = e_G,\ gA = A \Rightarrow g \in A$). Avec le premier théorème d'isomorphisme, nous avons donc $G/K \simeq \mathrm{Im}(\pi)$.

Le but va donc être de montrer que $\mathrm{Im}(\pi) \simeq S_3$. Nous savons déja que $\mathrm{Im}(\pi)$ est isomorphe à un sous-groupe de S_3, mais lequel ?

Nous savons que $|\mathrm{Im}(\pi)|$ divise $6 = |S_3|$.

- $|\mathrm{Im}(\pi)| = 1 \Rightarrow G = K \Rightarrow G \subset A$, absurde.
- $|\mathrm{Im}(\pi)| = 2 \Rightarrow |G/K| = 2 \Rightarrow |K| = \frac{3}{2}|A|$, or $K \subset A$, absurde.
- $|\mathrm{Im}(\pi)| = 3 \Rightarrow |G/K| = 3 \Rightarrow K = A$, or $K \triangleleft G$ et $A \not\triangleleft G$, absurde.

Donc nous avons forcément $|\mathrm{Im}(\pi)| = 6$. Et le seul sous-groupe de S_3 d'ordre 6, est S_3 lui-même. Donc, $\mathrm{Im}(\pi) \simeq S_3$, et ainsi $G/K \simeq S_3$.

Le sens direct est démontré, montrons le sens indirect.
Nous supposons que G admet $C_3 \times C_3$ comme quotient, donc il existe un sous-groupe $N \triangleleft G$ tel que G/N soit isomorphe à $C_3 \times C_3$, on a donc $\sigma(G/N) = \sigma(C_3 \times C_3)$.
En utilisant le lemme 1.3.4, nous savons que $\sigma(C_3 \times C_3) = 3 + 1 = 4$.
Ainsi, d'après le lemme 1.3.3, $\sigma(G) \leq \sigma(G/N) = \sigma(C_3 \times C_3) = 4$.
Mais, avec le théorème 2.1.1 et $\sigma(G) \neq 3$, il ne reste qu'une possibilité : $\sigma(G) = 4$.
Nous supposons que G admet S_3 comme quotient, donc il existe un sous-groupe $N \triangleleft G$ tel que G/N soit isomorphe à S_3, on a donc $\sigma(G/N) = \sigma(S_3)$.
En utilisant la proposition 1.2.1, nous savons que $\sigma(S_3) = 4$.
Ainsi, d'après le lemme 1.3.3, $\sigma(G) \leq \sigma(G/N) = \sigma(S_3) = 4$.
Mais, avec le théorème 2.1.1 et $\sigma(G) \notin 3$, il ne reste qu'une possibilité : $\sigma(G) = 4$.

■

Théorème 2.2.2 (Cohn, 1993)**.** Soit G un groupe. Alors $\sigma(G) = 5$ si et seulement si $\sigma(G) \notin \{3, 4\}$ et G admet A_4 comme quotient.

Démonstration.
Commençons par montrer le sens direct, nous allons utiliser la stratégie suivante :

$$\begin{aligned}[\sigma(G) = 5] &\Rightarrow [\exists\ A < G \text{ tels que } |G/A| = 3] \\ &\Rightarrow [\exists\ N \triangleleft G \text{ tel que } G/N \simeq A_4]\end{aligned}$$

Notons $G = H_1 \cup \ldots \cup H_5$ où H_1, ..., H_5 sont 5 sous-groupes propres tels que $|H_1| \geq \ldots \geq |H_5|$, et donc tels que $i_1 \leq i_2 \leq i_3 \leq i_4 \leq i_5$.

En utilisant le lemme 1.3.2, on a $i_2 \leq \sigma(G) - 1 = 5 - 1 = 4$. Or, si $i_2 = 2$ nous avons forcément $i_1 = i_2 = 2$, et nous nous retrouvons dans le cas de la démonstration du théorème 2.1.2 et on aurait donc $\sigma(G) = 3$, absurde. Ainsi, $i_2 \in \{3, 4\}$.

Si $i_2 = 4$, alors on a démontré la première implication, il suffit de poser $A = H_2$.

Si $i_3 = 3$, avec le théorème 1.3.1, on a $|G| \leq |H_2| + |H_3| + |H_4| + |H_5|$ et donc $1 \leq \frac{1}{i_2} + \frac{1}{i_3} + \frac{1}{i_4} + \frac{1}{i_5}$. Or, $3 = i_2 \leq i_3 \leq i_4 \leq i_5$, donc on a forcément $i_3 \in \{3, 4\}$. Mais si $i_3 = 3$ nous nous retrouvons dans le cas de la démonstration du théorème 2.2.1 et on aurait $\sigma(G) = 4$, absurde. Ainsi $i_3 = 4$.

On a donc démontré la première implication, il suffit de poser $A = H_3$.

$$\begin{array}{lccccccc} \text{Notons} & \pi : & G & \to & S_{G/A} & & & \\ & & g & \mapsto & \pi_g : & G/A & \to & G/A \\ & & & & & hA & \mapsto & ghA \end{array}$$

Nous avons $|G/A| = 4$ donc $S_{G/A} \simeq S_4$.

