

FEUILLE TD 1 – CORRECTION PARTIELLE – GROUPES

EXERCICE 1 – GROUPE SYMÉTRIQUE. Soit \mathfrak{S}_n le groupe symétrique sur n lettres.

1. Quel est l'ordre maximal d'un élément de \mathfrak{S}_3 ? de \mathfrak{S}_4 ? de \mathfrak{S}_5 ? de \mathfrak{S}_n ?
2. Donner le treillis¹ des sous-groupes de \mathfrak{S}_3 , en précisant à chaque fois lesquels des sous-groupes sont distingués. Répéter l'exercice avec le groupe alterné \mathfrak{A}_4 .
Soient G un groupe et $K \subseteq H$ deux sous-groupes de G . On suppose que $K \triangleleft H$ et que $H \triangleleft G$. A-t-on $K \triangleleft G$? Démontrer que si K est caractéristique dans H et que H est caractéristique dans G , alors K est caractéristique dans G .
3. Une *partition d'un entier* n est une suite $0 < \lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_r$ d'entiers tels que $\sum_{i=1}^r \lambda_i = n$. Montrer que les classes de conjugaison de \mathfrak{S}_n sont en bijection avec les partitions de n .

SOLUTION.

1. Plusieurs façons de faire : décrire tous les éléments de \mathfrak{S}_3 : Id, (12), (13), (23), (123), (132) ou alors en utilisant la décomposition de toute permutation en produit de cycles à supports disjoints dont l'ordre est alors le ppcm des longueurs des cycles² ou encore en utilisant le théorème de Lagrange et le fait que \mathfrak{S}_3 n'est pas cyclique car non abélien. Bref, on trouve 3 pour chacun des deux 3-cycles. De même, pour \mathfrak{S}_4 , on trouve 4 atteint pour les six 4-cycles. Pour \mathfrak{S}_5 , on obtient 6 pour chacun des 20 produits d'une transposition et d'un 3-cycle à supports disjoints. De manière générale, on voit que l'ordre maximal dans \mathfrak{S}_n est donné par

$$g(n) = \max_{\substack{0 < \lambda_1 \leq \dots \leq \lambda_r \\ \lambda_1 + \dots + \lambda_r = n}} \text{ppcm}(\lambda_1, \dots, \lambda_r).$$

On retrouve bien les résultats précédents puisqu'on a les partitions suivantes :

$$3 = 1+1+1 = 1+2 = 3, \quad 4 = 1+1+1+1 = 2+2 = 1+3 = 4 \quad \text{et} \quad 5 = 1+1+1+1+1 = 1+1+1+2 = 1+1+3 = 1+4 = 2+3 = 5.$$

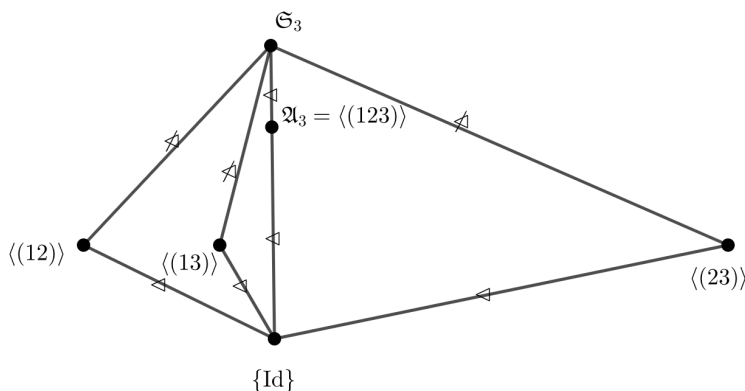
On obtient par le théorème de Lagrange que $g(n) \mid n!$ et g est croissante puisque toute permutation de \mathfrak{S}_n peut être vue comme une permutation de \mathfrak{S}_k pour $k \geq n$. On a par exemple

n	3	4	5	6	7	8	9	10	11	12	13
g(n)	3	4	6	6	12	15	20	30	30	60	60

Landau³ a démontré⁴ en 1903 l'équivalent

$$\log(g(n)) \underset{n \rightarrow +\infty}{\sim} \sqrt{n \log(n)}.$$

2. On obtient facilement le treillis suivant⁵



1. C'est-à-dire le graphe non orienté dont les sommets sont les sous-groupes de G et où une arête relie deux sous-groupes H_1 et H_2 si, et seulement si, $H_1 \subseteq H_2$ ou $H_2 \subseteq H_1$.

2. Car on vérifie immédiatement qu'un cycle de longueur ℓ est d'ordre ℓ et le fait que les cycles soient à support disjoints entraîne qu'ils commutent.

3. On appelle d'ailleurs classiquement cette fonction g la fonction de Landau.

4. En utilisant des résultats d'arithmétique notamment sur la répartition des nombres premiers.

5. Cela se révélera utile quand on verra la théorie de Galois mais aussi dans le cours de géométrie du second semestre quand on classifera les revêtements galoisiens. ! Un treillis est un objet mathématique qui a une définition précise comme ensemble ordonné avec certaines bonnes propriétés qu'on ne précisera pas ici !

car les sous-groupes sont d'ordre 1, 2, 3 ou 6 et les groupes d'ordre 2 et 3 sont nécessairement cycliques. Un groupe d'ordre 2 est alors simplement engendré par un élément d'ordre 2, autrement dit ici une transposition et donc de la forme $\langle(ab)\rangle = \{\text{Id}, (ab)\}$ tandis qu'un sous-groupe d'ordre 3 est engendré par un élément d'ordre 3, autrement dit un 3-cycle et est alors donné par $\langle(abc)\rangle = \{\text{Id}, (abc), (acb)\}$ si bien qu'on a une unique sous-groupe d'ordre 3, à savoir

$$\mathfrak{A}_3 = \langle(123)\rangle = \{\text{Id}, (123), (132)\}.$$

Par ailleurs, on sait que \mathfrak{A}_3 est distingué dans \mathfrak{S}_3 et puisque

$$(abc)(ab)(acb) = (bc)$$

si $\{a, b, c\} = \{1, 2, 3\}$, aucun des sous-groupes d'ordre 2 ne sont distingués⁶ dans \mathfrak{S}_3 .

Passons à \mathfrak{A}_4 . On sait que

$$\mathfrak{A}_4 = \{\text{Id}, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}.$$

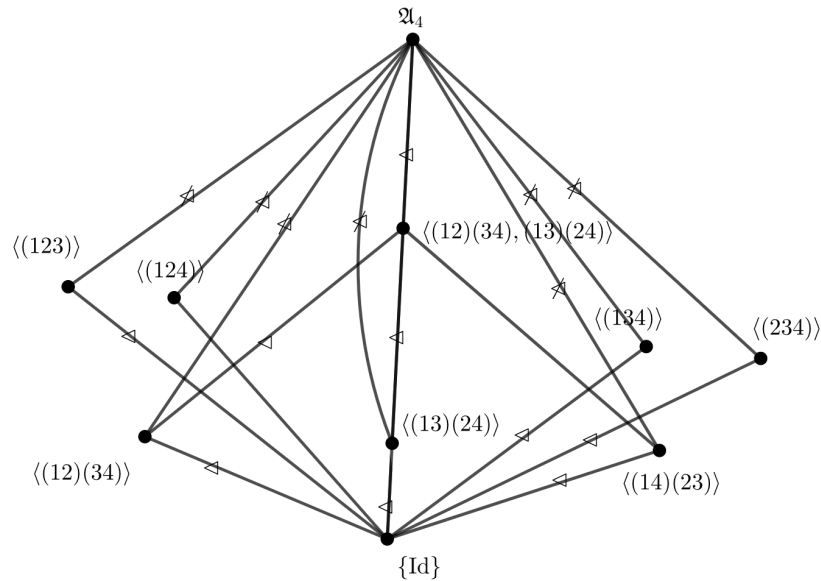
De plus, $\#\mathfrak{A}_4 = 12$ donc les sous-groupes non triviaux sont d'ordre 6, 4, 3 ou 2. Or, on sait qu'un sous-groupe d'ordre 6 est soit cyclique soit isomorphe à \mathfrak{S}_3 . Ici la seule option serait \mathfrak{S}_3 car on n'a pas d'élément d'ordre 6 mais dans \mathfrak{S}_3 aucune paire d'éléments d'ordre 2 ne commutent tandis qu'ici tous les éléments d'ordre 2 commutent⁷

$$(12)(34)(13)(24) = (13)(24)(12)(34).$$

Pour les groupes d'ordre 4, on a deux possibilités $\mathbf{Z}/4\mathbf{Z}$ et $(\mathbf{Z}/2\mathbf{Z})^2$. Ici, pas d'élément d'ordre 4 donc la seule possibilité est la seconde et on voit qu'on a un seul tel sous-groupe engendré par n'importe quelle paire d'éléments d'ordre 2 qui commutent, autrement dit par n'importe quelle paire de doubles transpositions

$$\langle(12)(34), (13)(24)\rangle \cong (\mathbf{Z}/2\mathbf{Z})^2.$$

Pour les sous-groupes d'ordre 2, on en a autant que de doubles transpositions et pour ceux d'ordre 3, moitié moins que de 3-cycles. Il s'ensuit le treillis suivant :



Le groupe trivial est toujours distingué, les sous-groupes d'ordre 2 sont d'indice 2 dans le groupe de Klein donc distingué dans celui-ci. Par ailleurs⁸, les sous-groupes d'ordre 3 sont tous conjugués et donc non distingués et de même pour les sous-groupes d'ordre 2. On peut le voir à la main⁹ du fait que

$$(ab)(cd)(abc)(ab)(cd) = (adb) \quad \text{et} \quad (abc)(ab)(cd)(acb) = (ad)(bc) \quad \text{si} \quad \{a, b, c, d\} = \{1, 2, 3, 4\}$$

Reste à traiter le cas du groupe de Klein qui est distingué dans \mathfrak{A}_4 . Cela découle de la question suivante ou des théorèmes de Sylow mais peut se voir aussi à la main grâce aux calculs précédents. En particulier, on a montré que \mathfrak{A}_4 est engendré par une double transposition

6. On pouvait le déduire sans calcul des théorèmes de Sylow, puisque ces sous-groupes d'ordre 2 sont les 2-Sylow de \mathfrak{S}_3 .

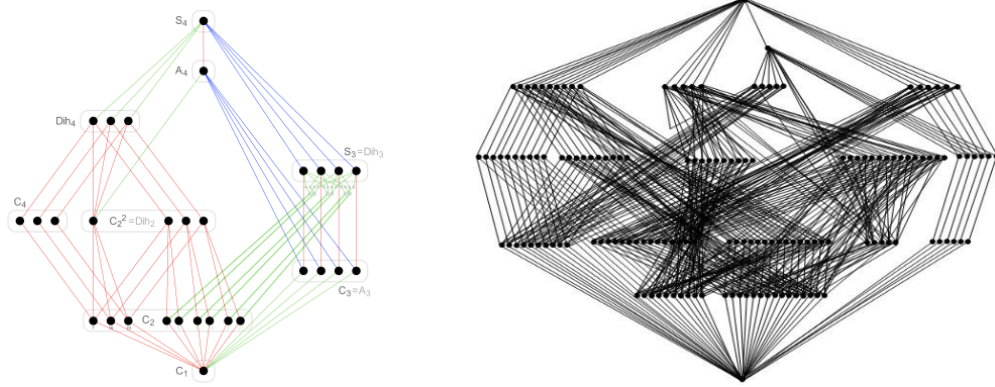
7. Une autre méthode est donnée dans l'exercice 8.

8. On peut là encore le voir grâce aux théorèmes de Sylow avec les 3-Sylows de \mathfrak{A}_4 .

9. Plus généralement, c'est aussi une conséquence de la question suivante.

et un 3-cycle et on retrouve le fait qu'être distingué n'est pas une relation transitive car $\langle (12)(34) \rangle \triangleleft \langle (12)(34), (13)(24) \rangle \triangleleft \mathfrak{A}_4$ mais $\langle (12)(34) \rangle \not\triangleleft \mathfrak{A}_4$.

On peut continuer avec \mathfrak{S}_4 ou \mathfrak{S}_5 mais la situation devient vite plus pénible avec les treillis respectifs suivants et pas moins de 156 sous-groupes dans le cas de \mathfrak{S}_5 :



Supposons à présent que $K \triangleleft H$ et que $H \triangleleft G$. A-t-on $K \triangleleft G$? Démontrer que si K est caractéristique dans H et que H est caractéristique dans G et montrons qu'alors K est caractéristique dans G . Pour ce faire, soit $\varphi \in \text{Aut}(G)$. Il s'agit d'établir que $\varphi(K) \subseteq K$. Puisque H est caractéristique dans G , $\varphi(H) \subseteq H$ et donc $\varphi|_H$ est un morphisme de groupes de H dans H qui est bijectif. On a donc un élément de $\text{Aut}(H)$ et comme $K \subseteq H$, $\varphi(K) = \varphi|_H(K) \subseteq K$ car K est caractéristique dans H , ce qu'il fallait démontrer!

► **COMPLÉMENTS .** – On a en fait la classification à isomorphisme près des groupes d'ordre ≤ 11 .

- Le seul groupe d'ordre 1 est le groupe trivial;
- Si G est d'ordre p avec p premier alors nécessairement tout élément $g \in G$ distinct de l'identité est d'ordre p et engendre G si bien que ¹⁰ $G \cong \mathbf{Z}/p\mathbf{Z}$. Cela résout les cas 2, 3, 5, 7, 11;
- Si G est d'ordre 4, on a que $G \cong \mathbf{Z}/4\mathbf{Z}$ si G contient un élément d'ordre 4 et sinon $G \cong (\mathbf{Z}/2\mathbf{Z})^2$ et G est engendré par toute paire d'éléments d'ordre 2 (qui commutent). En effet, l'ordre d'un élément non trivial de G divise 4 par Lagrange et vaut donc 2 ou 4. Si on a un élément d'ordre 4, alors G est cyclique et $G \cong \mathbf{Z}/4\mathbf{Z}$. Sinon, tout élément non trivial est d'ordre 2 et on peut faire appel à l'exercice 11 ou raisonner à la main. On doit avoir (puisque G est d'ordre 4) au moins un élément d'ordre 2, que nous pouvons appeler x . Puisque $x^2 = e$, $x^{-1} = x$ et donc on doit nécessairement avoir dans G un autre élément $y \neq x$ d'ordre 2. On a ainsi

$$\{e, x, y, xy\} \subseteq G \quad \text{et donc} \quad G = \{e, x, y, xy\}.$$

Noter qu'ici on a utilisé que $xy \neq e, x, y$. On en déduit que $yx \in G$ et $yx \neq e, x, y$ donc $yx = xy$ et cela permet d'écrire la table de G . On reconnaît celle de $(\mathbf{Z}/2\mathbf{Z})^2$ si bien que $G \cong (\mathbf{Z}/2\mathbf{Z})^2$.

- Si G est d'ordre 6, on a que $G \cong \mathbf{Z}/6\mathbf{Z}$ si ¹¹ G contient un élément d'ordre 6 (ou deux éléments d'ordre 2 et 3 respectivement qui commutent) et sinon ¹² $G \cong \mathfrak{S}_3$ et G est engendré par un élément τ d'ordre 2 et un élément σ d'ordre 3 tels que $\tau\sigma\tau = \sigma^2$. En effet, l'ordre d'un élément non trivial de G vaut (par Lagrange) 2, 3 ou 6. Si on a un élément d'ordre 6, alors G est cyclique et $G \cong \mathbf{Z}/6\mathbf{Z}$. On peut donc supposer que tout élément non trivial est d'ordre 2 ou 3. On va montrer qu'il existe un élément d'ordre 2 et un élément d'ordre 3. En effet, si tous les éléments sont d'ordre 2, il vient qu'alors G est abélien ¹³ et contient au moins deux éléments d'ordre 2 distincts qui commutent. Le sous-groupe engendré par ces deux éléments est alors isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$

10. En effet, pour $x \in G \setminus \{e\}$, $G = \{e, x, x^2, \dots, x^{p-1}\}$. On pose alors l'application

$$\varphi : \begin{cases} \mathbf{Z}/p\mathbf{Z} & \longrightarrow G \\ \bar{k} & \longmapsto x^k. \end{cases}$$

On vérifie comme toujours qu'une application définie sur un quotient est bien définie. Soient pour cela $\bar{k} = \bar{k}'$ pour $k, k' \in \mathbf{Z}$. Par définition, on a $k = k' + p\ell$ pour un certain entier ℓ . On a alors

$$x^k = x^{k'+p\ell} = x^{k'} (x^p)^\ell = x^{k'}$$

puisque $x^p = e$. L'application est donc bien définie et surjective vue la description de G plus haut. Comme $\#G = \#(\mathbf{Z}/p\mathbf{Z}) = p$, on a une bijection. Par ailleurs, il s'agit d'un morphisme de groupes puisque pour tous \bar{k}, \bar{k}' dans $\mathbf{Z}/p\mathbf{Z}$ (attention ici que la loi de groupe sur $\mathbf{Z}/p\mathbf{Z}$ est **additive** tandis que celle sur G est **multiplicative**),

$$f(\bar{k} + \bar{k}') = f(\overline{k+k'}) = x^{k+k'} = x^k x^{k'} = f(\bar{k}) f(\bar{k}').$$

On a donc bien un isomorphisme et le résultat!

11. Noter que par théorème chinois, puisque 3 et 2 sont premiers entre eux, $G \cong \mathbf{Z}/6\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$.

