Petits groupes simples finis

Daniel PERRIN

Ce texte reprend le thème d'un TER (Travail d'Étude et de Recherche de maîtrise) plusieurs fois posé à Orsay. Je me suis notamment appuyé sur l'excellente rédaction de Christophe Bertauld[1] *que je remercie ici.*

On renvoie à [DP] pour le b.a. ba de théorie des groupes utilisé ici.

1 Introduction

1.1 Le problème

La question peut-être la plus naturelle sur les groupes finis de cardinal donné n est de les déterminer tous à isomorphisme près. Posée ainsi, la question est totalement inabordable, sauf si n est très simple du point de vue arithmétique, par exemple un nombre premier[2] p, ou un nombre qui n'a que très peu de facteurs premiers, par exemple pq ou p^2, voir [DP]. À l'opposé, la classification des p-groupes (c'est-à-dire les groupes d'ordre une puissance de p) est très compliquée[3], dès que l'exposant est ≥ 4.

Malgré cela, cette question naïve est une bonne façon d'explorer le sujet (et d'apprendre les rudiments de la théorie) et on peut se donner l'objectif de déterminer tous les groupes finis de cardinal $\leq K$ avec un K raisonnable (par exemple avec $K = 60$, voire 100, en évitant soigneusement $n = 32, 64, 96$ et quelques autres).

Un procédé standard et systématique pour faire ce travail est ce qu'on appelle le **dévissage**. L'idée est de procéder de proche en proche, en commençant par les groupes d'ordres $1, 2, 3, 4, \ldots$ et en ramenant l'étude des groupes d'ordre n à celle de groupes d'ordres $< n$, supposés connus. Pour cela, si G est un groupe d'ordre n, on cherche un sous-groupe N de G, non trivial (donc de cardinal strictement compris entre 1 et n) et on regarde le quotient G/N ... Ah, on rencontre ici la première difficulté de la théorie. Si l'on travaille avec des groupes non abéliens, on sait que le quotient G/N,

1. Merci aussi à Rémy Allix, Fabienne Argoud, Raphaël Fino et Cécile Julaud.
2. Dans ce qui suit, les lettres p et q désigneront toujours des nombres premiers.
3. Il y a déjà 14 groupes d'ordre 16 à isomorphisme près.

vu comme ensemble de classes, n'est un groupe que si N est un sous-groupe distingué de G.

Qu'à cela ne tienne, on cherche donc un sous-groupe distingué non trivial N de G, qui est un groupe connu puisque de cardinal $< n$, on considère le quotient G/N, connu lui aussi pour la même raison, et il ne reste plus qu'à reconstituer G à partir de N et $H = G/N$. Ce beau programme se heurte à deux écueils :

1) D'abord, reconstituer, c'est facile à dire, mais en général difficile à faire. C'est ce qu'on appelle le calcul des extensions de N par H. Pour des petites valeurs de n on aura souvent affaire à des extensions scindées (produits directs ou semi-directs), que l'on peut calculer explicitement, voir [DP], mais ensuite les choses se compliquent.

2) Avant cela, il y a une autre difficulté, incontournable : et s'il n'existe pas de sous-groupe distingué N non trivial dans G ? C'est malheureusement possible, un groupe qui n'a pas de sous-groupe distingué non trivial est appelé un groupe [4] **simple** et il est évidemment impossible à dévisser.

Les groupes simples apparaissent ainsi comme les briques élémentaires de la théorie, qu'il faut absolument connaître pour espérer comprendre les autres. Leur investigation est une partie importante de la théorie des groupes finis, qui a été abordée depuis longtemps, le premier point étant de donner des exemples de tels groupes.

Les plus évidents sont les groupes abéliens $\mathbf{Z}/p\mathbf{Z}$ avec p premier, évidemment simples, puisqu'ils n'ont aucun sous-groupe non banal. Moins évidents, mais connus depuis Galois [5], les groupes alternés $\mathfrak{A}_n$ avec $n \geq 5$ sont simples eux aussi. Sont apparus ensuite les groupes linéaires ou orthogonaux sur les corps finis et un certain nombre de variantes de ces groupes qui constituent des séries infinies. Enfin, ne rentrant dans aucune des cases précédentes, 26 groupes dits sporadiques (groupes de Mathieu, de Conway, monstre de Fischer-Griess, etc). Il ne restait plus *(sic)* qu'à montrer qu'on avait ainsi une liste complète. C'est ce qui a été fait dans les années 1980 avec une preuve dont on dit qu'elle avoisine les 10000 pages.