Notons K le noyau de π, $K = \ker(\pi) \triangleleft G$. Nous avons $K \subset A$, ($g \in K \Rightarrow \forall\ h \in G,\ ghA = hA \Rightarrow$ pour $h = e_G,\ gA = A \Rightarrow g \in A$). Avec le premier théorème d'isomorphisme, nous avons donc $G/K \simeq \mathrm{Im}(\pi)$.

Le but va donc être de montrer que $\mathrm{Im}(\pi) \simeq A_4$. Nous savons déja que $\mathrm{Im}(\pi)$ est isomorphe à un sous-groupe de S_4, mais lequel ?

Nous savons que $|\mathrm{Im}(\pi)|$ divise $24 = |S_4|$.

- $|\mathrm{Im}(\pi)| = 1 \Rightarrow G = K \Rightarrow G \subset A$, absurde.
- $|\mathrm{Im}(\pi)| = 2 \Rightarrow |G/K| = 2 \Rightarrow |K| = \frac{4}{2}|A|$, or $K \subset A$, absurde.
- $|\mathrm{Im}(\pi)| = 3 \Rightarrow |G/K| = 3 \Rightarrow |K| = \frac{4}{3}|A|$, or $K \subset A$, absurde.
- $|\mathrm{Im}(\pi)| = 4 \Rightarrow |G/K| = 4 \Rightarrow G/K \simeq C_2 \times C_2$ ou C_4, or $\sigma(G) \leq \sigma(G/K)$ et $\sigma(C_2 \times C_2) = 3$ d'après le lemme 1.3.4 $\Rightarrow G/K \simeq C_4$, absurde.
- $|\mathrm{Im}(\pi)| = 6 \Rightarrow |G/K| = 6$, or $A/K < G/K$ et $[G/K : A/K] = |G/A| = 4 \Rightarrow |G/A| = 4$ divise $6 = |G/K|$, absurde.
- $|\mathrm{Im}(\pi)| = 8 \Rightarrow |G/K| = 8 = 2^3 \Rightarrow$ par le théorème 1.3.6, $\sigma(G/K) = 2 + 1 = 3 \Rightarrow$ par le lemme 1.3.3, on a $5 = \sigma(G) \leq \sigma(G/K) = 3$, absurde.
- $|\mathrm{Im}(\pi)| = 24 \Rightarrow |G/K| = 24$ et $G/K \simeq S_4 \Rightarrow [G/K : G/A] = 24/4 = 6$ et $(G/K)/(G/A) \simeq S_3 \Rightarrow$ par le lemme 1.3.3, on a $\sigma(G/K) = \sigma(S_4) = 5 < 4 = \sigma(S_3) = \sigma((G/K)/(G/A))$, absurde.

Donc nous avons forcément $|\mathrm{Im}(\pi)| = 12$. Et le seul sous-groupe de S_4 d'ordre 12, est A_4. Donc, $\mathrm{Im}(\pi) \simeq A_4$, et ainsi $G/K \simeq A_4$.

Le sens direct est démontré, montrons le sens indirect.
Nous supposons que G admet A_4 comme quotient, donc il existe un sous-groupe $N \triangleleft G$ tel que G/N soit isomorphe à A_4, on a donc $\sigma(G/N) = \sigma(A_4)$.
En utilisant le lemme 1.2.2, nous savons que $\sigma(A_4) = 5$.
Ainsi, d'après le lemme 1.3.3, $\sigma(G) \leq \sigma(G/N) = \sigma(A_4) = 5$.
Mais, avec le théorème 2.1.1 et $\sigma(G) \notin \{3, 4\}$, il ne reste qu'une possibilité : $\sigma(G) = 5$.

■

2.3 Cas 6 et 7

Dans cette section nous traiterons les cas $\sigma(G) = 6$ et 7. Commençons par introduire un groupe qui sera utile pour la suite.

Nous noterons W le produit semi-direct $C_5 \rtimes C_4$ d'ordre 20 engendré par a et b vérifiant $a^5 = b^4 = e, ba = a^2b$.

Théorème 2.3.1 (Cohn, 1993)**.** Soit G un groupe. Alors $\sigma(G) = 6$ si et seulement si $\sigma(G) \notin \{3, 4, 5\}$ et G admet $C_5 \times C_5$ ou D_5 ou W comme quotient.

Démonstration.
Commençons par montrer le sens direct, nous allons utiliser la stratégie suivante :

$$\begin{aligned}[\sigma(G)=6] &\Rightarrow [i_1 \in \{2,5\} \text{ et } i_2=i_3=i_4=i_5=i_6=5] \\ &\Rightarrow [\exists\, X < G \text{ tel que } G/X \simeq D_5 \text{ ou } W \text{ ou } C_5 \times C_5]\end{aligned}$$

Notons $G = H_1 \cup \ldots \cup H_6$ où H_1, ..., H_6 sont 6 sous-groupes propres tels que $|H_1| \geq \ldots \geq |H_6|$, et donc tels que $i_1 \leq \ldots \leq i_6$.