12. On a aussi que $G \cong \mathfrak{S}_3 \cong \mathbf{D}_3$ le groupe des isométries laissant invariant le triangle équilatéral formé des racines cubiques de l'unité et $\mathfrak{S}_3 \cong \mathbf{Z}/3\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$ est le seul produit semi-direct non trivial d'ordre 6.

13. En effet, pour tous $g, h \in G$, on a $(gh)^2 = e$ de sorte que $ghgh = e$ et en multipliant par h à droite il vient $ghg = h$ (car $h^2 = e$) et enfin en multipliant par g à droite on obtient $gh = hg$ (car $g^2 = e$).

donc d'ordre 4, ce qui contredit le théorème de Lagrange. De même, si l'on avait que des éléments d'ordre 3, alors on disposerait d'au moins deux éléments x, y avec $y \neq x, x^2$ d'ordre 3 et

$$\{e, x, x^2, y, y^2, xy\} \subseteq G,$$

où $xy \neq e, x, x^2, y, y^2$. On a alors que $xy^2 \neq e, x, x^2, y, y^2, xy$ et on aurait alors au moins 7 éléments dans G . On peut donc supposer que l'on dispose d'un élément τ d'ordre 2 et un élément σ d'ordre 3 et alors

$$\{e, \tau, \sigma, \sigma^2, \tau\sigma, \tau\sigma^2\} \subseteq G \quad \text{et donc} \quad G = \{e, \tau, \sigma, \sigma^2, \tau\sigma, \tau\sigma^2\}$$

et où tous ces éléments sont deux à deux distincts. Alors, $\sigma\tau \in G$ et comme $\sigma\tau \neq \tau\sigma$, sinon le produit fournit un élément d'ordre ¹⁴ 6, on a nécessairement que $\tau\sigma\tau = \sigma^2$. Cela permet de dresser la table de multiplication du groupe G et on reconnaît celle de \mathfrak{S}_3 si bien que $G \cong \mathfrak{S}_3$.

- Si G est d'ordre 8, les exercices sur le groupe diédral et les quaternions ainsi le cours sur les produits semi-directs garantira que G est isomorphe soit à $(\mathbb{Z}/2\mathbb{Z})^3$, soit à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, soit à $\mathbb{Z}/8\mathbb{Z}$, soit au groupe diédral D_4 soit au groupe des quaternions H_8 .
- Si G est d'ordre $9 = 3^2$, le cours garantira que G est abélien et donc le théorème de structure des groupes abéliens de type fini garantit que $G \cong \mathbb{Z}/9\mathbb{Z}$ ou $G \cong (\mathbb{Z}/3\mathbb{Z})^2$;
- Si G est d'ordre $10 = 2 \times 5$ avec $2 \mid 5 - 1$, le cours sur le produit semi-direct garantira que G est soit abélien et isomorphe à $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ soit isomorphe à l'unique produit semi-direct non trivial $\mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}$ (qui est en fait isomorphe au groupe diédral ¹⁵ D_5).

Pour aller plus loin, je vous renvoie aux feuilles de TD des années précédentes ¹⁶ pour le cours d'Algèbre M1 MF, on peut classer les groupes d'ordre p^2q avec p et q deux nombres premiers distincts ce qui traite le cas de 12 (qui peut également se traiter "à la main"), 13 est premier, 14 et 15 sont alors couverts par le cours sur le produit semi-direct! On remarquera donc qu'il y a quelque chose qui semble se passer pour les groupes d'ordre 8 ou 12 (on a plus de travail et plus de classes d'isomorphismes). On peut aussi classer ¹⁷ (à isomorphisme près) les groupes de cardinal ≤ 15 on s'arrête à 15 pour une bonne raison, à savoir que le cardinal 16 est plus délicat et qu'on obtient beaucoup de classes d'isomorphismes (précisément 14). En fait, on peut voir que plus l'ordre du groupe possède de facteurs premiers de multiplicité grande, plus cela donne de la marge et donne lieu à de nombreuses classes d'isomorphismes. Pour une taille de cardinal donnée, l'ordre qui va maximiser ces critères est la puissance de 2. On peut par exemple l'illustrer par le fait que parmi tous les groupes d'ordre ≤ 2000 (à isomorphisme près), 99,2% sont d'ordre ¹⁸ $2^{10} = 1024$. En fait, on conjecture que presque tous les groupes finis sont des 2-groupes dans le sens où

$$\lim_{N \rightarrow +\infty} \frac{\#\{\text{classes d'iso. de 2-groupes } G \text{ de cardinal } \leq N\}}{\#\{\text{classes d'iso. de groupes } G \text{ de cardinal } \leq N\}} = 1$$

et même

$$\lim_{N \rightarrow +\infty} \frac{\#\left\{\text{classes d'iso. de 2-groupes } G \text{ de cardinal } 2^{\left\lceil \frac{\log(N)}{\log(2)} \right\rceil}\right\}}{\#\{\text{classes d'iso. de groupes } G \text{ de cardinal } \leq N\}} = 1.$$

3. Le résultat découle du fait que la classe de conjugaison d'un élément de \mathfrak{S}_n est entièrement déterminée par la forme de sa décomposition en produit de cycles à supports disjoints. Soit $c = (a_1, \dots, a_k)$ un k -cycle de \mathfrak{S}_n . Alors pour tout $\sigma \in \mathfrak{S}_n$, on a

$$\sigma c \sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k)).$$

Toute permutation se décompose alors de façon unique en produit de cycles à support disjoints et on voit que tout conjugué d'une décomposition donnée possède une décomposition de la même forme et réciproquement il n'est pas difficile pour deux permutations σ_1, σ_2 ayant le même type de décomposition en produit de cycles à supports disjoints de construire $\mu \in \mathfrak{S}_n$ tel que $\sigma_1 = \mu \sigma_2 \mu^{-1}$. La classe de conjugaison correspondant à une partition donnée est l'ensemble des permutations dont la décomposition en cycles à support disjoint fait intervenir des cycles de longueurs $\lambda_1, \lambda_2, \dots, \lambda_r$. Par exemple, dans \mathfrak{S}_4 , la classe de conjugaison des doubles transpositions ¹⁹ correspond à la partition $2 + 2 = 4$ et un 3-cycles à $3 + 1 = 4$.

¹⁴. En effet, $(\sigma\tau)^6 = \sigma^6\tau^6$ car G est abélien si $\sigma\tau = \tau\sigma$. Mais comme $\tau^2 = \sigma^3 = e$, on a $(\sigma\tau)^6 = e$. L'ordre de $\tau\sigma$ (qui est différent de e) vaut donc 2, 3 ou 6 mais $(\tau\sigma)^2 = \tau^2\sigma^2$ (toujours par caractère abélien de G) et donc $(\tau\sigma)^2 = \sigma^2 \neq e$ car $\tau^2 = e$ et σ est d'ordre 3. De même, $(\tau\sigma)^3 = \tau \neq e$ et l'ordre de $\tau\sigma$ est bien 6.

¹⁵. Voir l'exercice 3.

¹⁶. Disponibles sur la page web de David Harari.

¹⁷. Voir à nouveau les feuilles de TD de l'an dernier.

¹⁸. Voir Besche, Eick et O'Brien, *The groups of order at most 2000*.

¹⁹. C'est aussi un exercice intéressant de les dénombrer et on obtient que le cardinal correspondant à une partition λ vaut

$$\frac{n!}{\prod_{j=1}^n a_j(\lambda)! j^{a_j(\lambda)}}$$

► **COMPLÉMENTS** . – Pour \mathfrak{A}_n , c'est un peu plus subtil. Comme $\mathfrak{A}_n \triangleleft \mathfrak{S}_n$, la classe de conjugaison d'un élément de \mathfrak{A}_n dans \mathfrak{S}_n est contenue dans \mathfrak{A}_n . Par ailleurs, comme $[\mathfrak{S}_n : \mathfrak{A}_n] = 2$, on a que la classe de conjugaison d'un élément de \mathfrak{A}_n est soit égale à la classe de conjugaison de cet élément dans \mathfrak{S}_n soit la moitié de la classe de conjugaison de cet élément dans \mathfrak{S}_n (dit autrement la classe de conjugaison d'un élément $\sigma \in \mathfrak{A}_n$ dans \mathfrak{S}_n est soit égale à la classe de conjugaison de cet élément dans \mathfrak{A}_n soit la réunion de deux classes de conjugaison de même cardinal dans \mathfrak{A}_n). En effet, on sait que la classe de conjugaison d'un élément est l'orbite par l'action de conjugaison et il est facile de voir que pour $\sigma \in \mathfrak{A}_n$

$$\#Cl_{\mathfrak{S}_n}(\sigma) = \frac{n!}{\#Z_{\mathfrak{S}_n}(\sigma)} \quad \text{et} \quad \#Cl_{\mathfrak{A}_n}(\sigma) = \frac{n!}{2\#Z_{\mathfrak{A}_n}(\sigma)}$$

avec

$$Z_{\mathfrak{S}_n}(\sigma) = \{\mu \in \mathfrak{S}_n : \mu\sigma\mu^{-1} = \sigma\} \quad \text{et} \quad Z_{\mathfrak{A}_n}(\sigma) = \{\mu \in \mathfrak{A}_n : \mu\sigma\mu^{-1} = \sigma\}.$$

Soit $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma)$ soit $Z_{\mathfrak{A}_n}(\sigma) \subsetneq Z_{\mathfrak{S}_n}(\sigma)$ strictement et il existe $\mu_0 \in \mathfrak{S}_n \setminus \mathfrak{A}_n$ tel que $\mu\sigma\mu^{-1} = \sigma$. Alors, le groupe alterné étant d'indice 2, $\mathfrak{S}_n = \mathfrak{A}_n \sqcup \mathfrak{A}_n\mu_0$ si bien que

$$\begin{array}{ccc} \{\mu \in \mathfrak{S}_n \setminus \mathfrak{A}_n : \mu\sigma\mu^{-1} = \sigma\} & \longrightarrow & Z_{\mathfrak{A}_n}(\sigma) \\ \mu & \longmapsto & \mu\mu_0 \end{array}$$

est une bijection qui montre que $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma) \sqcup \{\mu \in \mathfrak{S}_n \setminus \mathfrak{A}_n : \mu\sigma\mu^{-1} = \sigma\}$ avec

$$\#Z_{\mathfrak{A}_n}(\sigma) = \#\{\mu \in \mathfrak{S}_n \setminus \mathfrak{A}_n : \mu\sigma\mu^{-1} = \sigma\}.$$

Reste à déterminer quand une classe dans \mathfrak{S}_n reste entière et quand elle se scinde en deux. Montrons qu'elle se scinde en deux si, et seulement si, la décomposition de σ ne comporte que des cycles de longueur impaire 2 à 2 distinctes. Si tel est le cas, σ commute avec le sous-groupe engendré par les cycles apparaissant dans sa décomposition en produit de cycles à supports disjoints. En effet, si τ commute à σ , comme la conjugaison préserve le type de décomposition en produit de cycles à supports disjoints et que tous les cycles apparaissant dans celle de σ sont de longueur différente, cela implique que τ commute à chacun de ces cycles individuellement. Fixons à présent la décomposition en cycle de $\sigma = c_1 c_2 \cdots c_r$. On utilise alors que si c est un cycle de longueur ℓ , alors le centralisateur de c est donné par

$$\{c^i \mu : i \in \{0, \dots, \ell - 1\}, \mu \in \mathfrak{S}_{n-\ell}\}$$

avec $\mathfrak{S}_{n-\ell}$ le sous-groupe de \mathfrak{S}_n fixant tous les éléments du support de c . Il est clair que toutes les permutations de cette forme commutent à c et on conclut par un argument de cardinalité, puisque le cardinal de ce centralisateur est simplement le $n!$ divisé par le cardinal de la classe de conjugaison de c , à savoir le nombre de ℓ -cycles, soit $\frac{n(n-1)\cdots(n-\ell+1)}{\ell}$. On obtient ainsi bien que les deux ensembles ont même cardinal $\ell \times (n - \ell)!$. On en déduit donc puisque τ commute à c_1 que $\tau = c_1^i \tau_1$ avec τ_1 de support disjoint à celui de c_1 . On obtient que τ_1 commute à σ et donc τ_1 commute à c_2 et donc $\tau_1 = c_2^j \tau_2$ et de proche en proche τ appartient au sous-groupe engendré par c_1, \dots, c_r . Il en résulte, puisque tous les cycles de σ sont de longueur impaire que τ est de signature $+1$ et $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma)$. On pouvait aussi calculer le cardinal de $Z_{\mathfrak{S}_n}(\sigma)$ (voir la note de bas de page 19) et constater qu'il est impair de sorte que tout élément de $Z_{\mathfrak{S}_n}(\sigma)$ est d'ordre impair. Or, tout élément de $\mathfrak{S}_n \setminus \mathfrak{A}_n$ étant d'ordre pair, on a le résultat! Réciproquement, si on a un cycle de longueur paire c , on voit alors que

$$\forall \mu \in \mathfrak{S}_n, \quad \mu\sigma\mu^{-1} = (\mu c)\sigma(\mu c)^{-1}$$

et donc $Z_{\mathfrak{S}_n}(\sigma) \subsetneq Z_{\mathfrak{A}_n}(\sigma)$ strictement. Alternativement, si σ comporte deux cycles $c = (a_1, \dots, a_k)$ et $c' = (a'_1, \dots, a'_k)$ de même longueur impaire, alors, notant $d = (a_1 \ a'_1) \cdots (a_k \ a'_k)$ (de signature -1), on a

$$\forall \mu \in \mathfrak{S}_n, \quad \mu\sigma\mu^{-1} = (\mu d)\sigma(\mu d)^{-1}$$

et donc à nouveau $Z_{\mathfrak{S}_n}(\sigma) \subsetneq Z_{\mathfrak{A}_n}(\sigma)$ strictement.

Montrons pour finir que tout sous-groupe H de \mathfrak{S}_n d'indice n est isomorphe à \mathfrak{S}_{n-1} .

Supposons pour commencer que $n \geq 5$. On note $G = \mathfrak{S}_n$ et soit H un sous-groupe d'indice n . Notons $X = G/H$ l'ensemble quotient de cardinal n . On dispose de l'action naturelle de G sur X qui induit un morphisme de groupe $\psi : G \rightarrow \mathfrak{S}(X) \cong \mathfrak{S}_n$. Montrons qu'il s'agit d'un isomorphisme. Son noyau est un sous-groupe distingué de G , donc égal à $\{1\}$, \mathfrak{A}_n ou \mathfrak{S}_n . Mais on voit que ²⁰

$$\text{Ker}(\psi) = \bigcap_{a \in G} aHa^{-1} \subseteq H.$$

où $a_i(\lambda)$ désigne le nombre de λ_k égaux à i . On fait pour cela agir G sur lui-même par conjugaison et on montre que le cardinal du stabilisateur de σ est donné par $\prod_{j=1}^n a_j(\lambda)! j^{a_j(\lambda)}$. En effet, pour envoyer σ sur lui-même par conjugaison, on procède cycle par cycle. Le premier cycle de longueur j est envoyé sur un autre cycle de longueur j .

On a alors $a_j(\lambda)$ choix parmi tous les cycles de longueur j . Ensuite, on a j manières d'envoyer par conjugaison un j -cycle sur un autre j -cycle. Pour le second cycle de longueur j , il reste $a_j(\lambda) - 1$ choix parmi tous les cycles de longueur j et toujours j manières d'envoyer par conjugaison un j -cycle sur un autre j -cycle. On obtient finalement un facteur $a_j(\lambda)! j^{a_j(\lambda)}$ et le produit apparaît lorsqu'on parcourt toutes les longueurs de cycles possibles.

20. De manière générale, le noyau est l'intersection des stabilisateurs.

Or, $\#H = (n-1)!$ et $(n-1)! < n!/2$ (car $2 < n$) si bien que nécessairement $\text{Ker}(\psi) = \{\text{Id}\}$ et par cardinalité, ψ est un isomorphisme. On peut alors restreindre cette action au sous-groupe H et le groupe H est alors clairement un point fixe pour cette action restreinte. Cela donne lieu à une action de H sur $X \setminus \{H\}$ et ainsi à un morphisme $\varphi : H \rightarrow \mathfrak{S}(X \setminus \{H\}) \cong \mathfrak{S}_{n-1}$. Ce morphisme est injectif (car ψ l'est) et donc un isomorphisme par égalité des cardinaux.

Les cas $n = 2, 3$ sont immédiats et pour $n = 4$, on utilise le fait qu'un sous-groupe d'indice 4 est de cardinal 6 donc abélien ou isomorphe à \mathfrak{S}_3 . Mais si ce groupe était abélien, alors on aurait un élément d'ordre 6, ce qui n'est pas le cas.

EXERCICE 2 — GROUPE DIÉDRAL. On considère les deux transformations suivantes du plan euclidien : la rotation ρ de centre O et d'angle $\frac{\pi}{2}$, et la symétrie σ par rapport à l'axe des abscisses. Le groupe diédral \mathbf{D}_4 est le sous-groupe des isométries du plan engendré par ρ et σ .

1. Calculer l'ordre de σ et de ρ . Décrire l'isométrie $\sigma\rho\sigma^{-1}$.
2. Montrer que \mathbf{D}_4 contient 8 éléments; caractériser ces éléments géométriquement.
3. Déterminer les classes de conjugaison dans \mathbf{D}_4 .
4. Donner le treillis des sous-groupes de \mathbf{D}_4 , en précisant les sous-groupes distingués.

SOLUTION.