Comme cette preuve ne tiendrait pas dans cette marge, nous nous limiterons ici à un objectif plus raisonnable. Précisément, nous allons déterminer tous les groupes simples de cardinal ≤ 168 et montrer qu'hormis les groupes triviaux $\mathbf{Z}/p\mathbf{Z}$, il n'y en a que deux : le groupe alterné $\mathfrak{A}_5$ d'ordre 60 et le groupe simple d'ordre 168, isomorphe au choix à $PSL(2, \mathbf{F}_7)$ ou $PSL(3, \mathbf{F}_2)$.

4. Pour éviter des canulars, le groupe réduit à l'unité n'est pas considéré comme un groupe simple (de même que 1 n'est pas un nombre premier).

5. C'est la simplicité des groupes alternés qui empêche l'équation générale de degré ≥ 5 d'être résoluble par radicaux.

Nous décrirons ensuite ces groupes de manière plus géométrique.

1.2 Rappels et notations

Pour tous ces rappels, on renvoie le lecteur à [DP].

Le résultat le plus important quand on aborde les groupes finis est sans conteste le théorème de Lagrange : si N est un sous-groupe de G, le cardinal de N divise le cardinal de G. De nombreux théorèmes peuvent être vus comme des réciproques partielles de ce résultat. Ainsi, on a les résultats suivants :

1.1 Proposition. *1) Un groupe cyclique d'ordre n admet exactement un sous-groupe (cyclique lui aussi) de cardinal d pour tout d diviseur de n.*

2) Dans un groupe abélien de cardinal n il y a des sous-groupes (distingués) de cardinal d pour tout d diviseur de n.

Les théorèmes de Sylow, eux aussi, sont des réciproques partielles de Lagrange. Avant d'évoquer ces résultats, rappelons qu'un p-groupe (p premier, toujours) est un groupe dont le cardinal est une puissance de p et qu'on a un le résultat suivant :

1.2 Théorème. *Le centre d'un p-groupe est différent de $\{1\}$.*

Si G est un groupe de cardinal $n = p^\alpha m$ avec $\alpha \geq 1$ et p ne divisant pas m, on appelle **p-sous-groupe de Sylow** (voire p-Sylow) un sous-groupe de G de cardinal p^α. On a alors les deux théorèmes suivants :

1.3 Théorème. *Si p divise le cardinal de G, il existe des p-sous groupes de Sylow de G.*

On note $n_p(G)$ voire simplement n_p le nombre de p-Sylow de G.

1.4 Théorème. *Soit G un groupe de cardinal $p^\alpha m$ avec $p \not| m$.*

1) Les p-Sylow de G sont tous conjugués (donc leur nombre n_p divise n).

2) On a $n_p \equiv 1 \pmod{p}$ (donc n_p divise m).

Nous aurons aussi besoin du résultat suivant :

1.5 Proposition. *Tout groupe d'ordre p^2 est abélien.*

2 La non simplicité des groupes d'ordre ≤ 168

L'objectif de ce paragraphe est de prouver le théorème suivant :

2.1 Théorème. *Tout groupe d'ordre* $1 < n \leq 168$*, avec* n *non premier et différent de* 60 *et* 168 *est non simple.*

2.2 *Remarques.* 1) Si G est de cardinal p avec p premier, il est cyclique d'ordre p donc isomorphe à $\mathbf{Z}/p\mathbf{Z}$ et simple ("banal" ou "trivial"). En effet, si N est un sous-groupe de G, non réduit à l'élément neutre, son cardinal est un diviseur de p, différent de 1, donc égal à p. On élimine donc les nombres premiers ≤ 168 (il y en a 39).

2) Hormis ce cas, les p-groupes ne sont jamais simples. En effet, si G est un p-groupe, son centre est un sous-groupe distingué différent de l'élément neutre en vertu de 1.2. Si le groupe n'est pas abélien, il n'est donc pas simple à cause du centre et s'il est abélien il ne l'est pas non plus à cause de 1.1. On élimine ainsi tous les cardinaux de la forme p^r avec p premier et $r > 1$ qui sont ≤ 168. Il y en a 13 qui sont $4, 8, 16, 32, 64, 128$; $9, 27, 81$; $25, 125$; 49 et 121.