Montrons dans un premier temps que $i_1 \in \{2,5\}$ et que $i_2 = i_3 = i_4 = i_5 = i_6 = 5$. Si nous avons deux sous-groupes d'indice 2, alors nous nous retrouvons dans le cas de la démonstration du théorème 2.1.2, et on aurait $\sigma(G) = 3$, absurde. Si nous avons deux sous-groupes d'indice 3, alors nous nous retrouvons dans le cas de la démonstration du théorème 2.2.1, et on aurait $\sigma(G) = 4$, absurde. Si nous avons un sous-groupe d'indice 4, alors nous nous retrouvons dans le cas de la démonstration du théorème 2.2.2, et on aurait $\sigma(G) = 5$, absurde. Ainsi, il n'y a pas de sous-groupe d'indice 4, et au plus un sous-groupe d'indice 2 ou 3, et donc $i_3 \geq 5$.

Si $i_1 = 2$ et $i_2 = 3$, alors $H_1 \lhd G$ (sous-groupe d'indice 2) et $H_2 \lhd G$ (tous les conjugués de H_2 ont le même indice que H_2, mais nous venons de voir que c'est le seul sous-groupe d'indice 3, ainsi son seul conjugué est lui-même). En écrivant $G = \left(\bigcup_{r=1}^{2} H_r\right) \cup \left(\bigcup_{r=3}^{6} H_r\right)$, nous pouvons utiliser le lemme 1.3.8, rappelons que $5 \leq i_3 \leq \ldots \leq i_6$, et donc

$$|G| \leq \sum_{r=3}^{6} |H_r| \quad \Rightarrow \quad 1 \leq \sum_{r=3}^{6} \frac{1}{i_r} \quad \Rightarrow \quad 1 \leq \sum_{r=3}^{6} \frac{1}{5} = \frac{4}{5} < 1$$

Ce qui est absurde, nous pouvons donc écarter le cas $(i_1, i_2) = (2,3)$, ainsi $i_2 \geq 5$.

En appliquant le théorème 1.3.1, nous avons $|G| \leq \sum_{k=2}^{6} |H_k|$ et donc $1 \leq \sum_{k=2}^{6} \frac{1}{i_k}$. Or, $5 \leq i_2 \leq \ldots \leq i_6$, donc on a forcément $i_2 = \ldots = i_6 = 5$.

Il reste à traiter i_1, nous savons déjà que $i_1 \in \{2,3,5\}$, il reste donc à montrer que le cas $i_1 = 3$ est impossible. Supposons que $i_1 = 3$, alors $H_1 \lhd G$ (tous les conjugués de H_1 ont le même indice que H_1, mais nous avons vu que c'est le seul sous-groupe d'indice 3, ainsi son seul conjugué est lui-même). Comme $|G| = \sum_{k=2}^{6} |H_k|$, le théorème 1.3.1 nous donne $H_2 \cap H_3 \subset H_1$. D'où, $i_1 = 3$ divise $i(H_2 \cap H_3)$, mais nous savons également que $H_2 \cap H_3 \subset H_2$ et donc $i_2 = 5$ divise $i(H_2 \cap H_3)$, ainsi 15 divise $i(H_2 \cap H_3)$. De plus, comme $i_2 = i_3 = 5$,

$$|H_2 \cap H_3| = \frac{|H_2||H_3|}{|H_2H_3|} = \frac{|H_2||H_3||G||G|}{|G||G|H_2H_3|} + \frac{1}{i_2}\frac{1}{i_3}\frac{|G|}{|H_2H_3|}|G| = \frac{|G|}{25}\frac{|G|}{|H_2H_3|} \geq \frac{|G|}{25}$$

Et donc, $i(H_2 \cap H_3) \leq 25$, ainsi $i(H_2 \cap H_3) = 15$. Puisque $H_1 \lhd G$ et que H_1 et H_2 sont maximaux, nous avons également

$$i(H_1 \cap H_2) = \frac{|G|}{|H_1 \cap H_2|} = \frac{|G||H_1H_2|}{|H_1||H_2|} = i_1 i_2 \frac{|H_1H_2|}{|G|} = i_1 i_2 = 15$$

Posons $X = H_2 \cap H_3 = H_1 \cap H_2$ (nous venons de voir que le sous-groupe de gauche est inclus dans celui de droite et que les deux sous-groupes ont le même indice, de la même façon $X = H_1 \cap H_3$), comme $H_1 \lhd G$, alors $X \lhd H_2$, de la même façon on a également

$X \triangleleft H_3$. Or, H_2 et H_3 engendrent G en tant que sous-groupes maximaux, et donc $X \triangleleft G$.