1. On vérifie aisément²¹ que $\sigma^2 = \text{Id}$ et donc σ est d'ordre 2 tandis que $\rho^4 = \text{Id}$ donc ρ est d'ordre 2 ou 4 mais ρ^2 est la rotation d'angle π donc ρ est d'ordre 4.
On se convainc aisément sur un dessin que $\sigma\rho\sigma^{-1} = \sigma\rho\sigma$ est la rotation d'angle $-\frac{\pi}{2}$, à savoir ρ^{-1} . On peut le démontrer en utilisant le fait que les matrices de σ et ρ sont respectivement

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

de sorte que la matrice de $\sigma\rho\sigma$ est bien donnée par

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

qui est bien la matrice de la rotation de centre l'origine et d'angle $-\frac{\pi}{2}$. Plus simplement, on peut voir que $\sigma\rho\sigma$ est un automorphisme orthogonal de déterminant 1 donc une rotation et on détermine son angle en calculant l'image de $e_1 = (1, 0)$.

2. Il est facile de voir que \mathbf{D}_4 contient au moins 8 éléments distincts²² : Id , la symétrie σ , les rotations ρ, ρ^2 et ρ^3 d'angle $\frac{\pi}{2}, \pi$ et $\frac{3\pi}{2}$ ainsi que $\sigma\rho, \sigma\rho^2$ et $\sigma\rho^3$ qui sont respectivement des symétries orthogonales par rapport à la droite d'angle respectivement $\frac{\pi}{4}, \frac{\pi}{2}$ et $\frac{3\pi}{4}$. On voit alors qu'on a ainsi tous les éléments de \mathbf{D}_4 grâce à la relation $\sigma\rho\sigma = \rho^{-1}$. En effet, par définition d'un groupe engendré par deux éléments, tout élément de \mathbf{D}_4 est de la forme $\sigma^k \rho^{r_1} \sigma \rho^{r_2} \sigma \cdots \rho^{r_s} \sigma^\ell$ avec $k, \ell \in \{0, 1\}$ et $r_1, \dots, r_s \in \{1, \dots, 3\}$ et la relation $\sigma\rho\sigma = \rho^{-1}$ permet de voir qu'un tel élément est de la forme $\sigma^s \rho^r$ avec $s \in \{0, 1\}$ et $r \in \{0, 1, 2, 3\}$ car σ est d'ordre 2 et ρ d'ordre 4. En dehors de l'identité, on a donc deux éléments d'ordre 4 ($\pm\rho$) et 5 éléments d'ordre 2.
3. Il est clair que la classe de conjugaison de l'identité est réduite à $\{\text{Id}\}$ tout comme celle de $\rho^2 = -\text{Id}$ est donnée par $\{-\text{Id}\}$. La relation $\sigma\rho\sigma^{-1}$ montre que la classe de conjugaison de ρ est donnée par $\{\rho, \rho^3\} = \{\rho, -\rho\}$ (le conjugué d'une rotation est une rotation). Enfin, la relation $\sigma\rho\sigma = \rho^3$ fournit que $\rho\sigma\rho^{-1} = -\sigma$ qui implique facilement que la classe de conjugaison de σ est $\{\sigma, \sigma\rho^2 = -\sigma\}$ et enfin la classe de conjugaison de $\sigma\rho$ est $\{\sigma\rho, \sigma\rho^3\} = \{\sigma\rho, -\sigma\rho\}$.
4. Les sous-groupes potentiels sont d'ordre 1, 2, 4 ou 8. les sous-groupes d'ordre 1 et 8 sont immédiats. Pour les sous-groupes d'ordre 2, ils sont cycliques engendrés par un élément d'ordre 2, on en a donc cinq engendrés respectivement par $\sigma, -\sigma, -\text{Id}$ (qui est le centre de \mathbf{D}_4 car le centre est la réunion des éléments dont la classe de conjugaison est réduite à un singleton), $\sigma\rho$ et $-\sigma\rho$. Pour les sous-groupes d'ordre 4, on sait qu'un tel sous-groupe est soit cyclique engendré par un élément d'ordre 4 soit par deux éléments d'ordre 2 qui commutent. Dans le premier cas, on obtient ici le sous-groupe engendré par ρ et dans le second on obtient deux sous-groupes (car on n'a pas d'autres éléments d'ordre 2 qui commutent) $\{\text{Id}, -\text{Id}, \sigma, -\sigma\}$ et $\{\text{Id}, -\text{Id}, \sigma\rho, -\sigma\rho = \sigma\rho^3\}$ isomorphes à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. On obtient le treillis suivant

21. Soit géométriquement soit via les matrices.

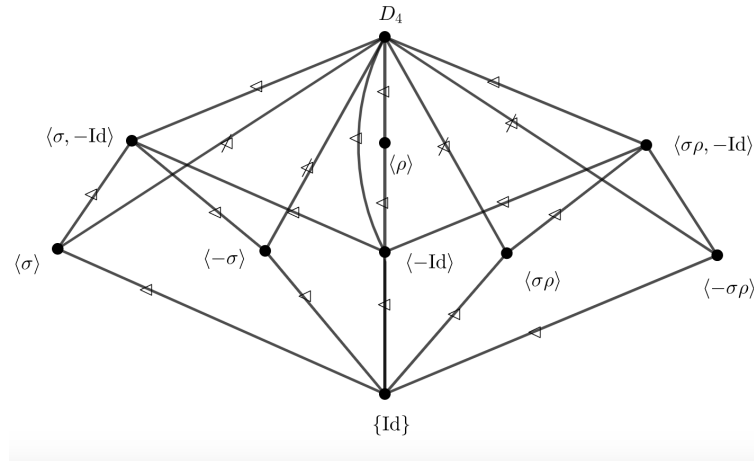
22. On rappelle que les isométries du plan forment un groupe pour la loi de composition des applications et qu'une isométrie du plan est soit une rotation d'angle θ si elle est de déterminant 1, auquel cas sa matrice dans la base canonique est donnée par

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

tandis qu'une isométrie indirecte de déterminant -1 est une symétrie orthogonale par rapport à une droite. On rappelle que la matrice de la symétrie orthogonale par rapport à la droite d'angle $\frac{\theta}{2}$ par rapport à l'axe des abscisses est donné dans la base canonique par

$$\begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$$

Cela se vérifie notamment facilement en passant aux nombres complexes.



Tous les sous-groupes d'indice 2 sont distingués. Il reste donc le cas des sous-groupes d'ordre 2. Les relations ci-dessus montrent qu'aucun n'est distingué sauf celui engendré par $\{-Id\}$ qui est en fait le centre et le groupe dérivée de D_4 et est même caractéristique (de même que $\langle \rho \rangle$).

► **COMPLÉMENTS .** – Pour un entier $n > 0$, le groupe diédral D_n est le sous-groupe des isométries du plan engendré par σ et par la rotation ρ de centre O et d'angle $\frac{2\pi}{n}$. On montre alors que D_n contient $2n$ éléments et correspond au groupe des isométries du plan préservant le polygone régulier P_n du plan à n côtés de sommet les racines n -ièmes de l'unité. Tout ce qu'on a fait se généralise en effet parfaitement au cas général. On constate de même que $\sigma\rho\sigma = \rho^{-1}$ et cette relation entraîne que tout élément de D_n est de la forme $\sigma^\ell \rho^k$ pour $\ell, k \in \mathbb{N}$. Comme σ est d'ordre 2 et ρ d'ordre n , on obtient que D_n est d'ordre $2n$ et que

$$D_n = \{Id, \rho, \dots, \rho^{n-1}, \sigma, \sigma\rho, \dots, \sigma\rho^{n-1}\}.$$

On peut montrer que

$$Z(D_n) = \begin{cases} D_n & \text{si } n \in \{1, 2\} \\ \{Id\} & \text{si } n \text{ impair et } n \geq 3 \\ \{Id, \rho^{\frac{n}{2}} = -Id\} & \text{sinon} \end{cases} \quad \text{et} \quad D(D_n) = \begin{cases} \{Id\} & \text{si } n \in \{1, 2\} \\ \langle \rho \rangle & \text{si } n \text{ impair et } n \geq 3 \\ \langle \rho^2 \rangle & \text{sinon.} \end{cases}$$

Dans le cas pair, $D_n/Z(D_n) \cong D_{n/2}$ et $D_n^{\text{ab}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ si n est pair et $\cong \mathbb{Z}/2\mathbb{Z}$ si n est impair. On verra que $D_n = \langle \rho \rangle \rtimes \langle \sigma \rangle \cong \mathbb{Z}/n\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$ avec $\varphi(1)$ donné par $\bar{m} \mapsto -\bar{m}$. On a $D_2 \cong \mathbb{Z}/2\mathbb{Z}$ et $D_3 \cong \mathfrak{S}_3$. Le groupe D_n est résoluble et nilpotent si, et seulement si, son ordre est une puissance de 2. Les classes de conjugaison sont $\{Id\}$, $\{-Id\}$, $\{\rho^k, \rho^{-k}\}$ pour $k \in \{1, \dots, \frac{n}{2} - 1\}$, $\{\sigma, \sigma\rho^2, \dots, \sigma\rho^{n-2}\}$ et $\{\sigma\rho, \sigma\rho^3, \dots, \sigma\rho^{n-1}\}$ si n est pair tandis que si n est impair, on obtient $\{Id\}$, $\{\rho^k, \rho^{-k}\}$ pour $k \in \{1, \dots, \frac{n-1}{2}\}$ et $\{\sigma, \sigma\rho, \dots, \sigma\rho^{n-1}\}$. Enfin, pour tous diviseurs positifs d et d' de n et $k \in \{0, 1, \dots, \frac{n}{d'} - 1\}$, on pose

$$H_h = \langle \rho^{\frac{n}{d}} \rangle \cong \mathbb{Z}/d\mathbb{Z} \quad \text{et} \quad H_{d',k} = \langle \rho^{\frac{n}{d'}}, \sigma\rho^k \rangle \cong D_{d'}.$$

Alors tout sous-groupe de D_n est égal à un sous-groupe H_d pour un unique diviseur d de n ou à un sous-groupe $H_{d',k}$ pour un unique diviseur d' et un unique k . Lorsque n est pair, les sous-groupes distingués sont les H_d pour $d \mid n$ et D_n et si n est impair les H_d pour $d \mid n$ et D_n ainsi que $H_{\frac{n}{2},0}$ et $H_{\frac{n}{2},1}$. Il s'agit d'un exemple de groupe donné par générateurs et relations. Ces groupes seront très important dans le cours de Géométrie au second semestre.

Finalement terminons par la caractérisation géométrique du groupe D_n . Il est clair que D_n est contenu dans le groupe des isométries de P_n . Montrons alors que le cardinal de ce groupe d'isométries est $2n$ pour conclure. Puisqu'une isométrie préserve les distances, on constate immédiatement que l'image par une isométrie qui préserve P_n d'un sommet est un autre sommet (en considérant la distance d'un point de P_n à l'origine, qui est maximale uniquement pour les sommets). On en déduit que l'image du sommet A ne peut être qu'un autre sommet, ce qui laisse n choix. Mais alors l'image d'un sommet adjacent de A , disons B , toujours pour des raisons de conservation de la distance doit être adjacent à l'image de B , ce qui laisse 2 possibilités. On constate qu'on a donc au plus $2n$ choix, l'image de l'arête AB déterminant complètement l'isométrie. Comme on a en a déjà $2n$, on les a bien toutes!

EXERCICE 3 — QUATERNIONS ET GROUPES D'ORDRE 8. On note H l'ensemble des matrices de $\mathcal{M}_2(\mathbb{C})$ de la forme

$$M_{a,b} := \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}.$$

On pose $H^* = H - \{0\}$.

1. Montrer que H^* est un sous-groupe non commutatif de $\text{GL}_2(\mathbb{C})$.
2. On note 1 la matrice identité, et on pose $I := M_{i,0}$, $J = M_{0,1}$, $K = M_{0,i}$. Soit $\mathbf{H}_8 = \{\pm 1, \pm I, \pm J, \pm K\}$. Montrer que \mathbf{H}_8 est un sous-groupe non commutatif de cardinal 8 de H^* .
Indication : On observera que $IJ = K = -JI$, avec des relations analogues par permutations circulaires de I, J, K .
3. Montrer que le centre et le sous-groupe dérivé de \mathbf{H}_8 sont tous deux égaux à $\{\pm 1\}$.
4. Montrer que l'abélianisé de \mathbf{H}_8 est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.
5. Est-ce qu'un groupe dont tous les sous-groupes sont distingués est nécessairement abélien ?

SOLUTION.

1. On a que $\det(M_{a,b}) = |a|^2 + |b|^2 \neq 0$ dès que $M_{a,b} \neq 0$ (ce qui est équivalent à $(a, b) \neq (0, 0)$) donc $H \subseteq \text{GL}_2(\mathbb{C})$ et contient l'identité. On calcule également le produit $M_{a,b}M_{c,d} = M_{ac-b\bar{d}, ad+b\bar{c}}$ ce qui permet de conclure à la stabilité par produit et enfin $M_{a,b}^{-1} = M_{\frac{\bar{a}}{|a|^2+|b|^2}, -\frac{b}{|a|^2+|b|^2}}$ ce qui permet de montrer la stabilité par passage à l'inverse. Il n'est pas commutatif car $M_{i,0}M_{0,1} \neq M_{0,1}M_{i,0}$.
2. On vérifie par le calcul que $I^2 = J^2 = K^2 = IJK = -1$ et que $IJ = -JI = K$, $KI = -IK = J$ et $JK = -KJ = I$ de sorte qu'on obtient bien un groupe de cardinal 8 de table

	1	I	J	K	-1	-I	-J	-K
1	1	I	J	K	-1	-I	-J	-K
I	I	-1	K	-J	-I	1	-K	J
J	J	-K	-1	I	-J	K	1	-I
K	K	J	-I	-1	-K	-J	I	1
-1	-1	-I	-J	-K	1	I	J	K
-I	-I	1	-K	J	I	-1	K	-J
-J	-J	K	1	-I	J	-K	-1	I
-K	-K	-J	I	1	K	J	-I	-1

à 5 classes de conjugaisons $\{1\}$, $\{-1\}$, $\{\pm I\}$, $\{\pm J\}$ et $\{\pm K\}$. Il est non commutatif par exemple car $IJ \neq JI$.

3. On voit immédiatement que $Z(\mathbf{H}_8) = \{\pm \text{Id}\}$. Puis on voit que tous les commutateurs sont triviaux sauf $[I, J] = [I, K] = [J, K] = -\text{Id}$ si bien que $D(\mathbf{H}_8) = \langle -\text{Id} \rangle = \{\pm \text{Id}\}$.
4. Notons $H = D(\mathbf{H}_8)$. L'abélianisé \mathbf{H}_8/H est donc d'ordre 4 et on voit que les classes ne sont autres que $H = \{\pm 1\}$, $IH = \{\pm I\}$, $JH = \{\pm J\}$ et $KH = \{\pm K\}$ dont on voit²³ qu'on a $IH^2 = JH^2 = KH^2 = H$. On a donc nécessairement que $\mathbf{H}_8^{\text{ab}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Une autre façon de voir les choses est de considérer la projection canonique $\pi : \mathbf{H}_8 \rightarrow \mathbf{H}_8/H$. On a alors que $\pi(I)^2 = \pi(I^2) = \pi(-1) = \pi(1)$ puisque $-1 \in H = \text{Ker}(\pi)$. On a donc que $\pi(I) \neq \pi(1)$ car $I \notin H$ est d'ordre 2. On obtient de même que tous les éléments non triviaux sont d'ordre 2 dans \mathbf{H}_8/H (on utilise ici la surjectivité de π). Une autre méthode consiste à exploiter le fait que $H = D(\mathbf{H}_8) = Z(\mathbf{H}_8)$. Ainsi, si $\mathbf{H}_8/H \cong \mathbb{Z}/4\mathbb{Z}$, alors $\mathbf{H}_8/Z(\mathbf{H}_8)$ serait cyclique et d'après le cours, cela entraînerait que \mathbf{H}_8 est abélien, ce qui n'est pas le cas ! On a donc nécessairement que $\mathbf{H}_8^{\text{ab}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

► **COMPLÉMENTS.** – Noter que les quaternions fournissent un exemple²⁴ de groupe G tel que $G/Z(G)$ abélien mais non cyclique et que G est non commutatif ! L'hypothèse de cyclicité ne peut donc pas être affaiblie dans le résultat de votre cours !

5. On voit facilement que les sous-groupes de \mathbf{H}_8 sont $\{1\}$, \mathbf{H}_8 , $\{\pm 1\}$ (d'ordre 2) et $\langle I \rangle = \{\pm 1, \pm I\}$, $\langle J \rangle$ et $\langle K \rangle$ (tous trois cycliques d'ordre 4). Les sous-groupes triviaux sont naturellement distingués tout comme ceux d'ordre 4 (car d'indice 2) et le sous-groupe d'ordre 2 étant égal au centre (ou au sous-groupe dérivé) l'est aussi. Ainsi, on a un exemple de groupe non commutatif dont tous les sous-groupes propres sont distingués et cycliques.

► **COMPLÉMENTS.** – Si $\mathbf{H}_8 = N \rtimes H$, alors nécessairement N ou H est d'ordre 2, donc égal à $\{\pm 1\}$. Si c'est H , alors H serait distingué et donc le produit serait direct. Cela impliquerait que \mathbf{H}_8 est abélien. On peut donc supposer que $N = \{\pm 1\}$. Mais dans ce cas, $\text{Aut}(N)$ est réduit à un élément et tout morphisme $H \rightarrow \text{Aut}(N)$ est trivial et on conclurait de la même manière que le produit semi-direct serait direct et \mathbf{H}_8 abélien. Ainsi \mathbf{H}_8 n'est pas un produit semi-direct non trivial.