3) La démonstration qui suit est l'occasion d'utiliser un certain nombre de techniques sur les groupes finis. Il est clair qu'il y a de nombreuses façons de procéder (on verra quelques exemples de variantes ci-dessous) et que les choix que j'ai faits sont discutables. Le lecteur ne manquera pas de trouver sa propre voie.

2.1 L'utilisation des théorèmes de Sylow

2.1.1 Le gros Sylow est distingué

Le deuxième théorème de Sylow montre qu'un q-sous-groupe de Sylow est distingué si et seulement si il est tout seul, autrement dit si n_q vaut 1. On en déduit le lemme suivant :

2.3 Lemme. *Soit* $n = q^\alpha m$ *avec* $\alpha \geq 1$*,* q *premier,* $q \not| m$ *et* $m > 1$ *et soit* G *un groupe d'ordre* n*. On suppose que* m *n'a aucun diviseur congru à* 1 *modulo* q *autre que* 1*. Alors on a* $n_q = 1$ *et* G *est non simple. C'est le cas en particulier si l'on a* $m < q$*.*

Démonstration. C'est clair puisque n_q divise m et qu'on a $n_q \equiv 1 \pmod{q}$. Si m est plus petit que q, il ne peut avoir de diviseur non trivial congru à 1 modulo q (le plus petit est $q + 1$).

2.4 *Remarque.* L'application de ce lemme avec pour q le plus grand facteur premier de n et $m < q$ montre déjà le théorème dans bon nombre de cas, notamment les groupes d'ordres pq^α (p, q premiers $p < q$ et $\alpha \geq 1$). On élimine ainsi les 50 cardinaux de la forme pq et ceux de la forme pq^2, pq^3, pq^4 avec $p < q$ (7 valeurs : $18, 50, 98, 75, 147, 54$ et 162).

Avec m non premier, cela permet aussi d'éliminer des entiers de la forme $q^\alpha m$, soit parce que q est plus grand que m, soit simplement parce que m n'a pas de facteur non trivial congru à 1 modulo q. Ainsi, on peut éliminer les entiers de la forme $4q^\alpha$ avec q premier $\geq 5 > 4$. On élimine ainsi les 11 nombres de la forme $4q$ entre $4\times 5 = 20$ et $4\times 41 = 164$ ainsi que $4\times 5^2 = 100$. De même on élimine les entiers de la forme $8q$ avec $q \geq 11 > 8$ (il y en a 4), mais aussi $8 \times 5 = 40$ (car 8 n'a pas de diviseur congru à 1 modulo 5) et les entiers de la forme $9q$ avec $q = 5, 7, 11, 13, 17$ et $27 \times 5 = 135$. Enfin, cette technique permet de traiter les quatre cas suivants : $84 = 12\times 7$, $126 = 18\times 7$, $140 = 20 \times 7$ (car $12, 18$ et 20 n'ont aucun diviseur non trivial congru à 1 modulo 7) et $156 = 12 \times 13$.

2.1.2 Un petit Sylow distingué ?

Le même argument s'applique lorsque l'on a $n = p^\alpha m$ avec p premier ne divisant pas m (cette fois p n'est plus le plus grand facteur premier de n) et que m n'a pas de diviseur congru à 1 modulo p. On a alors $n_p = 1$ et l'unique p-Sylow est distingué. Mais, on ne retrouve ainsi que quatre cardinaux déjà éliminés ci-dessus : $3^2 \times 5 = 45$, $3^2 \times 11 = 99$, $3^2 \times 17 = 153$ et $3^3 \times 5 = 135$.