Regardons le groupe G/X, nous savons que $|G/X| = i(H_1 \cap H_2) = 15$.
• Montrons que G/X est cyclique. Notons n_5 le nombre de 5-Sylow de G/X, alors d'après les théorèmes de Sylow, nous avons $n_5 \equiv 1 \pmod 5$ et n_5 divise 3, ainsi $n_5 = 1$. Notons K l'unique 5-Sylow, alors $K \triangleleft G/X$ et $K \simeq C_5$. Soit L un 3-Sylow, qui existe d'après les théorèmes de Sylow, $L \simeq C_3$. Nous avons alors

1. $K \triangleleft G/X$, $L < G/X$
2. $K \cap L = \{e_{G/X}\}$, car $x \in K \cap L \Rightarrow \nu(x)$ divise 3 et 5
3. $|K||L| = 15 = |G/X|$

Nous pouvons donc affirmer que $G/X \simeq K \rtimes L$. Or, les différents produits semi-directs sont définis par les morphismes $\pi : C_3 \to \mathrm{Aut}(C_5) \simeq C_4$, mais 3 ne divise pas 4, il n'y a donc que le morphisme trivial. Et donc le produit semi-direct et en fait un produit direct, ainsi $G/X \simeq K \times L \simeq C_5 \times C_3 \simeq C_{15}$ (le dernier isomorphisme provient du Lemme chinois, $3 \wedge 5 = 1$), et donc G/X est cyclique.
• Montrons maintenant que $\sigma(G/X) \leq 6$, pour cela posons $\pi : G \to G/X, g \mapsto gX$. Or, $G = \bigcup_{i=1}^{6} H_i$ donc $G/X = \bigcup_{i=1}^{6} \pi(H_i)$; il reste à montrer que les $\pi(H_i)$ sont des sous-groupes propres de G/X.
- Premièrement, $\pi(H_i) = G/X \Leftrightarrow \{\pi(h) \mid h \in H_i\} = G/X$
$\Leftrightarrow \{hX \mid h \in H_i\} = G/X$
$\Leftrightarrow \{hX \mid h \in H_i\} = \{gX \mid g \in G\}$
$\Leftrightarrow G \subset H_i$

Ce qui est impossible car H_i est un sous-groupe propre de G ; donc $\pi(H_i) \neq G/X$.
- De même, $\pi(H_i) = \{X\} \Leftrightarrow \{\pi(h) \mid h \in H_i\} = \{X\}$
$\Leftrightarrow \{hX \mid h \in H_i\} = \{X\}$
$\Leftrightarrow H_i \subset X$
$\Leftrightarrow H_i \subset H_i \cap H_1$
$\Leftrightarrow H_i \subset H_1$

Ce qui est impossible car $\sigma(G) = 6$; donc $\pi(H_i) \neq \{X\}$.
Ainsi, G/X est union de 6 sous-groupes propres, mais nous ne savons pas si 6 est le plus petit entier vérifiant cela. Donc $\sigma(G/X) \leq 6$.

Nous avons donc démontrer deux choses sur le groupe G/X, qui sont :

- G/X est cyclique
- $\sigma(G/X) \leq 6$

Ce qui, d'après la proposition 1.1.5, est absurde. Ainsi i_1 ne peut pas être égale à 3. Nous avons donc démontré la premiére implication, en effet nous avons forcément $i_1 \in \{2, 5\}$ et $i_2 = i_3 = i_4 = i_5 = i_6 = 5$.

Cas n°1 : Supposons que $i_1 = 2$.
Soient $r, s \in \{2, \ldots, 6\}$ tels que $r \neq s$. Comme H_1 est d'indice 2 dans G, alors $H_1 \triangleleft G$ et avec le théorème 1.3.1, nous avons $H_r \cap H_s \subset H_1$. D'où, $i_1 = 2$ divise $i(H_r \cap H_s)$, mais nous savons également que $H_r \cap H_s \subset H_r$ et donc $i_r = 5$ divise $i(H_r \cap H_s)$, ainsi 10 divise $i(H_r \cap H_s)$. De plus

$$|H_r \cap H_s| = \frac{|H_r||H_s|}{|H_r H_s|} = \frac{|H_r||H_s||G||G|}{|G||G|H_r H_s|} + \frac{1}{i_r}\frac{1}{i_s}\frac{|G|}{|H_r H_s|}|G| = \frac{|G|}{25}\frac{|G|}{|H_r H_s|} \geq \frac{|G|}{25}$$

Et donc, $i(H_r \cap H_s) \leq 25$, ainsi $i(H_r \cap H_s) = 10$ ou 20. Puisque $H_1 \triangleleft G$, nous avons également

$$i(H_1 \cap H_r) = \frac{|G|}{|H_1 \cap H_r|} = \frac{|G||H_1 H_r|}{|H_1||H_r|} = i_1 i_2 \frac{|H_1 H_r|}{|G|} = i_1 i_r = 15$$

Nous venons donc de montrer que pour tout $r, s \in \{2 \dots, 6\}$ tels que $r \neq s$, nous avons

$$i(H_1 \cap H_r) = 10 \text{ et } i(H_r \cap H_s) = 10 \text{ ou } 20$$

Nous avons alors maintenant deux sous-cas.