Soit maintenant un groupe G d'ordre 8. Si G a un élément d'ordre 8, alors $G \cong \mathbb{Z}/8\mathbb{Z}$. Si G est d'exposant 2, alors $G \cong (\cong \mathbb{Z}/2\mathbb{Z})^3$. Si maintenant G est d'exposant 4 abélien, on a que $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Reste alors à traiter le cas d'exposant 4 non abélien. On a ainsi un élément $r \in G$ d'ordre 4 et on pose $R = \langle r \rangle \cong \mathbb{Z}/4\mathbb{Z}$. Soit alors $s \in G \setminus R$ d'ordre minimal. Si s est d'ordre 2, alors on pose $S = \langle s \rangle$ et $S \cap R = \{e\}$ et G est engendré par R et S et $R \triangleleft G$ car d'indice 2. On sait alors que $G \cong R \rtimes S \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_4$ (on a un seul tel produit semi-direct non abélien à isomorphisme près). Enfin, si s est d'ordre 4 (et que tout élément de $G \setminus R$ est d'ordre 4), renommons r et s par I et J et notons $K = IJ$. On sait que I^2 est d'ordre 2 et c'est le seul élément d'ordre 2 de G . On

23. Par exemple car $(IH)^2 = IHIH$ et, puisque H est distingué dans \mathbf{H}_8 , $HI = IH$ et $(IH)^2 = I^2H = -H = H$. On rappelle alors que H est l'élément neutre du groupe quotient \mathbf{H}_8/H .

24. Et oui, encore !

peut le renommer $I^2 = -1$. De même, on obtient $J^2 = -1$. Mais $K \notin R$ car $J \notin R$ donc K est d'ordre 4 et $K^2 = -1$ est d'ordre 2. On a alors que $Z(G) = \{\pm 1\}$. On sait en effet que $Z(G)$ est un sous-groupe de G de cardinal 2 ou 4 (car G est supposé non abélien et est un 2-groupe). Si le cardinal de $Z(G)$ était 4, alors il s'agit d'un sous-groupe distingué d'indice 2 et on aurait $G/Z(G) \cong \mathbf{Z}/2\mathbf{Z}$ cyclique si bien que G serait abélien, ce qui est absurde. On a donc que $Z(G)$ est d'ordre 2, nécessairement engendré par un élément d'ordre 2 et comme -1 est le seul élément de G d'ordre 2, on a le résultat. On a donc 8 éléments distincts de G , à savoir $\pm 1, \pm I, \pm J$ et $\pm K$ et donc $G = \{\pm 1, \pm I, \pm J, \pm K\}$ avec $I^2 = J^2 = K^2 = -1$ et $K = IJ$. On a par ailleurs que $IJ, IK, JK \notin Z(G)$ et comme $JI \notin R$ car $J \notin R$ et $I \in R$, on a $JI \in \{J, K, -J, -K\}$ car $R = \{\pm 1, \pm I\}$. On a alors clairement $JI \neq \pm J$ et $JI \neq IJ$ sinon I et J commuteraient et donc I commuterait à K et ainsi $I \in Z(G)$. D'où $JI = -IJ = -K$ et de même on montre que $KI = -IK = J$ et $JK = -KJ = I$ et on retrouve la table de multiplication des quaternions donc $G \cong \mathbf{H}_8$.

EXERCICE 4. Soient G un groupe et H un sous-groupe d'indice fini $n \geq 2$.

1. Montrer qu'il existe un sous-groupe distingué K de G , contenu dans H , tel que $[G : K]$ divise $n!$ et $[H : K] \mid (n-1)!$.
Indication : On pourra considérer l'action de G sur G/H .
2. **APPLICATION 1 :** Montrer que si H est d'indice 2 dans G , alors H est distingué dans G . Le démontrer également de façon plus élémentaire.
3. **APPLICATION 2 :** Montrer que si G est un p -groupe, et si H est d'indice p dans G , alors H est distingué dans G .
4. **APPLICATION 3 :** Supposons que G est fini et que $m = [G : H]$ est le plus petit diviseur premier de l'ordre de G . Montrer que H est distingué dans G .
5. On suppose que G est fini. Montrer que G n'est pas la réunion des conjugués gHg^{-1} de H .
6. Montrer que 2. reste vrai si G est infini.
7. Est-ce que 2. reste vrai si on ne suppose plus que $[G : H]$ est fini?
8. Soit G un groupe fini agissant transitivement sur un ensemble fini X tel que $\#X \geq 2$. Montrer qu'il existe $g \in G$ ne fixant aucun point de X .
9. Soit $k \geq 5$ un entier et soit H un sous-groupe de \mathfrak{S}_k d'indice compris entre 2 et $k-1$. Montrer que $H = \mathfrak{A}_k$. On admettra le fait que les seuls sous-groupes distingués de \mathfrak{S}_k sont $\{1\}, \mathfrak{A}_k$ et \mathfrak{S}_k .

SOLUTION.

1. Faisant agir G sur G/H , on obtient un morphisme $h : G \rightarrow \mathfrak{S}(G/H) \cong \mathfrak{S}_n$. Montrons que le noyau de h convient. Attention ici qu'on n'a pas supposé G fini et donc $[G : \text{Ker}(h)]$ n'est pas donné par $\#G/\#\text{Ker}(h)$. Le théorème de factorisation fournit un morphisme injectif $\tilde{h} : G/\text{Ker}(h) \rightarrow \mathfrak{S}(G/H) \cong \mathfrak{S}_m$. On peut ainsi identifier $G/\text{Ker}(h)$ à un sous-groupe de \mathfrak{S}_m et en déduire par Lagrange que $[G : \text{Ker}(h)] \mid m!$.

Soit $g \in \text{Ker}(h)$. On a alors pour tout $a \in G$, $gaH = aH$ qui implique immédiatement que $g \in H$. On peut aussi utiliser le résultat rappelé dans le complément en bas de page 5 qui stipule que le noyau du morphisme $h : G \rightarrow \mathfrak{S}(X)$ associé à une action du groupe G sur un ensemble X est donné par

$$\text{Ker}(h) = \bigcap_{x \in X} \text{Stab}_G(x).$$

Or, ici on obtient immédiatement par double inclusion que $\text{Stab}_G(aH) = aHa^{-1}$ de sorte que

$$\text{Ker}(h) = \bigcap_{a \in G} aHa^{-1} \subseteq H.$$

On restreint alors l'action précédente en une action de H sur G/H et utilisé le fait que puisque H est un point fixe de G/H pour cette action, cela donne lieu à une action de H sur $G/H \setminus \{H\}$ de même noyau que h . De manière plus générale, si un groupe G agit sur X et que l'on dispose d'un élément $x_0 \in X$ appartenant à l'intersection des fixateurs pour $g \in G$, autrement dit tel que pour tout $g \in G$, $g \cdot x_0 = x_0$, alors l'action de G sur X induit par restriction une action de G sur $X \setminus \{x_0\}$. En effet, si $x \in X \setminus \{x_0\}$, alors pour tout $g \in G$, $g \cdot x \in X \setminus \{x_0\}$ car sinon $g \cdot x = x_0$ et donc en faisant agir g^{-1} , $x = g^{-1} \cdot x_0$ mais $g^{-1} \cdot x_0 = x_0$, ce qui fournit une contradiction! On a alors que l'action de G sur X fournit un morphisme $h : G \rightarrow \mathfrak{S}(X)$ et celle restreinte à $X \setminus \{x_0\}$ un morphisme $h_2 : G \rightarrow \mathfrak{S}(X \setminus \{x_0\})$ et

$$\text{Ker}(h) = \bigcap_{x \in X} \text{Stab}_G(x) = \bigcap_{x \in X \setminus \{x_0\}} \text{Stab}_G(x)$$

car par définition, $\text{Stab}_G(x_0) = G$. Or,

$$\text{Ker}(h_2) = \bigcap_{x \in X \setminus \{x_0\}} \text{Stab}_G(x) \quad \text{de sorte que} \quad \text{Ker}(h) = \text{Ker}(h_2).$$

Le même raisonnement que ci-dessus permet alors de conclure que $K = \text{Ker}(h)$ convient.

► **REMARQUE.** – On ne peut pas utiliser ici le troisième théorème d'isomorphisme car je rappelle que ce théorème garantit que si $N \triangleleft G$ et $H \triangleleft G$ avec $N \leq H$, alors $H/N \triangleleft G/N$ et l'application $f : G/N \rightarrow G/H$ qui à gN associe gH est bien définie de noyau H/N et passe au quotient pour donner un isomorphisme $(G/N)/(H/N) \cong G/H$. L'hypothèse que les deux groupes sont distingués est importante sinon G/H ou G/N n'a pas de structure de groupe et H/N n'est pas nécessairement distingué dans G/N . Par ailleurs, comme vous le verrez dans le cours, le fait qu'on ait un isomorphisme $G/H \cong N$ **n'implique pas** que $G \cong H \times N$ et en particulier ici on n'a pas nécessairement $G/N \cong G/H \times H/N$ (penser par exemple à $G = \mathbf{H}_8$, $H = Z(\mathbf{H}_8) \cong \mathbf{Z}/2\mathbf{Z}$ et $N = G/H \cong (\mathbf{Z}/2\mathbf{Z})^2$). En revanche, on a bien dans tous les cas une **bijection** entre G/N et $G/H \times H/N$. Cela est évident par cardinalité si G est fini mais ici ce n'est pas dans les hypothèses et il faut alors remarquer que l'application ensembliste surjective (l'ensemble d'arrivée n'étant pas nécessairement un groupe) $f : G/\text{Ker}(h) \rightarrow G/H$ qui à $g\text{Ker}(h)$ associe gH est bien définie et passe au quotient pour la relation donnée par le groupe $H/\text{Ker}(h)$ pour donner une application surjective (par surjectivité de f). En effet, si $gN = g'N$ avec $g'^{-1}g \in H$, alors on a bien $gH = g'H$. L'application quotient est alors injective si, et seulement si, $gH = g'H$ implique que gN et $g'N$ sont en relation pour la relation d'équivalence associée à H/N . Cela est clairement le cas et fournit la bijection souhaitée. En conclusion, il faut être prudent avec ce théorème d'isomorphisme et dans cette question, on ne pouvait pas l'utiliser directement mais uniquement en redémontrant une version "bijection" puisqu'un des sous-groupes, à savoir H , n'est pas supposé distingué et que G n'est pas supposé fini. Une fois la **bijection** $G/\text{Ker}(h) \cong G/H \times H/\text{Ker}(h)$ obtenue, on peut alors dire que $[G : \text{Ker}(h)] = [G : H] \times [H : \text{Ker}(h)]$ et donc $[G : H] \times [H : \text{Ker}(h)] = m \times [H : \text{Ker}(h)] \mid m!$ et finalement $[H : \text{Ker}(h)] \mid (m-1)!$.

2. On a $m = 2$ et la question 4. fournit alors que $[H : \text{Ker}(h)] = 1$ soit $H = \text{Ker}(h)$. Ainsi $H \triangleleft G$. On donne une démonstration plus élémentaire dans l'exercice 8 mais celle-ci a l'avantage de se généraliser comme on va le voir en question 7.
3. On a donc que G et H sont finis de cardinal une puissance de p . Par 4., on a donc $\#H \mid (p-1)!\# \text{Ker}(h)$. Mais $\#H$ est premier avec $(p-1)!$ donc $\#H \mid \# \text{Ker}(h)$ et la question 3. permet alors de conclure à nouveau à l'égalité $H = \text{Ker}(h)$. Ainsi $H \triangleleft G$. Noter que l'indice d'un sous-groupe H d'un p -groupe est une puissance de p et que dès que l'indice est supérieur à p le raisonnement tombe en défaut. Il est en réalité faux comme en témoigne l'exemple du groupe \mathbf{D}_4 qui est un 2-groupe dont certains sous-groupes d'ordre 2 (et donc d'indice 4) ne sont pas distingués comme on a pu le voir lors de l'exercice 2.
4. De même, $\#H \mid (m-1)!\# \text{Ker}(h)$ et $\#H = \#G/m$ ne contient que des facteurs premiers $\geq m$ et donc $\#H$ est premier avec $(m-1)!$ et on conclut comme en question précédente. Idem, le raisonnement et le résultat tombent en défaut dès qu'on autorise des indices qui ne sont pas le plus petit facteur premier du cardinal de G , comme par exemple un sous-groupe d'ordre 3 (engendré par un 3-cycle) dans \mathfrak{S}_4 .
5. On a clairement que ²⁵

$$\bigcup_{g \in G} gHg^{-1} = \bigcup_{\bar{g} \in G/H} gHg^{-1}.$$

où gHg^{-1} ne dépend que de la classe de g dans G/H car $(gh)H(gh)^{-1} = gHg^{-1}$. Il vient par conséquent que (bien faire attention ici que e appartient à chacun des conjugués)

$$\begin{aligned} \# \left(\bigcup_{g \in G} gHg^{-1} \setminus \{e\} \right) &= \# \left(\bigcup_{\bar{g} \in G/H} gHg^{-1} \setminus \{e\} \right) \\ &\leq \sum_{\bar{g} \in G/H} \# (gHg^{-1} \setminus \{e\}) \\ &\leq \sum_{\bar{g} \in G/H} \# (H \setminus \{e\}) \leq \#(G/H)(\#H - 1) = \#G \left(1 - \frac{1}{\#H} \right) < \#G - 1 \end{aligned}$$

car $H \neq G$ si bien que

$$\# \left(\bigcup_{g \in G} gHg^{-1} \setminus \{e\} \right) < \#(G \setminus \{e\}) \quad \text{et} \quad \bigcup_{g \in G} gHg^{-1} \neq G.$$

6. On dispose toujours de l'action de G sur G/H qui fournit un morphisme $\varphi : G \rightarrow \mathfrak{S}(G/H)$ avec $\mathfrak{S}(G/H)$ un groupe fini. On note alors K le sous-groupe de $\mathfrak{S}(G/H)$ des bijections fixant H et on a alors que $\varphi(H)$ est un sous-groupe de K . Par ailleurs, la transitivité

²⁵. Noter qu'alors, puisque gHg^{-1} est un sous-groupe de G , si H est d'indice 2, cela entraînerait que G est la réunion de deux sous-groupes, aucun n'étant inclus dans l'autre, ce qui est impossible! On a un résultat similaire pour les espaces vectoriels. Attention en revanche que ce résultat ne se généralise pas à strictement plus de deux groupes ou espace vectoriels car par exemple

$$\mathfrak{S}_3 = \mathfrak{A}_3 \cup \langle (12) \rangle \cup \langle (13) \rangle \cup \langle (23) \rangle \quad \text{ou} \quad \mathbf{F}_2^2 = \text{Vect}(1, 0) \cup \text{Vect}(0, 1) \cup \text{Vect}(1, 1).$$

En revanche, dans le cas d'un espace vectoriel E sur un corps k **infini**, on a bien que

$$E \neq F_1 \cup F_2 \cup \dots \cup F_n$$

pour tous F_1, F_2, \dots, F_n des sous-espaces vectoriels stricts de E . En effet, on peut supposer $F_n \not\subseteq F_1 \cup F_2 \cup \dots \cup F_{n-1}$ et choisir $x \in F_n \setminus F_1 \cup F_2 \cup \dots \cup F_{n-1}$ et $y \notin F_n$. On a alors que pour tout $\lambda \in k$, $\lambda x + y \notin F_n$ et pour tout $i \leq n-1$, il existe au plus un $\lambda \in k$ tel que $\lambda x + y \in F_i$, ce qui vient contredire le caractère infini du corps k . En effet, si on dispose de $\lambda \neq \mu$ tels que $\lambda x + y$ et $\mu x + y$ sont dans F_i , alors $(\lambda - \mu)x \in F_i$ ce qui est absurde!

de l'action garantit que $\varphi(G)$ n'est pas contenu dans K (puisque contenant des bijections qui envoient H sur n'importe quel autre classe à gauche aH avec $a \in G \setminus H$) donc $\varphi(H)$ est un sous-groupe strict du groupe fini $\varphi(G)$ et la question précédente entraîne alors que

$$\bigcup_{g \in G} \varphi(g)\varphi(H)\varphi(g)^{-1} \neq \varphi(G).$$

Ainsi nécessairement

$$\bigcup_{g \in G} gHg^{-1} \neq G.$$

7. Le résultat devient alors faux en général. On pose $G = GL_n(\mathbb{C})$ et $H = T_n(\mathbb{C}) \cap G$ le sous-groupe des matrices triangulaires supérieures inversibles. On sait alors que toute matrice de G est trigonalisable, autrement dit conjuguée à une matrice de $T_n(\mathbb{C})$ de sorte que

$$\bigcup_{g \in G} gHg^{-1} = G$$

mais H est d'indice infini dans G . Pour voir que l'indice est infini (autrement que par l'absurde en utilisant la question précédente), on peut par exemple utiliser le fait que toute matrice M de $GL_n(\mathbb{C})$ s'écrit sous la forme $M = \exp(N) = \left(\exp\left(\frac{N}{n}\right)\right)^n$ et donc toute matrice de $GL_n(\mathbb{C})$ est une puissance n -ième pour tout entier naturel n .