2.1.3 Comptage

Le calcul du nombre de sous-groupes de Sylow assorti d'un argument de comptage donne le résultat suivant :

2.5 Lemme. *Un groupe de cardinal pqr avec p, q, r premiers distincts, n'est pas simple.*

Démonstration. Supposons par exemple qu'on a $p < q < r$. Si G n'est pas simple, aucun des Sylow d'ordres p, q, r n'est isolé. Le nombre n_r de r-Sylow divise pq et il est $\geq r + 1$. Comme p, q sont plus petits que r, on a $n_r = pq$. Pour les q-Sylow, dont le nombre divise pr et est $\geq q + 1$ on peut seulement affirmer qu'on a $n_q \geq r$ et de même on a $n_p \geq q$. Mais, les éléments distincts de 1 de ces Sylow ne sont jamais dans l'intersection (car celle-ci, dont le cardinal divise deux nombres premiers, est réduite à $\{1\}$). On a donc $pq(r - 1) + r(q - 1) + q(p - 1) + 1$ éléments au moins dans le groupe, c'est-à-dire $pqr + r(q - 1) - q + 1$. Comme q est au moins égal à 3 et que r est $> q$, ce nombre est $> pqr$ et c'est absurde.

2.6 *Remarques.* 1) On élimine ainsi les 13 nombres de la forme pqr (le plus grand est $3 \times 5 \times 11 = 165$).

2) La même technique permet de traiter d'autres cas, par exemple $56 = 8 \times 7$ ou $132 = 12 \times 11$. Pour 56, s'il y a plusieurs 7-Sylow, il y en a 8 d'où

$8 \times 6 = 48$ éléments d'ordre 7 et il reste 8 éléments donc un seul 2-Sylow. Pour 132, si n_{11} est > 1 on a $n_{11} = 12$, d'où 120 éléments d'ordre 11, si n_3 est > 1 on a $n_3 = 4$ d'où 8 éléments d'ordre 4, ce qui ne laisse la place que pour un unique 2-Sylow.

2.2 Les arguments d'opérations

2.2.1 Le principe

Le trait commun de tous les arguments qui suivent réside dans le lemme :

2.7 Lemme. *Soit G un groupe simple de cardinal n. On suppose que G opère non trivialement sur un ensemble X de cardinal r. Alors, n est un diviseur de $r!$.*

Démonstration. Dire que G opère sur X signifie qu'on a un homomorphisme $\varphi : G \to \mathfrak{S}(X) \simeq \mathfrak{S}_r$. Dire que l'opération est non triviale se traduit par le fait que l'image de φ n'est pas réduite à l'identité. Le noyau de φ n'est donc pas égal à G et, comme c'est un sous-groupe distingué de G, il est réduit à $\{1\}$. On voit que φ est une injection de G dans $\mathfrak{S}_r$, de sorte que G s'identifie à un sous-groupe du groupe symétrique et son cardinal divise donc $r!$.

2.8 Corollaire. *Si un groupe de cardinal n opère non trivialement sur un ensemble X de cardinal r et si n ne divise pas $r!$ (par exemple si on a $n > r!$) le groupe G n'est pas simple.*

2.2.2 Applications

Parmi les opérations non triviales il y a les opérations transitives (au moins si l'ensemble n'est pas réduit à un point). On en connaît au moins deux (voir [DP]) :

- l'opération par conjugaison de G sur ses p-sous-groupes de Sylow,
- l'opération par translation de G sur lui-même ou sur l'ensemble G/H des classes à gauche modulo H.

La première opération, permet de montrer le lemme suivant :

2.9 Lemme. *Soit G un groupe d'ordre n et soit p un facteur premier de n. Si n_p est le nombre de p-Sylow de G et si n ne divise pas $n_p!$, le groupe G n'est pas simple.*

Démonstration. Si n_p est égal à 1 l'unique p-Sylow est distingué. Sinon, le groupe opère transitivement sur l'ensemble à $n_p > 1$ éléments de ses p-Sylow. On a ainsi un homomorphisme $\varphi : G \to \mathfrak{S}_{n_p}$ qui n'est pas trivial (i.e. n'envoie

pas G sur $\{\mathrm{Id}\}$) car l'opération est transitive et $n_p > 1$. Comme n ne divise pas $n_p!$, φ ne peut être injectif. Son noyau est donc un sous-groupe distingué de G, non trivial.