Sous-cas n°1 : Supposons qu'il existe un couple $r, s \in \{2 \dots, 6\}$ tels que $r \neq s$ et $i(H_r \cap H_s) = 10$. Posons $X = H_r \cap H_s$, alors

$$\frac{|H_2|}{|X|} = \frac{|H_2|/|G|}{|X|/|G|} = \frac{1/i_2}{1/i(X)} = \frac{1/5}{1/10} = 2$$

D'où, X est d'indice 2 dans H_2, et donc $X \triangleleft H_2$. Nous procédons de la même façon pour montrer que $X \triangleleft H_3$. Et puisque H_2 et H_3 engendrent G (ce sont deux sous-groupes maximaux), $X \triangleleft G$. Regardons donc le groupe G/X, nous savons que $|G/X| = i(X) = 10$, et que H_2/X et H_3/X sont deux sous-groupe d'ordre 2. Ainsi, G/X est un groupe d'ordre 10 qui n'est pas cyclique, montrons qu'on a forcément $G \simeq D_5$. Notons n_5 le nombre de 5-Sylow de G/X, alors d'après les Théorèmes de Sylow, nous avons $n_5 \equiv 1 \pmod 5$ et n_5 divise 2, ainsi $n_5 = 1$. Notons K l'unique 5-Sylow, alors $K \triangleleft G/X$ et $K \simeq C_5$. Soit L un 2-Sylow, qui existe d'après les Théorèmes de Sylow, $L \simeq C_2$. Nous avons alors

1. $K \triangleleft G/X$, $L < G/X$
2. $K \cap L = \{e_{G/X}\}$, car $x \in K \cap L \Rightarrow \nu(x)$ divise 2 et 5
3. $|K||L| = 10 = |G/X|$

Nous pouvons donc affirmer que $G/X \simeq K \rtimes L$. Or, les différents produits semi-directs sont définis par les morphismes $\pi : C_2 \to \mathrm{Aut}(C_5) \simeq C_4$, mais C_4 possède deux éléments d'ordre divisant 2, qui sont 0 et 2, ainsi $\pi(1) = 0$ ou 2. Mais G/X n'est pas cyclique donc $\pi(1) \neq 0$ (sinon on aurait $G/X \simeq C_{10}$), et ainsi $\pi(1) = 2$. Nous venons donc de voir qu'il n'y a que deux groupes d'ordre 10 (à isomorphisme près), le groupe cyclique et un autre, mais le groupe diédral D_{10} est d'ordre 10 mais n'est pas cyclique, il est donc forcément isomorphe à cet autre groupe définit par le produit semi-direct $\pi(1) = 2$. Ainsi, $G/X \simeq D_5$. Le premier sous-cas est démontré.

Sous-cas n°2 : Supposons que pour tout $r, s \in \{2 \dots, 6\}$ tels que $r \neq s$, nous avons $i(H_r \cap H_s) = 20$. Ici, $1 = \sum_{k=2}^{6} \frac{1}{i_k}$, d'où $|G| = \sum_{k=2}^{6} |H_k|$, et donc en appliquant le théorème 1.3.1, $H_2 \cap H_3 \subset H_1$. Posons $B_2 = H_1 \cap H_2$, $B_3 = H_1 \cap H_3$ et $X = B_2 \cap B_3$.

$$\frac{|B_2|}{|X|} = \frac{|B_2|/|G|}{|X|/|G|} = \frac{1/i(B_2)}{1/i(X)} = \frac{1/i(H_1 \cap H_2)}{1/i(H_2 \cap H_3)} = \frac{1/10}{1/20} = 2$$

D'où, X est d'indice 2 dans B_2, et donc $X \triangleleft B_2$. Nous procédons de la même façon pour montrer que $X \triangleleft B_3$. Et puisque B_2 et B_3 engendrent H_1 (ce sont deux sous-groupes maximaux), $X \triangleleft H_1$. Posons $N_G(X) = \{g \in G \mid gXg^{-1} = X\}$, le normalisateur de X dans G. Nous venons de voir que $H_1 \triangleleft X$, donc $H_1 \subset N_G(X)$. Or, H_1 est un sous-groupe maximal de G, ainsi $N_G(X) = H_1$ ou G. Supposons que $N_G(X) = H_1$, alors X possède