Supposons alors que $GL_n(\mathbb{C})$ possède un sous-groupe H d'indice fini non trivial, disons d'indice $r \geq 2$. On sait (comme en question 1.) qu'on peut trouver un sous-groupe K distingué de $GL_n(\mathbb{C})$ tel que $K \subseteq H$. Le fait que H soit d'indice fini implique que K est d'indice fini²⁸, disons d'indice $m \geq 2$ (car $m \geq r$ puisque $K \subseteq H$). Pour toute matrice $M \in GL_n(\mathbb{C})$, il existe B telle que $M = B^m$ et ainsi la classe de M dans le **groupe** quotient $GL_n(\mathbb{C})/K$ est triviale si bien que ce dernier quotient est nécessairement trivial et $K = GL_n(\mathbb{C})$. Cela impliquerait que $H = GL_n(\mathbb{C})$, ce qui est exclu puisqu'on a supposé $r \geq 2$. Ainsi, on a qu'un seul sous-groupe d'indice fini dans $GL_n(\mathbb{C})$, c'est lui-même, d'indice 1. Puisque $T_n(\mathbb{C}) \neq GL_n(\mathbb{C})$, on en déduit qu'il est nécessairement d'indice infini.

8. On choisit $x_0 \in X$ et on note $H = \text{Stab}_G(x_0)$. On a alors que H est un sous-groupe de G différent de G (sinon $X = \{x_0\}$ par transitivité). On peut donc trouver $g_0 \in G$, $g_0 \notin \bigcup_{g \in G} gHg^{-1}$. Soit alors $x \in X$. On sait qu'il existe $g \in G$ tel que $x = g \cdot x_0$ et alors

$\text{Stab}_G(x) = gHg^{-1}$ donc par construction $g_0 \notin \text{Stab}_G(x)$, ce qui signifie que $g_0 \cdot x \neq x$ ce qui conclut la preuve.

Noter que par conséquent, pour une action transitive, tous les stabilisateurs sont conjugués! Et ici, on cherchait en réalité un élément de

$$\bigcap_{x \in X} \overline{\text{Stab}_G(x)}$$

où \overline{E} représente le complémentaire de l'ensemble E . On cherchait donc un élément de G qui n'appartienne pas à

$$\bigcup_{x \in X} \text{Stab}_G(x) = \bigcup_{g \in G} gHg^{-1} \quad \text{pour } H = \text{Stab}_G(x_0).$$

9. Par 1., H contient un sous-groupe distingué K de \mathfrak{S}_k d'indice divisant $[\mathfrak{S}_k : H]!$. Comme H n'est pas d'indice 1, ce groupe ne peut pas être \mathfrak{S}_k tout entier sinon $H = \mathfrak{S}_k$ serait d'indice 1. Ce sous-groupe est donc (puisque $k \geq 5$) soit le groupe trivial soit le groupe alterné. Supposons qu'il s'agisse du groupe trivial. On a alors que $k!$ divise $[\mathfrak{S}_k : H]! \in \{2!, \dots, (k-1)!\}$ ce qui est absurde donc $K = \mathfrak{A}_k$ et $K \subseteq H$ donc $[G : H] \leq [G : K]$ si bien que $[G : H] = 2$ et $H = \mathfrak{A}_k$ puisque le seul²⁹ sous-groupe d'indice 2 de \mathfrak{S}_k est le groupe alterné.

Noter qu'on a un sous-groupe d'indice 1, à savoir \mathfrak{S}_k tout entier, et des sous-groupes d'indice k , à savoir³⁰ les

$$\mathfrak{S}_k(i) = \{\sigma \in \mathfrak{S}_k : \sigma(i) = i\} \cong \mathfrak{S}_{k-1}$$

pour tout $i \in \{1, \dots, k\}$.

26. Un autre exemple est $G = SO_3(\mathbb{R})$ et $H = SO_2(\mathbb{R})$ comme sous-groupe des rotations autour de l'axe des abscisses. Alors toute rotation étant conjuguée à une rotation d'axe fixé, on a un autre contre-exemple.

27. On dit que le groupe $GL_n(\mathbb{C})$ est *divisible*.

28. En effet, $K = \text{Ker}(h)$ et on peut plonger $GL_n(\mathbb{C})/K$ dans $\mathfrak{S}(GL_n(\mathbb{C})/H) \cong \mathfrak{S}_r$ via l'action de $GL_n(\mathbb{C})$ sur $GL_n(\mathbb{C})/H$ par translation à gauche.

29. Cela découle soit du fait que l'on connaît tous les sous-groupes de \mathfrak{S}_n pour $n \leq 4$ et les sous-groupes distingués de \mathfrak{S}_n pour $n \geq 5$ ou plus simplement du fait qu'un sous-groupe d'indice 2 donne lieu au quotient à un morphisme surjectif (donc non trivial) de $\mathfrak{S}_n \rightarrow \{\pm 1\}$. Or, le seul morphisme non trivial de \mathfrak{S}_n dans le groupe multiplicatif $\{\pm 1\}$ est la signature. Cela se voit en montrant qu'une transposition est nécessairement envoyée sur -1 et en utilisant le fait que les transpositions engendrent \mathfrak{S}_n . Il existe au moins une transposition envoyée sur -1 sinon puisqu'elles engendrent \mathfrak{S}_n , le morphisme est trivial mais alors puisque toutes les transpositions sont conjuguées et que $\{\pm 1\}$ est abélien, toutes les transpositions ont la même image, à savoir -1 , ce qui permet de conclure.

30. On peut même établir que ce sont les seuls en utilisant des arguments similaires à ceux du complément à la fin de l'exercice 1!

Exercices complémentaires semaine 1

EXERCICE 5 — GROUPES D'EXPOSANT 2.

1. Soit G un groupe tel que $g^2 = 1$ pour tout $g \in G$. Montrer que G est abélien et donner des exemples de tels groupes finis et infinis.
2. Montrer que si G est fini, il existe un entier n tel que G est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^n$.

SOLUTION.

1. Pour tous $g, h \in G$, on a $(gh)^2 = 1$ soit $ghgh = 1$ et en multipliant à droite par hg il vient $hg^2hgh = hg$ soit $h^2gh = hg$ soit $gh = hg$ et G est abélien. On verra en question suivante que les groupes finis d'exposant 2 sont tous de la forme $(\mathbf{Z}/2\mathbf{Z})^n$ pour un certain entier n . Un exemple de tel groupe infini est $\prod_{i \in I} \mathbf{Z}/2\mathbf{Z}$ avec I infini, par exemple $(\mathbf{Z}/2\mathbf{Z})^{\mathbb{N}}$ l'ensemble des suites à valeurs dans $\mathbf{Z}/2\mathbf{Z}$.

2. • **Méthode 1 :** Puisque G est fini, il admet une partie génératrice minimale³¹, disons $\{g_1, \dots, g_n\}$. On a alors par définition d'une partie génératrice et en utilisant le fait que G est abélien dont tout élément distinct du neutre est son propre inverse par la question précédente, que

$$G = \{g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n} : \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n \in \{0, 1\}\}.$$

Cela donne envie de poser

$$f : \begin{cases} (\mathbf{Z}/2\mathbf{Z})^n & \longrightarrow G \\ (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) & \longmapsto g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n}. \end{cases}$$

On a aisément qu'il s'agit d'un morphisme et par ce qui précède, il est surjectif. Reste à voir qu'il est injectif pour conclure! Si ce n'est pas le cas, il existe un élément non trivial $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \neq (0, 0, \dots, 0)$ dans le noyau, autrement dit tel que

$$g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n} = 1.$$

Sans perte de généralités, on peut supposer que $\varepsilon_1 \neq 0$ et donc $\varepsilon_1 = 1$. On a donc

$$g_1 g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n} = 1 \quad \text{soit} \quad g_1 = g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n}$$

et $\{g_2, \dots, g_n\}$ est une partie génératrice de G , contredisant la minimalité de $\{g_1, g_2, \dots, g_n\}$. Cela démontre l'injectivité et donc f est un isomorphisme qui permet de conclure!

- **Méthode 2 :** On considère $(G, +)$ muni d'une loi additive³² d'exposant 2, autrement dit tel que pour tout $g \in G$, $2g = 0$. On a alors que $\mathbf{Z}/2\mathbf{Z}$ est un corps et on vérifie que G est muni d'une structure de $\mathbf{Z}/2\mathbf{Z}$ -espace vectoriel muni de la loi $+$ et de la loi externe suivante

$$\forall \bar{k} \in \mathbf{Z}/2\mathbf{Z}, \quad \forall g \in G, \quad \bar{k} \cdot g = kg$$

qui est bien définie car si $\bar{k} = \bar{k}'$, alors il existe un entier ℓ tel que $k' = k + 2\ell$ si bien que

$$k'g = kg + 2\ell g = 0 \quad \text{car} \quad 2\ell g = \ell(2g) = 0.$$

On vérifie alors que $(G, +, \cdot)$ est un $\mathbf{Z}/2\mathbf{Z}$ -espace vectoriel. Comme G est une famille génératrice finie, il est de dimension finie. On sait donc que si $n = \dim_{\mathbf{Z}/2\mathbf{Z}}(G) = n$, alors³³ $G \cong (\mathbf{Z}/2\mathbf{Z})^n$, en tant que $\mathbf{Z}/2\mathbf{Z}$ -espaces vectoriels. Mais, un isomorphisme de $\mathbf{Z}/2\mathbf{Z}$ -espaces vectoriels est en particulier un isomorphisme des groupes additifs sous-jacents si bien qu'on $G \cong (\mathbf{Z}/2\mathbf{Z})^n$ en tant que groupes, et on retrouve bien le résultat!

► **COMPLÉMENTS .** – On peut se demander pour quels entiers e , un groupe d'exposant³⁴ e est-il nécessairement commutatif. Clairement $e = 1$ ou 2 convient d'après 1 et ce sont les seuls. Si $e \geq 3$ divisible par 4, alors $\mathbf{Z}/e\mathbf{Z} \times \mathbf{H}_8$ est d'exposant e et non commutatif. Si maintenant $4 \nmid e$, alors e admet un facteur premier impair et $\mathbf{Z}/e\mathbf{Z} \times U(p)$ avec $U(p)$ le sous-groupe de $\text{GL}_p(\mathbf{F}_p)$ formé des matrices triangulaires supérieures avec des 1 sur la diagonale est d'exposant e car pour toute matrice $M \in U(p)$, $(M - I_p)^p = 0$ et comme on est en caractéristique p , $M^p = I_p$.

EXERCICE 6 — GROUPES DE TYPE FINI. Soit G un groupe admettant une partie génératrice finie. Montrer que G est fini ou dénombrable. Est-il vrai réciproquement que tout groupe dénombrable admet une partie génératrice finie?

SOLUTION. Soit S une partie génératrice de G . Notons T l'ensemble des éléments de G qui sont dans S ou dont l'inverse est dans S . Pour tout $r \in \mathbb{N}$, notons G_r l'ensemble des éléments g de G de la forme

$$g = x_1 x_2 \cdots x_r,$$

31. En effet, G (qui est fini) engendre G donc le cardinal des familles génératrices est une partie non vide de \mathbb{N} qui admet donc un plus petit élément.

32. On prend cette convention pour coller à la définition usuelle d'un espace vectoriel. De plus, on a établi qu'un groupe d'exposant 2 est commutatif et on note usuellement une loi commutative $+$.

33. Noter qu'une base étant une famille génératrice minimale, on fait en fait la même chose que dans la première méthode!

34. On dit qu'un groupe G est d'exposant e si pour tout $g \in G$, $g^e = 1$.

avec $x_i \in T$ pour tout i (avec la convention habituelle que le produit vide est le neutre de G). Alors, le fait que S engendre G dit que G est la réunion des G_r pour $r \in \mathbb{N}$. Chaque G_r est fini (car T est fini, et le cardinal de G_r est au plus celui de T^r), donc G est (au plus) dénombrable comme union dénombrable d'ensembles finis.

La réciproque est fautive, même pour les groupes abéliens. Par exemple, $(\mathbb{Q}, +)$ n'est pas engendré par une partie finie (par l'absurde si on a une partie génératrice finie $p_1/q_1, \dots, p_n/q_n$, alors tout élément de \mathbb{Q} aurait un dénominateur sous forme réduite qui divise $q_1 \cdots q_n$ mais ce n'est pas le cas de $1/(1 + q_1 \cdots q_n)$ par exemple). De même pour $\mathbb{Z}^{(\mathbb{N})}$ (qui admet une famille libre infinie).

► **REMARQUE .** – Noter que la forme d'un élément de G , par définition du fait que S engendre G donne immédiatement une application f surjective³⁵ de $E = \{(x_1, \dots, x_r) \in S \cup S^{-1} : r \in \mathbb{N}\}$ (qui est dénombrable par des arguments similaires). L'axiome du choix garantit alors l'existence d'une section $s : G \rightarrow E$ telle que $f \circ s = \text{Id}_G$. Ainsi, s est injective et arrive dans un ensemble dénombrable donc G est dénombrable.

EXERCICE 7. On considère le groupe $G = \mathfrak{A}_4$. Soit $D(G)$ son sous-groupe dérivé. Soit V_4 le sous-groupe de G constitué de l'identité et des doubles transpositions.

1. Montrer que $V_4 \triangleleft G$, puis que $D(G) \subseteq V_4$. *Indication : On observera que G/V_4 est de cardinal 3.*
2. Montrer que $D(G) \neq \{1\}$ et que G ne possède pas de sous-groupe distingué de cardinal 2. En déduire que $D(G) = V_4$.
3. Montrer que si H est un sous-groupe d'indice 2 d'un groupe fini A , alors $H \triangleleft A$.
Indication : Regarder les classes à gauche et à droite suivant G .
4. Soit H un sous-groupe de $G = \mathfrak{A}_4$. Montrer que si H est d'indice 2, alors $D(G) \subseteq H$ et aboutir à une contradiction.
Indication : On considérera G/H .
Ainsi G (qui est de cardinal 12) n'a pas de sous-groupe de cardinal 6.
5. Montrer au contraire que pour tout $d \in \mathbb{N}^*$ tel que d divise 24, le groupe \mathfrak{S}_4 possède un sous-groupe de cardinal d .

SOLUTION.

1. Si l'on conjugue la double transposition $(a, b)(c, d)$ par une permutation σ , on obtient $(\sigma(a), \sigma(b))(\sigma(c), \sigma(d))$, ce qui montre que V_4 est distingué dans \mathfrak{S}_4 , et donc a fortiori dans \mathfrak{A}_4 . Ensuite, comme G/V_4 est de cardinal $12/4 = 3$, il est cyclique de cardinal 3 (car 3 est premier) et en particulier abélien, ce qui montre que $D(G) \subseteq V_4$.
2. On voit facilement que G n'est pas abélien, donc $D(G) \neq \{1\}$. D'autre part un sous-groupe H de G de cardinal 2 est composé de l'identité et d'une double transposition $\tau = (a, b)(c, d)$. Si l'on conjugue τ par $\sigma \in G$, on obtient $(\sigma(a), \sigma(b))(\sigma(c), \sigma(d))$, qui ne reste pas dans H si on choisit par exemple $\sigma \in G$ telle que $\sigma(a) = a$ et $\sigma(b) = c$, ce qui est toujours possible. On a vu que $D(G) \subseteq V_4$, donc le cardinal de $D(G)$ divise 4, mais on a aussi vu que ce ne peut être ni 1 ni 2, donc c'est 4 et $D(G) = V_4$.
3. Soit $a \notin H$. Comme le cardinal de l'ensemble G/H des classes à gauche est 2, cet ensemble est composé de H et de la classe aH , qui est le complémentaire de H dans A . De même l'ensemble $H \backslash G$ des classes à droite est composé de H et de Ha , qui est aussi le complémentaire de H dans A . Ainsi $aH = Ha$, et ceci reste vrai quand $a \in H$. Finalement $aHa^{-1} = H$ pour tout $a \in A$, autrement dit $H \triangleleft A$.
4. D'après 4., on a $H \triangleleft G$. Alors, le groupe G/H est abélien puisque de cardinal 2, ce qui montre que $H \supseteq D(G)$. Mais d'après c), le groupe $D(G)$ est de cardinal 4 alors que H est de cardinal 6, ce qui contredit le théorème de Lagrange.
5. C'est clair pour $d = 1$ et $d = 24$. Pour $d = 2$, on prend le groupe engendré par une transposition, pour $d = 3$ celui engendré par un 3-cycle et pour $d = 4$ celui engendré par un 4-cycle. Pour $d = 6$, le sous-groupe des permutations laissant fixe 1 est isomorphe à \mathfrak{S}_3 , il est donc de cardinal 6. Pour $d = 12$, on prend le sous-groupe \mathfrak{A}_4 . Reste le cas $d = 8$, auquel cas on a un sous-groupe isomorphe au groupe diédral \mathbf{D}_4 , par exemple celui engendré par un 4-cycle et une transposition.

35. Qui à un élément de $\{(x_1, \dots, x_r) \in S \cup S^{-1} : r \in \mathbb{N}\}$ associe $x_1 x_2 \cdots x_r$.

Exercices fondamentaux semaine 2

EXERCICE 8. Montrer que tout groupe d'ordre 255 est cyclique.