$i(N_G(X)) = i(H_1) = 2$ conjugués dans G, notons les X et Y. Alors, $H_2 \not\lhd X$, sinon $X \lhd G$ (et donc $N_G(X) = G$) puisque H_1 et H_2 engendrent G, ainsi il existe $b \in H_2$ tel que $bXb^{-1} \neq X$ et donc $bXb^{-1} = Y$. Ainsi, $X \subset H_2$ implique que $Y \subset H_2$, de la même façon nous avons $Y \subset H_3$, et donc $Y \subset H_2 \cap H_3 = X$ (car $H_1 \subset H_2 \cap H_3$), ce qui est absurbe, nous avons donc $N_G(X) = G$. Regardons donc le groupe G/X, que nous noterons $K = G/X$ pour la suite, nous savons que $|K| = |G/X| = i(X) = 20$, et que H_2/X et H_3/X sont deux sous-groupe d'ordre 4. Ainsi, K est un groupe d'ordre 20 qui n'est pas cyclique, montrons qu'on a forcément $K \simeq W$. Notons n_5 le nombre de 5-Sylow de K, alors d'après les théorèmes de Sylow, nous avons $n_5 \equiv 1 \pmod 5$ et n_5 divise 4, ainsi $n_5 = 1$. Notons F l'unique 5-Sylow, alors $F \lhd K$ et $F \simeq C_5$. Nous savons que $|K/F| = 20/5 = 4$, donc $K/F \simeq C_4$ ou $C_2 \times C_2$. Si $K/F \simeq C_2 \times C_2$, alors en utilisant deux fois le lemme 1.3.3, et le fait que $\sigma(C_2 \times C_2) = 3$, nous avons

$$6 = \sigma(G) \leq \sigma(G/X) = \sigma(K) \leq \sigma(K/F) = \sigma(C_2 \times C_2) = 3$$

Ce qui est absurde, ainsi $K/F \simeq C_4$. Notons a le générateur de F tel que $a^5 = e$ et Fb le générateur de K/F tel que $b^4 = e$, ainsi $F = \{e, a, a^2, a^3, a^4\}$ et $K/F = \{e, Fb, Fb^2, Fb^3\}$. Comme $F \lhd K$, on a $bab^{-1} \in F$ et donc $ba \in Fb$, regardons donc les différentes valeur possibles de ba. Clairement $ba \neq b$ (les deux éléments n'ont pas le même ordre) et $ba \neq ab$ (sinon K serait cyclique), il reste donc trois valeurs possibles.

- $ba = a^2b$, alors par la définition de W, on a $K \simeq W$.
- $ba = a^3b$, en posant $c = b^3$ on a $ca = a^2c$, et alors par la définition de W, on a $K \simeq W$ (Fc est un générateur de K/F).
- $ba = a^4b$, alors en posant $L = \{e, b^2\}$, on peut verifier (à la main) que $L \lhd K$, et donc K/L est groupe d'ordre 10 non-cyclique, ainsi $K/L \simeq D_5$ (démontrer dans le sous-cas n°1).

Cas n°2 : Supposons $i_1 = 5$.
Nous ne démontrerons pas ce cas, la conclusion étant G admet $C_5 \times C_5$ comme quotient.

Le sens direct est démontré

Montrons maintenant le sens indirect.
Nous supposons que G admet $C_5 \times C_5$ comme quotient, donc il existe un sous-groupe $N \lhd G$ tel que G/N soit isomorphe à $C_5 \times C_5$, on a donc $\sigma(G/N) = \sigma(C_5 \times C_5)$.
En utilisant le lemme 1.3.4, nous savons que $\sigma(C_5 \times C_5) = 5 + 1 = 6$.
Ainsi, d'après le lemme 1.3.3, $\sigma(G) \leq \sigma(G/N) = \sigma(C_5 \times C_5) = 6$.
Mais, avec le théorème 2.1.1 et $\sigma(G) \notin \{3, 4, 5\}$, il ne reste qu'une possibilité : $\sigma(G) = 6$.
Nous supposons que G admet D_5 comme quotient, donc il existe un sous-groupe $N \lhd G$ tel que G/N soit isomorphe à D_5, on a donc $\sigma(G/N) = \sigma(D_5)$.
En utilisant la proposition 1.2.3, nous savons que $\sigma(D_5) = 6$.
Ainsi, d'après le lemme 1.3.3, $\sigma(G) \leq \sigma(G/N) = \sigma(D_5) = 6$.
Mais, avec le théorème 2.1.1 et $\sigma(G) \notin \{3, 4, 5\}$, il ne reste qu'une possibilité : $\sigma(G) = 6$.
Nous supposons que G admet W comme quotient, donc il existe un sous-groupe $N \lhd G$ tel que G/N soit isomorphe à W, on a donc $\sigma(G/N) = \sigma(W)$.
De la mêm façon que pour les autres groupes, nous avons $\sigma(W) = 6$.
Ainsi, d'après le lemme 1.3.3, $\sigma(G) \leq \sigma(G/N) = \sigma(W) = 6$.
Mais, avec le théorème 2.1.1 et $\sigma(G) \notin \{3, 4, 5\}$, il ne reste qu'une possibilité : $\sigma(G) = 6$.

■

Le cas suivant, $\sigma(G) = 7$, devient considérablement plus lourd, impliquant de vastes détails et plusieurs pages d'argumentations. Mais au final, la réponse est amusante et plutôt inattendu. Cohn [1] a conjecturé, et en 1997 Tomkinson [3] a prouvé :

Théorème 2.3.2 (Tomkinson, 1997)**.** Il n'existe pas de groupe G tel que $\sigma(G) = 7$.