SOLUTION. Soit G d'ordre $255 = 3 \times 5 \times 17$. On sait par les théorèmes de Sylow que le nombre n_3 de 3-Sylow vaut 1 ou 85 (car il divise 85 et est congru à 1 modulo 3), celui n_5 des 5-Sylow vaut 1 ou 51 et on a un unique 17-Sylow, que l'on notera S_{17} . On ne peut pas avoir $n_3 = 85$ et $n_5 = 51$ car sinon on obtiendrait au moins $85 \times 2 + 51 \times 4 = 374$ éléments dans G . On a donc $n_3 = 1$ ou $n_5 = 1$. Supposons $n_3 = 1$ l'unique 3-Sylow. On est alors tenté d'établir que le morphisme

$$f : \begin{cases} S_5 \times S_3 \times S_{17} & \longrightarrow & G \\ (s_5, s_3, s_{17}) & \longmapsto & s_5 s_3 s_{17} \end{cases}$$

est un isomorphisme. En effet, pour établir qu'il s'agit d'un morphisme, il s'agit de montrer que pour tous $(s_5, s_3, s_{17}), (s'_5, s'_3, s'_{17}) \in S_5 \times S_3 \times S_{17}$, alors

$$s_5 s_3 s_{17} s'_5 s'_3 s'_{17} = s_5 s'_5 s_3 s'_3 s_{17} s'_{17}.$$

Puisque $S_{17} \triangleleft G$, on sait que $S_3 S_{17} = S_{17} S_3$ et $s'_3 s'_{17} = (s'_3 s'_{17} s'_3)^{-1} s'_3$. Mais comme S_3 est aussi distingué, on a

$$s'_3 s'_{17} s'_3^{-1} s'_{17}^{-1} \in S_{17} \cap S_3 = \{e\} \quad \text{si bien que} \quad s'_3 s'_{17} s'_3^{-1} = s'_{17}.$$

En d'autres termes, S_3 et S_{17} commutent. On a donc

$$s_5 s_3 s_{17} s'_5 s'_3 s'_{17} = s_5 s_3 s_{17} s'_5 s'_{17} s'_3.$$

Pour pouvoir continuer, on aurait besoin de savoir que S_5 commute avec S_3 et S_{17} mais cela n'est pas évident *a priori* (en tout cas par des arguments de comptage). Si on parvient à le démontrer alors on obtient un morphisme injectif en utilisant les intersections triviales et surjectif en utilisant le fait que $S_3 S_5 S_{17} = G$ et on peut donc conclure. Une façon de le faire est de considérer G/S_{17} qui est un groupe d'ordre $15 = 3 \times 5$ avec $3 \nmid 5 - 1 = 4$ donc $G/S_{17} \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$ contient un unique sous-groupe normal K d'ordre 5. En considérant alors la surjection canonique $\pi : G \rightarrow G/S_{17}$, il vient que $C = \pi^{-1}(K)$ est un sous-groupe distingué de G contenant S_{17} . Par les théorèmes d'isomorphisme, $\#C = \#K \times \#S_{17} = 85 = 5 \times 17$ avec $5 \nmid 17$ donc d'après le cours, un tel groupe est cyclique possédant donc un unique 5-Sylow C_5 (qui est aussi un 5-Sylow de G par cardinalité). Montrons que C_5 est distingué. Soit $g \in G$. On a alors

$$g C_5 g^{-1} \subseteq g C g^{-1} = C \quad \text{car} \quad C \triangleleft G.$$

Ainsi, $g C_5 g^{-1}$ est un 5-Sylow de C qui n'en possède qu'un seul, à savoir C_5 donc $g C_5 g^{-1} = C_5$ et on a gagné. En réalité, de manière plus générale, si un groupe G possède pour tout $p \mid \#G$ un unique p -Sylow, alors il est produit direct de ses p -Sylow et est nilpotent en raisonnant comme ci-dessus ou comme dans l'exercice sur les groupes nilpotents. Noter qu'on peut établir qu'un groupe d'ordre pq avec $p \nmid q - 1$ si $p < q$ sont deux nombres premiers distincts sans recourir au produit semi-direct par des arguments de cardinalité! En effet, un tel groupe possède un unique p -Sylow et un unique q -Sylow et alors on a au plus $1 + p - 1 + q - 1 = p + q - 1$ éléments d'ordre 1, p ou q . Or, $p + q - 1 < pq$ car $p + q - 1 < 2q - 1 \leq 2q < pq$ dès que $p > 2$. Si maintenant $p = 2$, il vient $p + q - 1 = q + 1 < 2q$. Dans tous les cas, il existe nécessairement un élément d'ordre pq et le groupe est cyclique! Noter que cela implique que G est produit de ses p -Sylow (ou plus simplement abélien) et donc nilpotent.

► **COMPLÉMENT.** – Voici une autre approche pour celles et ceux qui connaissent le produit semi-direct. Notons alors S_5 un 5-Sylow quelconque. On a alors

- a) $S_3 S_{17} \cong S_3 \times S_{17} \triangleleft G$ car $S_3 \triangleleft G$ et $S_{17} \triangleleft G$ (en appliquant le critère du cours);
- b) $S_3 S_{17} \cap S_5 = \{e\}$ (pour des raisons de cardinalité);
- c) $S_3 S_5 S_{17} = G$ (idem pour des raisons de cardinalité car il contient 3×17 éléments distincts dans $S_3 S_{17}$ et tous les gs pour $g \in S_3 S_{17}$ et $s \in S_5$ qui sont tous distincts).

On a donc $G = S_3 S_{17} \rtimes S_5$ associé à un morphisme $\varphi : S_5 \rightarrow \text{Aut}(S_3 S_{17})$. On a alors $^{37} \text{Aut}(S_3 S_{17}) \cong \text{Aut}(\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/17\mathbf{Z}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/16\mathbf{Z}$ donc le morphisme φ est nécessairement trivial (on n'a aucun élément d'ordre 5 à l'arrivée) et le produit direct. Par le lemme

36. En effet, il est clair qu'en considérant l'ordre d'un élément g de l'intersection d'un 3-Sylow et d'un 5-Sylow, que cet ordre doit diviser 3 et 5 et est donc égal à 1 si bien qu'un 3-Sylow et un 5-Sylow sont disjoints mais aussi que puisque les 3-Sylow (et les 5-Sylow) sont cycliques d'ordre premier (et ainsi tout élément non trivial en est un générateur), que l'intersection de deux 3-Sylow (et de deux 5-Sylow) distincts est trivial.

37. En effet, on a par ce qui précède et le théorème chinois que $S_3 S_{17} \cong S_3 \times S_{17} \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/17\mathbf{Z} \cong \mathbf{Z}/51\mathbf{Z}$. Or, deux groupes isomorphes ont des groupes d'automorphismes isomorphes donc $\text{Aut}(S_3 S_{17}) \cong \text{Aut}(\mathbf{Z}/51\mathbf{Z})$. Le cours garantit alors que $\text{Aut}(\mathbf{Z}/51\mathbf{Z}) \cong (\mathbf{Z}/51\mathbf{Z})^\times$ et le théorème chinois fournit à nouveau $(\mathbf{Z}/51\mathbf{Z})^\times \cong (\mathbf{Z}/3\mathbf{Z})^\times \times (\mathbf{Z}/17\mathbf{Z})^\times$. Pour finir, on sait alors par le cours que $(\mathbf{Z}/3\mathbf{Z})^\times \cong \mathbf{Z}/2\mathbf{Z}$ et $(\mathbf{Z}/17\mathbf{Z})^\times \cong \mathbf{Z}/16\mathbf{Z}$. **Attention** qu'en général, pour deux groupes G_1 et G_2 , on a $\text{Aut}(G_1 \times G_2) \not\cong \text{Aut}(G_1) \times \text{Aut}(G_2)$ défini par $\varphi \mapsto ([g_1 \mapsto \varphi(g_1, 1)], [g_2 \mapsto \varphi(1, g_2)])$ est un isomorphisme de réciproque $\text{Aut}(G_1) \times \text{Aut}(G_2) \rightarrow \text{Aut}(G_1 \times G_2)$ défini par $(\varphi_1, \varphi_2) \mapsto [(g_1, g_2) \mapsto (\varphi_1(g_1), \varphi_2(g_2))]$, comme on peut le voir avec $G_1 = G_2 = \mathbf{Z}/2\mathbf{Z}$ pour lesquels on a $\text{Aut}(G_1 \times G_2) \cong \text{GL}_2(\mathbf{Z}/2\mathbf{Z})$ tandis que $\text{Aut}(G_1) \times \text{Aut}(G_2) = \{\text{Id}\}$. En revanche, si le cardinal de G_1 et celui de G_2 sont premiers entre eux, alors on a bien $\text{Aut}(G_1 \times G_2) \cong \text{Aut}(G_1) \times \text{Aut}(G_2)$. En effet, $\text{Aut}(G_1) \times \text{Aut}(G_2) \rightarrow \text{Aut}(G_1 \times G_2)$ défini par $(\varphi_1, \varphi_2) \mapsto [(g_1, g_2) \mapsto (\varphi_1(g_1), \varphi_2(g_2))]$ est toujours un morphisme injectif et dans le cas où les ordres sont premiers entre eux, $\varphi \mapsto ([g_1 \mapsto \varphi(g_1, 1)], [g_2 \mapsto \varphi(1, g_2)])$ est un morphisme réciproque. Noter qu'en général il ne s'agit pas d'un morphisme comme en témoigne le contre-exemple ci-dessus (car il existe des isomorphismes de \mathbf{F}_2^2 qui ne stabilisent pas chacun des facteurs \mathbf{F}_2). Mais dans le cas où les ordres sont premiers entre eux, on obtient bien un morphisme car les sous-groupes $G_1 \times \{1\}$ et $\{1\} \times G_2$ sont caractéristiques (donc stables par tout automorphisme). Pour le voir, on peut dire que l'image de $G_1 \times \{1\}$ par un automorphisme φ de $G_1 \times G_2$ a même cardinal que G_1 et donc s'il contenait un élément de la forme $(g_1, g_2) \in G_1 \times G_2$ avec $g_2 \neq 1$. Mais, on peut alors si on note o_1 l'ordre de g_1 , obtenir que $(g_1^{o_1}, g_2^{o_1}) = (1, g_2^{o_1}) \in \varphi(G_1 \times \{1\})$. Mais puisque $o_1 \mid \#G_1$ qui est premier à $\#G_2$, alors $g_2^{o_1} \neq 1$. Ainsi, on a obtenu un élément de la forme $(1, g_2) \in \varphi(G_1 \times \{1\})$ avec $g_2 \neq 1$ mais cela implique que $\varphi(G_1 \times \{1\}) \cap (\{1\} \times G_2)$ est non trivial, ce qui est absurde puisqu'ils ont des cardinaux premiers entre eux.

chinois, on obtient donc que

$$G \cong S_3 \times S_5 \times S_{17} \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/17\mathbf{Z} \cong \mathbf{Z}/255\mathbf{Z}.$$

Enfin, une dernière approche est de faire agir G sur S_{17} par conjugaison (ce qui est possible car S_{17} est distingué). Cela fournit (puisque l'action a lieu par automorphismes) à un morphisme $f : G \rightarrow \text{Aut}(S_{17})$. On a alors

$$\text{Aut}(S_{17}) \cong \text{Aut}(\mathbf{Z}/17\mathbf{Z}) \cong (\mathbf{Z}/17\mathbf{Z})^* \cong \mathbf{Z}/16\mathbf{Z}.$$

Comme le cardinal de $\text{Aut}(S_{17})$ est premier à celui de G , ce morphisme est trivial et $S_{17} \subseteq Z(G)$. Mais alors G/S_{17} est cyclique car d'ordre pq avec $p < q$ et $q \nmid p-1$. Il s'ensuit que G est abélien. En effet, on peut démontrer que pour tout sous-groupe $H \leq Z(G)$, si G/H est cyclique, alors G est abélien. On conclut alors aisément au fait que l'application f est un isomorphisme ou par théorème de structure des groupes abéliens de type fini.

EXERCICE 9 — GROUPES RÉSOLUBLES.

1. Montrer que tout sous-groupe et tout groupe quotient d'un groupe résoluble est résoluble.
2. Montrer plus généralement que toute extension d'un groupe résoluble par un groupe résoluble est résoluble.
3. Donner un exemple d'un groupe résoluble qui n'est pas nilpotent.
4. Soient p et q deux nombres premiers distincts. Montrer que tout groupe d'ordre pq est résoluble.
5. Même question pour les groupes d'ordre pqr , si $p > q > r$ sont trois nombres premiers.
Indication : On pourra évaluer le nombre d'éléments d'ordre p et le nombre d'éléments d'ordre q .
6. Même question pour les groupes d'ordre p^2q .
Indication : On pourra être amené à comparer $1 + p$ et q .

SOLUTION.

La terminologie provient de la théorie de Galois. Le groupe de Galois du corps de décomposition d'un polynôme P à coefficients dans \mathbf{Q} est résoluble si, et seulement si, les racines de P sont exprimables par radicaux. Le fait que le groupe \mathfrak{S}_n ne soit plus résoluble dès que $n \geq 5$ explique pourquoi à partir du degré 5, il n'existe plus de méthode de résolution par radicaux (contrairement aux degrés 2, 3 et 4).

1. On utilise le fait que G est résoluble si, et seulement si il existe un entier n tel que $D^n(G) = \{e\}$. On constate alors que si $H \leq G$, pour tout n , $D^n(H) \leq D^n(G)$ donc H est résoluble. Soit maintenant $H \triangleleft G$ et considérons le groupe quotient G/H . On a alors le morphisme surjectif canonique $\pi : G \rightarrow G/H$ et par surjectivité, $D^n(G/H) = \pi(D^n(G))$ pour tout n , ce qui permet de conclure. On voit alors que de façon plus générale si $f : G \rightarrow H$ est un morphisme de groupes surjectif avec G résoluble, alors H est résoluble³⁸.

► **REMARQUE.** – On pouvait évidemment utiliser l'autre définition du cours. Si on se donne

$$G_0 = \{e\} \leq G_1 \leq \dots \leq G_n = G$$

comme dans le cours, alors les $H \cap G_i$ fonctionnent! En effet, si $G_i \triangleleft G_{i+1}$, alors $G_i \cap H \triangleleft G_{i+1} \cap H$ et si G_{i+1}/G_i est abélien, alors $G_{i+1} \cap H / G_i \cap H$ aussi. En effet, soit $g, g' \in G_{i+1} \cap H$. On sait puisque G_{i+1}/G_i est abélien qu'il existe $g_i \in G_i$ tel que $gg' = g'gg_i$. Or, ici, $gg', g'g \in G_{i+1} \cap H$ donc $g_i \in H$ et $g_i \in G_i \cap H$ si bien que dans $G_{i+1} \cap H / G_i \cap H$, on a bien $gg' = g'g$. De même, dans le cas du quotient,

$$\{e\} = G_0H/H \leq G_1H/H \leq \dots \leq G_nH/H = G/H$$

convient. En effet, on a bien $G_iH/H \triangleleft G_{i+1}H/H$ si³⁹ $G_i \triangleleft G_{i+1}$ et $(G_{i+1}H/H)/(G_iH/H) \cong G_{i+1}H/G_iH$ abélien via les théorèmes d'isomorphisme! Attention au fait que l'on ne peut pas simplifier par H (prendre par exemple $H = G$ pour s'en convaincre). En revanche, puisque H est dans le noyau de la projection canonique $G_{i+1}H \rightarrow G_{i+1}H/G_iH$, on peut supposer que deux éléments de $G_{i+1}H/G_iH$ proviennent de deux éléments de G_{i+1} . On considère donc $g, g' \in G_{i+1}$ et alors $gg' = g'gg_i$ avec $g_i \in G_i \subseteq G_iH$ de sorte que dans $G_{i+1}H/G_iH$, $gg' = g'g$.

On obtient par la même occasion des informations sur la classe de résolubilité, à savoir sur le plus petit indice n tel que $D^n(G) = \{e\}$.

38. Si $f : G_1 \rightarrow G_2$ est un morphisme de groupes, on a pour tout entier n , $f(D^n(G_1)) \subseteq D^n(G_2)$ avec égalité si f est surjectif.

39. En effet, $H \triangleleft G$ et $G_i \triangleleft G_{i+1}$. Ainsi, pour tout $x \in G_iH$ (donc $x = g_ih_1$ avec $g_i \in G_i$ et $h_1 \in H$) et $y \in G_{i+1}H$ (donc $y = g_{i+1}h_2$ avec $g_{i+1} \in G_{i+1}$ et $h_2 \in H$), on a

$$xyx^{-1} = g_{i+1}h_2g_ih_1h_2^{-1}g_i^{-1}.$$

Or, $H \triangleleft G$ donc $H \triangleleft G_i$ et $H \triangleleft G_{i+1}$ donc $h_2g_i = g_ih'_2$ pour $h'_2 \in H$ et $h'_2h_1h_2^{-1}g_i^{-1} = g_{i+1}^{-1}h$ pour $h \in H$ si bien que

$$xyx^{-1} = g_{i+1}g_i g_{i+1}^{-1}h \in G_iH \quad \text{car} \quad g_{i+1}g_i g_{i+1}^{-1} \in G_i \quad \text{car} \quad G_i \triangleleft G_{i+1}.$$

2. Soit $1 \rightarrow N \rightarrow G \rightarrow H \rightarrow 1$ une suite exacte avec H et N deux groupes résolubles et montrons que G est résoluble. On sait alors que l'application $p : G \rightarrow H$ est surjective donc comme en 1., il s'ensuit qu'il existe un entier n tel que $\{e\} = D^n(H) = p(D^n(G))$ si bien que $D^n(G) \subseteq \text{Ker}(p) = \text{Im}(i) = i(N) \cong N$ où $i : N \rightarrow G$ est injective. Ainsi, il existe un entier⁴⁰ m tel que $D^m(i(N)) = \{e\}$ et alors $D^{n+m}(G) = \{e\}$ et G est résoluble.

► **REMARQUE.** – Idem, on pouvait composer une suite de composition pour $i(N)$

$$G_0 = \{e\} \leq G_1 \leq \dots \leq G_m = i(N)$$

avec une suite de composition de $H \cong G/N$ (via les théorèmes d'isomorphisme)

$$G'_m = \{\bar{e}\} = N/N \leq G'_{m+1} = G_{m+1}/N \leq \dots \leq G'_{m+n} = G/N$$

avec G_i pour $i \in \{m+1, \dots, m+n\}$ des sous-groupes contenant N et tels que $G_i \triangleleft G_{i+1}$ et $G'_{i+1}/G'_i \cong G_{i+1}/G_i$ abéliens pour obtenir une suite de composition qui convient pour G

$$G_0 = \{e\} \leq G_1 \leq \dots \leq G_m = i(N) \leq G_{m+1} \leq \dots \leq G_{m+n} = G.$$

3. Un groupe nilpotent est résoluble mais la réciproque est fautive comme en témoigne l'exemple du groupe \mathfrak{S}_3 (on aurait aussi pu prendre \mathfrak{A}_4 ou \mathfrak{S}_4). Une preuve est donnée page 32 du polycopié de cours, on pouvait aussi utiliser le fait (pour $G = \mathfrak{S}_3$ par exemple) que $D(G) = \mathfrak{A}_3$ qui est abélien donc $D^2(G) = \{e\}$ pour obtenir la résolubilité et le fait qu'un groupe est nilpotent si, et seulement si, il existe un entier n tel que $C^n(G) = \{e\}$ où $C^0(G) = G$ et $C^{n+1}(G)$ est le groupe engendré par les commutateurs $ghg^{-1}h^{-1}$ avec $g \in G$ et $h \in C^n(G)$ (la preuve étant analogue à celle dans le cas résoluble, voir l'exercice 13). On a dans notre cas, $C^1(G) = D(G) = \mathfrak{A}_3$ et $C^2(G)$ est alors un sous-groupe non trivial de $C^1(G) = \mathfrak{A}_3$ car \mathfrak{A}_3 n'est pas central dans G si bien que nécessairement $C^2(G) = \mathfrak{A}_3$ et par récurrence immédiate, $C^n(G) = \mathfrak{A}_3 \neq \{e\}$. On pouvait aussi utiliser que les seuls sous-groupes distingués de \mathfrak{S}_3 sont $\{Id\}$, \mathfrak{A}_3 et \mathfrak{S}_3 et donc cela ne peut donner lieu qu'aux suites de compositions de groupes normaux $\{Id\} \triangleleft \mathfrak{S}_3$ mais \mathfrak{S}_3 est non abélien ou $\{Id\} \triangleleft \mathfrak{A}_3 \triangleleft \mathfrak{S}_3$ où on a bien $\mathfrak{S}_3/\mathfrak{A}_3$ abélien mais \mathfrak{A}_3 non inclus dans $Z(\mathfrak{S}_3) = \{Id\}$.
4. On peut utiliser le fait qu'on sait qu'un tel groupe est non simple (par exemple en reprenant la preuve de la non simplicité de G d'ordre pq qui établit que si $p < q$, alors G possède un seul q -Sylow qui est donc distingué). Il existe donc $H \triangleleft G$. On peut supposer sans perte de généralité que H est de cardinal p donc abélien et ainsi G/H est de cardinal q donc abélien et la suite $\{e\} \subseteq H \subseteq G$ montre que G est résoluble.
Reste à traiter le cas de $p = q$ mais on sait qu'un groupe d'ordre p^2 est abélien (voir le cours) donc résoluble. De manière générale, on sait qu'un p -groupe est nilpotent et donc résoluble⁴¹.
5. On a le résultat d'après ce qui précède si $p = q = r$. Si deux des nombres premiers sont égaux, on est ramené à la question suivante, on supposera donc que $p < q < r$. On a alors que $n_r \in \{1, pq\}$ et $n_q \in \{1, r, pr\}$. Supposons que $n_r, n_q \neq 1$. Alors G admet exactement $pq(r-1)$ éléments d'ordre r et au moins $r(q-1)$ éléments d'ordre q . cela fournit que

$$\#G \geq pq(r-1) + r(q-1).$$

Mais on remarque que

$$pq(r-1) + r(q-1) = pqr + rq - pq - r = \#G + (r-p)(q-1) - p > \#G$$

car $r-p > 1$ et $q-1 \geq p$. Ainsi $n_r = 1$ ou $n_q = 1$ et G admet un sous-groupe distingué d'ordre premier, donc abélien tel que le quotient soit un groupe de cardinal le produit de deux nombres premiers, donc résoluble. Ainsi, G est résoluble. En effet, si un groupe $H \triangleleft G$ est résoluble et que G/H aussi, alors G est résoluble par 2.

6. Supposons que $q < p$. On a alors que le nombre n_p de p -Sylow vaut 1 et donc on obtient un unique p -Sylow H d'ordre p^2 donc abélien donc résoluble tel que G/H soit d'ordre q donc cyclique donc résoluble et par 2., G est résoluble.
Si maintenant $p < q$. On a alors que $n_q \in \{1, p^2\}$ et $n_p \in \{1, q\}$. Si $n_p \neq 1$ et $n_q \neq 1$, alors on a au moins

$$1 + p^2(q-1) + p^2 - 1 + 1 = \#G + 1$$

40. Un groupe isomorphe à un groupe résoluble étant bien évidemment lui-même résoluble (car ils ont le même groupe dérivé ou en prenant l'image d'une suite de composition par un isomorphisme)!

41. En effet, on procède par récurrence sur n . Un groupe d'ordre p est bien nilpotent et supposons alors que $\#G = p^{n+1}$. On sait que $\{e\} \neq Z(G) \triangleleft G$ et donc on peut appliquer l'hypothèse de récurrence au p -groupe $Z(G)$ (si $Z(G) \neq G$ mais si tel est le cas, G est abélien et G est trivialement nilpotent). Il existe ainsi $\{e\} = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n = Z(G)$ avec $G_i \triangleleft Z(G)$ et donc comme ils sont centraux $G_i \triangleleft G$ et G_i/G_{i-1} inclus dans le centre de $Z(G)/G_{i-1}$ lui-même inclus dans le centre de G/G_{i-1} . On écrit alors par hypothèse de récurrence appliquée au p -groupe $G/Z(G)$, on obtient

$$G'_n = Z(G)/Z(G) \subseteq G'_{n+1} = G_{n+1}/Z(G) \subseteq \dots \subseteq G'_{n+m} = G/Z(G)$$

avec $G'_i \triangleleft G/Z(G)$ donc $G_i \triangleleft G$ et $G'_{i+1}/G'_i \cong G_{i+1}/G_i \leq Z(G/G_i) \cong Z(G'/G'_i)$. On a alors que

$$\{e\} = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n = Z(G) \subseteq G_{n+1} \subseteq \dots \subseteq G_{n+m} = G$$

montre que G est nilpotent.

éléments dans G (l'identité, puis $q - 1$ éléments d'ordre q dans les p^2 q -Sylow et enfin $p^2 - 1$ éléments d'ordre divisant p dans un des p -Sylow plus un autre tel élément au moins dans un second p -Sylow). On a donc une contradiction et donc soit $n_p = 1$ soit $n_q = 1$ et on obtient que le q -Sylow ou le p -Sylow est distingué et on conclut comme dans le premier cas!

► **COMPLÉMENTS.** – On peut montrer de même qu'un groupe d'ordre $p^\alpha q$ avec $p > q$ (car $n_p = 1$ et un p -groupe est résoluble et le quotient abélien aussi), d'ordre $p^\alpha q^\beta$ avec $p^\alpha < q + 1$ (car $n_q = 1$ et des p -groupes sont résolubles).

On peut alors déduire de tout cela que tout groupe d'ordre < 60 est résoluble. Pour l'ordre 60, on sait que \mathfrak{A}_5 est simple non abélien et par conséquent non résoluble.

Je rappelle qu'un groupe simple est résoluble si, et seulement si, il est commutatif (car $D(G) \triangleleft G$ et $D(G) \neq \{e\}$ donc $D(G) = G$) et cela a alors lieu si, et seulement si, c'est un groupe d'ordre premier. Pour la culture, je mentionne le théorème de Feit-Thompson (qui est très profond et difficile mais qui a joué un rôle majeur dans la classification des groupes finis simples) conjecturé par Burnside en 1911 démontré en 1963 et qui stipule que tout groupe d'ordre impair est résoluble. Il s'agissait d'une des pistes pour classer à isomorphisme près les groupes finis. On utilise les sous-groupes distingués non triviaux pour réaliser G comme extension de deux sous-groupes de cardinal strictement inférieurs. Ce procédé donne finalement lieu à des groupes simples que l'on sait aujourd'hui classer (un tel groupe est soit alterné, soit cyclique, soit de type Lie soit un des 26 groupes simples sporadiques). Le problème est alors que l'on ne sait pas classer les extensions de groupes! On a enfin le résultat suivant (sorte de réciproque partielle du théorème de Lagrange), à savoir le théorème de Hall : G est résoluble si, et seulement si, pour tout $d \mid n = \#G$ tel que $\text{pgcd}(d, \frac{n}{d}) = 1$, G possède un sous-groupe d'ordre d . Noter que si d est une puissance d'un nombre premier, l'hypothèse de résolubilité est inutile car le résultat découle des théorèmes de Sylow. En général, elle est nécessaire! On pourra en effet remarquer que \mathfrak{A}_5 ne contient pas de sous-groupes d'ordre 15 ou 20. On dispose par ailleurs d'une réciproque de ce résultat : un groupe G possédant au moins un sous-groupe d'ordre d pour chaque d diviseur de n tel que $\text{pgcd}(d, \frac{n}{d}) = 1$, alors G est résoluble. Cela implique immédiatement le théorème de Burnside!

On a également que le produit direct de deux groupes résolubles l'est puisque $D(G_1 \times G_2) \cong D(G_1) \times D(G_2)$.

Pour finir, établissons l'équivalence pour un groupe G fini⁴³ on a l'équivalence entre G résoluble et l'existence d'une suite de composition

$$\{e\} = G_0 \leq G_1 \leq \dots \leq G_n = G$$

avec $G_{i+1} \triangleleft G_i$ et G_{i+1}/G_i cyclique d'ordre premier. Il est en particulier clair que cette dernière propriété (puisque cyclique implique abélien) implique toujours résoluble. Établissons alors la réciproque dans le cas G fini. Commençons par montrer par récurrence sur le cardinal, que si H est un groupe abélien fini, alors une telle suite de compositions aux quotients cycliques d'ordre premier existe. Si H est simple, comme H est supposé abélien, il est cyclique d'ordre premier et alors $\{e\} \leq H$ convient! Sinon, on peut trouver un sous-groupe strict $N \triangleleft H$ d'ordre maximal. On considère alors la projection canonique $\pi : H \rightarrow H/N$. On en déduit que H/N est simple car sinon, il contiendrait un sous-groupe normal $K \triangleleft H/N$ et $\pi^{-1}(K)$ serait un sous-groupe distingué de H contenant N distinct de N et donc égal à H (car π est surjective). Ainsi, on aurait $K = H/N$, ce qui a été exclu. Par ailleurs, comme il s'agit d'un quotient d'un groupe abélien, H/N est abélien et comme on a vu qu'il est simple, il est cyclique d'ordre premier. On peut donc commencer notre suite de composition par $H_n = H \geq H_{n-1} = N$ où $\#N < \#H$. L'hypothèse de récurrence appliquée à N fournit $H_0 = \{e\} \leq H_1 \leq \dots \leq H_{n-1} = N$ à quotients cycliques d'ordre premiers. La suite $H_0 = \{e\} \leq H_1 \leq \dots \leq H_{n-1} = N \leq H_n = H$ convient alors. Pour conclure, si G est résoluble, on dispose d'une suite $\{e\} = G_0 \leq G_1 \leq \dots \leq G_n = G$ avec $G_{i+1} \triangleleft G_i$ et G_{i+1}/G_i abéliens. Pour tout $i \in \{0, \dots, n-1\}$, on peut donc trouver une suite de composition

$$G'_0 = \{\bar{e}\} \triangleleft G'_1 = G_{i,1}/G_i \triangleleft G'_2 = G_{i,2}/G_i \triangleleft \dots \triangleleft G'_{r_i} = G_{i+1}/G_i$$

avec les $G'_{i,j}$ pour $j \in \{1, \dots, r_i\}$ des sous-groupes contenant G_i vérifiant $G_{i,j} \triangleleft G_{i,j+1}$ et tels que G'_{i+1}/G'_i cyclique d'ordre premier. Par ailleurs, par les théorèmes d'isomorphisme, il vient que

$$G'_{j+1}/G'_j = (G_{i+1,j}/G_i)/(G_{i,j}/G_i) \cong G_{i+1,j}/G_{i,j} \quad \text{qui est donc cyclique d'ordre premier.}$$

Ainsi, la suite de composition convient (autrement dit est à quotients cycliques d'ordre premier)

$$\{e\} = G_0 \leq G_{0,1} \triangleleft \dots \triangleleft G_{0,r_0} = G_1 \triangleleft G_{1,1} \triangleleft \dots \triangleleft G_{1,r_1} = G_2 \triangleleft \dots \triangleleft G_n = G.$$

Noter qu'on ne peut pas imposer le fait que les G_i soient distingués dans G mais seulement dans G_{i+1} . Si on rajoute cette condition, on parle de groupe *hyper-résoluble* qui est une notion strictement plus forte. par exemple, en utilisant le fait que les seuls sous-groupes distingués de \mathfrak{S}_4 sont $\{\text{Id}\}$, V_4 (engendré par les doubles transpositions), \mathfrak{A}_4 et \mathfrak{S}_4 , une telle suite à quotients cycliques d'ordre premier est impossible avec la condition que les $G_i \triangleleft \mathfrak{S}_4$ tandis que la suite $\{e\} \leq \langle (12) \rangle \leq V_4 \leq \mathfrak{A}_4 \leq \mathfrak{S}_4$ est en revanche bien à quotients abéliens mais $\langle (12) \rangle \not\triangleleft \mathfrak{S}_4$.

EXERCICE 10 — GROUPES NILPOTENTS.

On dit qu'un sous-groupe H de G est maximal si $H \neq G$ et qu'aucun sous-groupe propre de G n'est compris strictement entre H et G .

1. Soient G un groupe fini, $N \triangleleft G$, $H \leq G$ et $\pi : G \rightarrow G/N$ la surjection canonique. Montrer que $\pi(H) \leq Z(G/N)$ si, et seulement si, $[H, G] \leq N$ où, pour $H_1, H_2 \leq G$, on note $[H_1, H_2]$ le sous-groupe de G engendré par les commutateurs de la forme $h_1 h_2 h_1^{-1} h_2^{-1}$ avec $h_1 \in H_1$ et $h_2 \in H_2$.

42. En réalité, on dispose du théorème de Burnside qui fournit que tout groupe d'ordre $p^n q^m$ est résoluble dont une démonstration passe par la théorie des représentations.

43. Noter que cette hypothèse n'est essentielle ici.

2. On définit la suite centrale descendante associée à G par $C^1(G) = [G, G]$ et $C^{n+1}(G) = [G, C^n(G)]$ pour $n \in \mathbb{N}^*$. En déduire que G est nilpotent si, et seulement si, il existe $n_0 \in \mathbb{N}^*$ tel que $C^{n_0}(G) = \{e\}$. Établir que le groupe G est alors nilpotent si, et seulement si, il existe $n_0 \in \mathbb{N}^*$ tel que $C^{n_0}(G) = \{e\}$.
3. Montrer qu'un groupe nilpotent est résoluble. Que dire de la réciproque?
4. Montrer que le centre d'un groupe nilpotent est non trivial.
5. Montrer que si G est nilpotent et que H est un sous-groupe de G , alors H est nilpotent.
6. Montrer que si $H \triangleleft G$ et que G est nilpotent, alors G/H est nilpotent.
7. On suppose H et G/H nilpotents. Le groupe G est-il nilpotent?
8. Soient p, q, r trois nombres premiers. Montrer que tout groupe d'ordre pqr est résoluble. Un tel groupe est-il nilpotent?
9. On suppose G fini. Montrer que G est nilpotent si, et seulement si, tout sous-groupe maximal de G est distingué et si, et seulement si, G est produit direct de ses p -Sylow pour tout nombre premier p divisant $\#G$.

SOLUTION.

On commence par donner un critère dans le cas des groupes nilpotents correspondant à celui du $D^n(G) = \{e\}$ pour les groupes résolubles. Soient G un groupe fini, $N \triangleleft G$, $H \leq G$ et $\pi : G \rightarrow G/N$ la surjection canonique. On a alors que $\pi(H) \leq Z(G/N)$ si, et seulement si, $[H, G] \leq N$ où, pour $H_1, H_2 \leq G$, on note $[H_1, H_2]$ le sous-groupe de G engendré par les commutateurs de la forme $h_1 h_2 h_1^{-1} h_2^{-1}$ avec $h_1 \in H_1$ et $h_2 \in H_2$. En effet, la condition que $\pi(H) \leq Z(G/N)$ équivaut à $[\pi(H), G/N] = \{\bar{e}\}$. On a clairement que $[\pi(H), G/N] = [\pi(H), \pi(G)] = \pi([H, G])$ par surjectivité du morphisme de groupes π . Ainsi, on a immédiatement que $[\pi(H), G/N] = \{\bar{e}\}$ si, et seulement si, $[H, G] \leq N$.