La preuve du théorème de Tomkinson était en effet très compliquée et nécessitait l'analyse de nombreux cas. Ainsi l'idée de classer les groupes qui sont l'union de n des sous-groupes appropriés pour n supérieur serait sans aucun doute une tâche formidable, car il semble qu'il n'y ai pas de modèle cohérent pour les petits n qui suggère une réponse générale.

3 Extension des hypothèses

3.1 Groupes comme union de sous-groupes propres distingués

Comme mentionné dans la section précédente, la situation devient de plus en plus compliquée lorsque le groupe G est l'union d'un plus grand nombre de sous-groupes. Peut-être que cela indique que nous n'avons pas posé tout à fait la bonne question en généralisant le résultat de Scorza ! Notez que notre preuve du théorème de Scorza implique le résultat suivant.

Théorème 3.1.1. Un groupe qui union de trois sous-groupes propres est un fait union de trois sous-groupes propres distingués.

On peut donc ajouter le mot distingué au résultat de Scorza, et cela reste vrai ! Cela suggère que l'on pourrait se demander : quand un groupe est-il l'union de sous-groupes propres distingués ?

Similairement à la définition 1.1.4, écrivons $\eta(G) = n \in \mathbb{N}^*$, si G est l'union de n sous-groupes propres distingués, mais n'est pas l'union de moins de n sous-groupes propres distingués.

Alors la réponse à cette nouvelle question, concernant le moment où $\eta(G) = n$, donne une autre jolie généralisation du théorème de Scorza. Dans les théorèmes du chapitre 2, nous avons prouvé :

Théorème 3.1.2. Soit G un groupe qui est union de sous-groupes propres distingués. Alors $\eta(G) = p+1$, où p est le plus petit premier tel que G possède un quotient isomorphe à $C_p \times C_p$, si un tel p existe ; sinon $\eta(G) = +\infty$.

Le théorème 3.1.2 nous donne une belle caractérisation des groupes qui sont union de sous-groupes propres distingués.

Corollaire 3.1.3. Un groupe est union de sous-groupes propres distingués si et seulement si il possède un quotient isomorphe à $C_p \times C_p$ pour un premier p.

3.2 Groupe comme union conjuguée de sous-groupes propres

Un autre question intéressante que l'on peut se poser, qui a des applications à la théorie de Galois, est la suivante : quand un groupe peut-il être couvert par les conjugués de n sous-groupes propres ?

Plus précisément, nous disons que G est l'union conjuguée de sous-groupes $A_1, \cdots, A_n$ si c'est l'union des conjugués d'un sous-groupes A_i pour $i = 1, \ldots, n$. De façon équivalente, G est l'union conjuguée de sous-groupes $A_1, \cdots, A_n$ si l'union $\bigcup_{i=1}^{n} A_i$ intersecte toutes les classes de conjuguaisons de G.

La première question qui se pose dans ce contexte est de savoir si un groupe G peut être l'union conjugué d'un sous-groupe propre. En d'autres termes : est-il possible pour un sous-groupe propre de G de contenir au moins un élément de chaque classe de conjugaison de G.

Pour des groupes infinis, il est possible qu'un groupe soit l'union conjuguée d'un sous-groupe. Par exemple, le groupe $GL_n(\mathbb{C})$ est l'union conjuguée du sous-groupe des matrices triangulaires supérieures, car chaque matrice $n \times n$ est conjuguée à une matrice triangulaire supérieure. Mais restons dans le cas des groupes finis.

Théorème 3.2.1. Un groupe fini ne peut pas s'écrire comme union des conjugués d'un sous-groupe propre.

Démonstration.
Soit G un groupe. Supposons que G peut s'écrire comme union des conjugués d'un sous-groupe propre A, notons $G = \bigcup_{k=1}^{n} A_k$ où les A_k sont les conjuqués de A. Evidemment $n > 1$ (A est un sous-groupe propre, donc $A = A_1 \neq G$). Notons $N_G(A) = \{g \in G \mid gAg^{-1}\}$ le normalisateur de A dans G, alors le nombre de conjugués de A dans G est $n = i(N_G(A)) = |G/N_G(A)|$. Or, $A \subset N_G(A)$, donc $|A| \leq |N_G(A)|$, d'où $n = |G/N_G(A)| \leq |G/A|$. Nous allons maintenant regarder le nombre d'éléments dans l'union $\bigcup_{k=1}^{n} A_k$, rappelons que l'élément neutre e_G est dans chaque A_k, ainsi

$$\left|\bigcup_{k=1}^{n} A_k\right| \leq \sum_{k=1}^{n} |A_k| - (n-1) = n|A| - (n-1) \leq |G/A||A| - (n-1) = |G| - (n-1) < |G|$$

Ce qui est absurde, donc G ne peut pas s'écrire comme union des conjugués d'un sous-groupe propre.

■

Il semble donc clair à première vue qu'il ne devrait pas être difficile d'écrire divers groupes comme l'union conjuguée de deux sous-groupes propres. Par exemple, le groupe

symétrique S_3 est l'union conjuguée de deux de ses sous-groupes d'indice 2 et 3 respectivement. Cependant, la question reste ouverte, déterminer quels groupes sont l'union conjuguée de deux sous-groupes propres !