On définit alors la suite centrale descendante associée à G par $C^1(G) = [G, G]$ et $C^{n+1}(G) = [G, C^n(G)]$ pour $n \in \mathbb{N}^*$. En déduire que G est nilpotent si, et seulement si, il existe $n_0 \in \mathbb{N}^*$ tel que $C^{n_0}(G) = \{e\}$. Le groupe G est alors nilpotent si, et seulement si, il existe $n_0 \in \mathbb{N}^*$ tel que $C^{n_0}(G) = \{e\}$. Si G est nilpotent, il existe une suite de groupes

$$\{e\} = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n = G$$

avec pour tout $i \in \{1, \dots, n\}$, $G_i \triangleleft G$ et pour tout $i \in \{1, \dots, n-1\}$, $G_{i+1}/G_i = \pi(G_{i+1}) \leq Z(G/G_i)$ avec $\pi : G \rightarrow G/G_i$ la surjection canonique, soit $[G, G_{i+1}] \leq G_i$ d'après ce qui précède. On a donc $C^1(G) \leq G_{n-1}$ puis $C^2(G) = [G, C^1(G)] \leq [G, G_{n-1}] \leq G_{n-2}$ et de proche en proche $C^n(G) \leq G_0 = \{e\}$ ce qui permet de conclure. Réciproquement, supposons que $C^n(G) = \{e\}$, on pose alors $G_n = G$, $G_{n-1} = C^1(G), \dots, G_0 = C^n(G)$ et on a alors

$$\{e\} = G_0 \subseteq G_1 \subseteq \dots \subseteq G_{n-1} = G$$

avec $G_i \triangleleft G$ car les $C^i(G)$ sont des sous-groupes caractéristiques de G et $[G, G_{i+1}] = G_i$ par définition, ce qui permet bien de montrer que G est nilpotent.

1. C'est du cours et évident à partir des définitions ou des caractérisations en termes de D^n et C^n . La réciproque est fautive comme on l'a vu dans l'exercice sur les groupes résolubles question 3.
2. Soit G un groupe nilpotent. Il existe $n \geq 0$ maximal tel que $C^n(G) \neq \{e\}$. On a alors $C^{n+1}(G) = \{e\}$ soit $[G, C^n(G)] = \{e\}$. Cela signifie que le sous-groupe non trivial $C^n(G)$ est contenu dans $Z(G)$ qui est donc non trivial. On pouvait aussi considérer le premier terme distinct de G_0 de la suite de composition $G_0 = \{e\} \triangleleft G_1$ qui vérifie ainsi $G_1 \cong G_1/G_0 \leq Z(G/G_0) \cong Z(G)$. Plus généralement, si $N \neq \{e\} \triangleleft G$, alors $N \cap Z(G) \neq \{e\}$ (si l'on ne suppose plus N normal, le résultat tombe en défaut comme on le voit avec D_4 et N d'ordre 2 dans D_4 non contenu dans le sous-groupe cyclique d'ordre 4). En posant dans notre cas $N_i = N \cap C^i(G)$, on a une suite d'extensions

$$N = N_0 \supseteq N_1 \supseteq \dots \supseteq N_n = \{e\}$$

où on vérifie que $[G, N_i] \subseteq N_{i+1}$. Choisissons alors l'entier k maximal tel que $N_k \neq \{e\}$. On a $N_k \leq N$ et $[G, N_k] \subseteq N_{k+1} = \{e\}$ donc $N_k \leq Z(G)$. Il faut penser aux groupes nilpotents comme des sortes de généralisation des p -groupes (dont vous avez vu dans le cours qu'ils sont nilpotents et dont on a vu que le centre est aussi non trivial!).

3. Une récurrence simple assure que pour tout $n \geq 0$, $C^n(H) \subseteq C^n(G)$, ce qui entraîne immédiatement le résultat. On a également que l'image d'un groupe nilpotent par un morphisme de groupes (car $f(C^n(G)) \subseteq C^n(f(G))$ avec égalité si le morphisme est surjectif) est nilpotent en raisonnant comme dans le cas résoluble.
4. On raisonne comme dans le cas résoluble en établissant que $\pi(C^n(G)) = C^n(G/H)$.
5. C'est faux comme on peut le voir avec $G = \mathfrak{S}_3$, $H = \mathfrak{A}_3$ et $G/H = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$. On a alors H et G/H abéliens donc nilpotents mais G non nilpotent. Ce qui fait que la preuve dans le cas résoluble ne fonctionne pas ici est que la propriété de la définition des groupes résolubles est relative dans le sens où elle ne dépend que de la relation de G_i à G_{i+1} tandis qu'ici, dans le cas nilpotent, elle dépend de la relation de G_i à G_{i+1} mais aussi à G ! En particulier, on a en général $C^n(C^m(G)) \neq C^{n+m}(G)$ et $C^n(C^m(G))$ est plus petit que $C^{n+m}(G)$. En effet, par exemple $C^1(C^n(G)) = [C^n(G), C^n(G)]$ tandis que $C^{n+1}(G) = [G, C^n(G)]$. On a en revanche le résultat plus faible suivant : si $H \leq G$ est un sous-groupe central (donc en particulier nilpotent), alors G/H nilpotent implique G nilpotent. En effet, on a l'existence d'un n tel que $C^n(G/H) = \{e\}$ donc $\pi(C^n(G)) = \{e\}$ soit $C^n(G) \leq H$ et donc $C^n(G)$ est central et $C^{n+1}(G) = \{e\}$. C'est ce qu'on utilise pour faire marcher la récurrence pour montrer qu'un p -groupe est nilpotent!

6. On a déjà traité la résolubilité. On sait que tout p -groupe est nilpotent donc si $p = q = r$, on obtient donc un groupe nilpotent. Si maintenant (sans perte de généralité), $p = q \neq r$, un tel groupe n'est pas nécessairement nilpotent comme en témoigne l'exemple de $\mathfrak{S}_3 \times \mathbf{Z}/2\mathbf{Z}$ (qui s'il était nilpotent entraînerait que \mathfrak{S}_3 est nilpotent). Supposons pour finir que $p < q < r$. Un tel groupe n'est pas non plus nécessairement nilpotent comme en témoigne l'exemple de $\mathfrak{S}_3 \times \mathbf{Z}/5\mathbf{Z}$ (qui s'il était nilpotent entraînerait que \mathfrak{S}_3 est nilpotent comme quotient par le sous-groupe distingué $\mathbf{Z}/5\mathbf{Z}$).
7. Supposons dans un premier temps que G est produit direct de ses p -Sylow. On a alors que chacun des p -Sylow est nilpotent en tant que p -groupe et on peut vérifier qu'un produit direct de groupes nilpotents est nilpotent (tout se passe composante par composante et $C^n(G_1 \times G_2) \cong C^n(G_1) \times C^n(G_2)$), ainsi G est nilpotent.

Réciproquement, supposons que G est nilpotent. Soit $M \leq G$ un sous-groupe maximal (qui existe car on a un nombre fini de sous-groupes stricts de G). Puisqu'il existe un n_0 tel que $C^{n_0}(G) = \{e\}$, il existe un entier minimal n tel que $C^n(G) \leq M$ et par minimalité de n , il existe $g \in C^{n-1}(G) \setminus M$. Alors, on a $[g, M] \subseteq [C^{n-1}(G), G] = C^n(G) \subseteq M$ ce qui assure que $gMg^{-1} \subseteq M$ et ⁴⁴ $g \in N_G(M) \setminus M$ (en tenant le même raisonnement avec g^{-1}). Par conséquent, $N_G(M)$ est un sous-groupe de G contenant M , distinct de M donc égal à G par maximalité. On a donc $N_G(M) = G$ et M est distingué dans G . On a donc que tout sous-groupe maximal est distingué. Soit S un p -Sylow de G . Supposons que $N_G(S) \neq G$. Alors $N_G(S)$ est contenu dans un sous-groupe maximal M de G . Par hypothèse, M est distingué dans G donc pour tout $g \in G$, $gSg^{-1} \subseteq gMg^{-1} = M$ donc S et gSg^{-1} sont deux p -Sylow de M , donc conjugués dans M . Il existe ainsi $m \in M$ tel que $gSg^{-1} = mSm^{-1}$ donc $m^{-1}g \in N_G(S) \subseteq M$ donc $g \in M$ ce qui implique que $M = G$, ce qui est absurde par définition d'un sous-groupe maximal. Ainsi $N_G(S) = G$ et S est distingué et l'unique p -Sylow de G .

Considérons alors l'application $\varphi : \prod_{p \mid \#G} S_p \rightarrow G$ défini par le produit dans G et où S_p désigne l'unique p -Sylow. Comme les p -Sylow ont des cardinaux premiers entre eux, on voit que les éléments d'un sous-groupe de Sylow commutent avec ceux d'un autre. En effet, soit $x \in S_p$ et $y \in S_q$ distincts de e , alors $xyx^{-1}y^{-1} \in S_q$ (car $xyx^{-1} \in S_q \triangleleft G$) et de même $xyx^{-1}y^{-1} \in S_p$ (car $yx^{-1}y^{-1} \in S_p \triangleleft G$) et ainsi, $xyx^{-1}y^{-1} \in S_p \cap S_q = \{e\}$ et $xy = yx$. Cela entraîne qu'on a un morphisme de groupes et ce dernier est clairement injectif (car par commutativité et le fait que les ordres soient premiers entre eux, l'ordre d'un élément $s_1 \cdots s_r$ est le ppcm des ordres des s_i donc un élément du noyau est nécessairement trivial ⁴⁵). On en déduit le résultat par cardinalité.

On termine par lister une propriété supplémentaire des groupes nilpotents : un groupe G est nilpotent si, et seulement si, $G/Z(G)$ est nilpotent (en effet le sens direct découle de l'exercice et dans le sens indirect si $\pi : G \rightarrow G/Z(G)$ et si $C^m(G/Z(G)) = \{e\}$ et $C^{n-1}(G/Z(G)) \neq \{e\}$, alors $C^n(G) \subseteq Z(G)$ et $C^{n-1}(G) \not\subseteq Z(G)$ donc $[G, C^n(G)] = \{e\}$).

Exercices complémentaires semaine 2

EXERCICE 11. Soient p un nombre premier et G un p -groupe fini. Soit $(A, +)$ un groupe abélien avec $A \neq \{0\}$. On suppose donnée une action de G sur A par automorphismes, c'est-à-dire que pour tout $g \in G$, la bijection $x \mapsto g \cdot x$ de A dans A est un automorphisme du groupe abélien A . On suppose de plus que A est de torsion p -primaire, i.e. pour tout $x \in A$, il existe $m \in \mathbf{N}$ tel que $p^m x = 0$.

- Montrer que si A est fini, son cardinal est une puissance de p .
Indication : On pourra utiliser la classification des groupes abéliens finis, ou encore le théorème de Sylow.
- On suppose que A est fini. Montrer qu'il existe $x \neq 0$ dans A tel que pour tout $g \in G$, on ait $g \cdot x = x$.
- On ne suppose plus A fini et soit $a \neq 0$ dans A . Montrer que le sous-groupe B de A engendré par $\{g \cdot a, g \in G\}$ est fini.
- En déduire que le résultat de 2. vaut encore sans l'hypothèse A fini.

SOLUTION.

- L'hypothèse est que tout élément est d'ordre une puissance de p . Le théorème de structure des groupes abéliens finis garantit que

$$G \cong \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z}$$

avec $d_1 \mid \cdots \mid d_r$. Si maintenant un des d_i possède un autre facteur premier que p , disons q , alors on sait que G va contenir un élément d'ordre q ce qui est absurde. D'où, tous les d_i sont des puissances de p et G est un p -groupe.

On peut aussi raisonner par l'absurde. Supposons qu'il existe un nombre premier $q \neq p$ divisant le cardinal de A . On sait alors qu'il existe q -Sylow S de A . On considère alors un élément $x \in S$ distinct de l'élément neutre. Puisque $x \in S$ et que S est un q -groupe, l'ordre de x est une puissance de q . Mais, l'hypothèse qu'il existe un entier m tel que $p^m x = 0$ (puisque $x \in A$) implique que l'ordre de x est une puissance de p , ce qui est absurde! On en déduit bien que A est un p -groupe.

⁴⁴. On rappelle que le normalisateur d'un sous-groupe M de G est le plus grand sous-groupe de G dans lequel M est distingué, à savoir $N_G(M) = \{g \in G : gMg^{-1} = M\}$. Il s'agit du stabilisateur de M pour l'action de G sur l'ensemble de ses sous-groupes par conjugaison.

⁴⁵. On peut aussi montrer que le cardinal de

$$\prod_{\substack{p \mid \#G \\ p \neq p_1}} S_p \text{ est donné par } \prod_{\substack{p \mid \#G \\ p \neq p_1}} \#S_p$$

est en particulier premier à p_1 . Un élément du noyau vérifie donc $s_1^{-1} = s_2 \cdots s_r \in S_{p_1} \cap \prod_{\substack{p \mid \#G \\ p \neq p_1}} S_p = \{e\}$ par cardinalité. On conclut de proche en proche.

2. Noter que puisque l'action est par automorphismes, $\text{Fix}(g)$ est alors un sous-groupe de A pour tout $g \in G$ et on cherche un élément de $\bigcap_{g \in G} \text{Fix}(g)$. L'équation aux classes fournit

$$\#A = \#A^G + \sum_{\omega \in \Omega'} \frac{\#G}{\#\text{Stab}_G(\omega)} \quad \text{avec} \quad A^G = \{x \in A : \forall g \in G, g \cdot x = x\} = \bigcap_{g \in G} \text{Fix}(g) = \text{réunion des orbites de cardinal 1}$$

et puisque $\frac{\#G}{\#\text{Stab}_G(\omega)}$ est une puissance de p car pour $\omega \in \Omega'$ (qui correspond aux orbites de cardinal > 1), la stabilisateur est un sous-groupe strict et G est un p -groupe. Par ailleurs, $p \mid \#A$ si bien que $p \mid \#A^G$. Mais $\#A^G \neq 0$ car $0 \in A^G$ (car on agit par automorphisme) et par conséquent $\#A^G \geq p$ et on a le résultat.

3. On peut utiliser le théorème de structure des groupes abéliens de type fini couplé au fait que tout élément de A est de torsion. On peut aussi utiliser que par définition et puisqu'on travaille dans un cadre commutatif

$$B = \left\{ \sum_{g \in G} n_g(g \cdot a) : \forall g \in G, n_g \in \mathbf{Z} \right\}.$$

Mais puisque chacun des $g \cdot a$ est d'ordre fini, il suffit de se restreindre à un nombre fini de n_g .

4. On applique simplement le résultat de 2. à B (sur lequel l'action de G se restreint⁴⁶) et il existe $x \neq 0$ dans $B \subseteq A$ tel que pour tout $g \in G, g \cdot x = x$.

EXERCICE 12 — GROUPE DES AUTOMORPHISMES.

- Soient p un nombre premier et $n \in \mathbf{N}$. Établir que $\text{Aut}((\mathbf{Z}/p\mathbf{Z})^n)$ est isomorphe à $\text{GL}_n(\mathbf{Z}/p\mathbf{Z})$. Pour quelles valeurs de n ce groupe est-il commutatif?
- On suppose que $n \geq 2$. Montrer que $(\mathbf{Z}/p\mathbf{Z})^n$ contient un sous-groupe distingué mais non caractéristique.
- On considère dans cette question le cas $p = n = 2$. Montrer que $\text{Aut}((\mathbf{Z}/2\mathbf{Z})^2)$ est isomorphe à \mathfrak{S}_3 .

SOLUTION.

- Voir le corrigé du partiel de l'an dernier, [ici](#), exercice 2.
- Voir le corrigé du partiel de l'an dernier, [ici](#), exercice 2.
- On sait que le cardinal de $\text{GL}_n(\mathbf{Z}/p\mathbf{Z})$ est⁴⁷ 6 et est non abélien. On sait alors qu'un tel groupe est isomorphe à \mathfrak{S}_3 . On renvoie eu premier DM pour une autre approche!

⁴⁶. En effet, B a été choisi de sorte à être de type fini et stable sous l'action de G . C'est une méthode usuelle pour passer de l'hypothèse fini à infini et il s'agit en fait du plus petit sous-groupe stable sous l'action de G et contenant a . Pour voir que B est stable sous l'action de g , on écrit un élément quelconque b de B sous la forme

$$b = \sum_{g \in G} n_g(g \cdot a) \quad n_g \in \mathbf{Z}$$

de sorte que pour tout $g' \in G$,

$$g' \cdot b = \sum_{g \in G} n_g g' \cdot (g \cdot a).$$

On a ici utilisé le fait que l'action est lieu par automorphisme (ce qui signifie que \cdot est \mathbf{Z} -linéaire dans le cas commutatif) et que la somme est finie car G est fini. On utilise ici que le côté morphisme uniquement (mais le côté automorphisme vient du fait que le morphisme sous-jacent $A \rightarrow A$ issu de l'action est une bijection). On a alors

$$g' \cdot b = \sum_{g \in G} n_g ((g'g) \cdot a) \quad \text{soit} \quad g' \cdot b = \sum_{g'' \in G} n_{g'^{-1}g''} (g'' \cdot a) \in B$$

en effectuant le changement de variable bijectif $G \rightarrow G$ donné par $g'' = g'g$.

⁴⁷. Car une telle matrice est donnée par le choix d'une première colonne non nulle (ce qui laisse $4 - 1 = 3$ choix) et d'une seconde colonne non colinéaire à la première (ce qui laisse $4 - 2 = 2$ choix).