Similairement à la définition 1.1.4, écrivons $\xi(G) = n \in \mathbb{N}^*$, si G est l'union conjuguée de n sous-groupes propres distingués, mais n'est pas l'union de moins de n sous-groupes propres distingués. Nous établissons ci-dessous quelques conditions nécessaires et suffisantes pour $\xi(G) = 2$.

Théorème 3.2.2. Soit G un groupe. Si G peut s'écrire comme l'union des conjugués de deux sous-groupes propres, alors G possède un sous-groupe maximal qui n'est pas distingué.

Démonstration.
Supposons que G peut s'écrire comme union des conjugués de deux sous-groupes propres A et B. Sans perdre de généralités, nous pouvons supposer A et B maximaux, quitte à les remplacer par des sous-groupes propres plus grand. Si A et B sont distingués dans G, alors leurs seuls conjugués sont eux-mêmes et d'après l'hypothèse, nous avons $G = A \cup B$, ce qui contredit le Théorème 2.1.2. Si un des deux sous-groupes propres maximaux A ou B n'est pas distingués dans G, alors nous avons le résultat voulu.

■

Le théorème 3.2.2 exclut immédiatement un certain nombre de possibilités pour G si l'on veut avoir $\xi(G) = 2$. Évidemment, G ne peut pas être abélien. De plus, on vérifie par exemple que le groupe diédral D_4 d'ordre 8 a la propriété que tout sous-groupe maximal est d'indice 2 et donc distingué. Nous avons donc $\xi(D_4) > 2$. En fait on a $\xi(D_4) = 3$, d'où l'égalité intéressante : $\sigma(D_4) = \eta(D_4) = \xi(D_4) = 3$.

Plus généralement, un groupe fini dans lequel chaque sous-groupe maximal est normal est appelé un groupe nilpotent. Ainsi le Théorème 3.2.2 implique que si G est nilpotent, alors $\xi(G) > 2$.

Dans le cas de groupes finis résolubles G, la question de savoir si G est l'union conjuguée de deux sous-groupes propres n'est pas totalement étrangère à la question que nous avons considérée dans la section précédente, à savoir si G peut être exprimé comme l'union de sous-groupes propres distingués !

Comme souligné dans les travaux de Jamali et Mousavi [4], les techniques de Cohn et Tomkinson, dans leurs travaux sur les groupes solubles, impliquent une approche très subtile entre les unions de sous-groupes distingués et les unions conjuguées de deux sous-groupes. En particulier, Jamali et Mousavi en déduisent ce qui suit :

Théorème 3.2.3 (Jamali-Mousavi)**.** Soit G un groupe non-cyclique résoluble. Alors, soit G est union de sous-groupes propres distingués, soit G est union de deux sous-groupes propres conjugués.

Leurs techniques, qui suivent les méthodes de Cohn et Tomkinson, ne sont pas naturelles permettent de séparer les deux conditions, néanmoins !

Notre théorème 3.1.2 et son corollaire séparent la première condition. Ainsi nous pouvons donner diverses conditions suffisantes pour qu'un groupe fini résoluble soit l'union conjuguée de deux sous-groupes propres. Par exemple, en combinant le corollaire 3.1.3 et le théorème 3.2.3, on peut facilement obtenir :

Corollaire 3.2.4. Soit G un groupe résoluble. Supposons que G possède un quotient K

tel que : K n'est pas cyclique, et K n'a pas de quotient isomorphe à $C_p \times C_p$ pour tout premier p. Alors G est union de deux sous-groupes propres conjugués.

Démonstration.
Le groupe G est résoluble, donc son quotient K est résoluble. Par hypothèse, K n'est pas cyclique, on peut donc appliquer le théorème 3.2.3 pour le groupe K. Donc, soit K est union de sous-groupes propres distingués, soit K est union de deux sous-groupes propres conjugués. Or, par hypothèse K n'a pas de quotient isomorphe à $C_p \times C_p$ pour tout premier p, donc avec le corollaire 3.1.3, K ne peut pas être union de sous-groupes propres distingués.

■

Bibliographie

[1] J.H.E. Cohn, *On n-sum groups*. Mathematica Scandinavica, 1994, Vol. 75 No. 1 (1994), pp. 44-58

[2] Mira Bhargava, *Groups as unions of proper subgroups*. The American Mathematical Monthly, May, 2009, Vol. 116, No. 5 (May, 2009), pp. 413-422

[3] M.J. Tomkinson, *Groups as the unions of proper subgroups*. Mathematica Scandinavica, 1997, Vol. 81, pp. 191-198

[4] A. Jamah et H. Mousavi,, *The structure of $G/\Phi(G)$ for finite non-nilpotent soluble groups G*. The 31st Iranian Mathematics Conference, University of Tehran, 2000

[5] Daniel Perrin, *Cours d'algèbre*. Ellipses, Collection CAPES/Agrégation, 1996