2.10 Corollaire. *Si n est de la forme $p^\alpha q^\beta$ et si n ne divise pas $p^\alpha!$ ou $q^\beta!$ (par exemple s'il est plus grand), le groupe n'est pas simple.*

Démonstration. Supposons, par exemple, que n ne divise pas $q^\beta!$. On sait que n_p divise q^β, donc est plus petit que q^β. Comme n ne divise pas $q^\beta!$, il ne divise pas non plus[6] $n_p!$ et on conclut par le lemme.

On peut appliquer le corollaire (dans le cas où n ne divise pas $q^\beta!$) avec $n = 2^\alpha \times 3$, avec $\alpha > 1$ et cela permet d'éliminer les nombres $12, 24, 48$ et 96. On élimine aussi par cette méthode $5 \times 16 = 80$ et $5 \times 32 = 160$ qui ne divisent pas $5! = 120$.

On peut aussi l'appliquer dans le cas où n ne divise pas $p^\alpha!$ avec $n = 4 \times 3^\beta$, $\beta \geq 2$. On élimine ainsi $36 = 4 \times 9$ et $108 = 4 \times 27$ car 9 et 27 ne divisent pas $4! = 24$.

Enfin, on peut appliquer directement le lemme dans certains cas. Par exemple si l'on a $n = 8 \times 3^\beta$ avec $\beta > 1$, le nombre n_3 divise 8 et il est congru à 1 modulo 3 donc, s'il est différent de 1, on a $n_p = 4$ et on conclut car n est > 24. On élimine ainsi le cas $n = 72$.

2.11 *Remarque.* On peut aussi éliminer $150 = 6 \times 5^2$ qui ne divise pas $n_5! = 6! = 720$, mais on va retrouver ce nombre au paragraphe suivant.

2.2.3 Les cas $n = 90$ et $n = 150$

On utilise ici une autre opération :

2.12 Lemme. *Soit G un groupe d'ordre $2m$ avec m impair, $m > 1$. Alors, G n'est pas simple.*

Démonstration. On fait opérer G sur lui-même par translation à gauche : $g.x = gx$. Cette opération est sans point fixe : la relation $gx = x$ implique $g = 1$. On obtient ainsi un homomorphisme injectif $\varphi : G \to \mathfrak{S}_n$. Le sous-groupe $\mathfrak{A}_n \cap G$ est distingué dans G, d'indice 1 ou 2 et il suffit de voir qu'il n'est pas égal à G. Soit σ un élément d'ordre 2 de G, son image par φ est d'ordre 2, donc un produit de transpositions disjointes, et sans point fixe, donc un produit de m transpositions. Comme m est impair c'est un élément de signature négative et on a donc un élément de G qui n'est pas dans $\mathfrak{A}_n$.

On traite ainsi les cas $n = 90 = 2 \times 3^2 \times 5$ et $n = 150 = 2 \times 3 \times 5^2$.

6. Si on a $a < b$, $a!$ divise $b!$.

2.2.4 Le cas $n = 120 = 2^3 \times 3 \times 5$

Ici encore c'est une opération qui va être décisive. Soit G un groupe d'ordre 120 et supposons que G soit simple. On considère les 5-Sylow de G. On a $n_5 \equiv 1 \pmod 5$ et n_5 divise 24. Cela ne laisse que deux choix : $n_5 = 1$ et le groupe n'est pas simple, ou $n_5 = 6$. Dans ce cas on a un homomorphisme injectif $\varphi : G \to \mathfrak{S}_6$. Or, on a le lemme suivant (voir aussi [DP] Ch. 1 cor. 8.6) :

2.13 Lemme. *Un sous-groupe d'indice* 6 *de* $\mathfrak{S}_6$ *est isomorphe à* $\mathfrak{S}_5$ *(donc non simple).*

Démonstration. Soit $G \subset M := \mathfrak{S}_6$ d'indice 6. On fait opérer (transitivement) M sur M/G par translation à gauche. On en déduit un homomorphisme $\psi : M \to \mathfrak{S}(M/G) \simeq \mathfrak{S}_6$. Le noyau de cette opération est un sous-groupe distingué de $M = \mathfrak{S}_6$ donc $\{1\}$, $\mathfrak{A}_6$ ou $\mathfrak{S}_6$ (voir [DP] Ch. 1 cor. 8.5). Comme l'opération est transitive, l'image est de cardinal multiple de 6, ce qui élimine les deux dernières possibilités. Il en résulte que ψ est injectif, donc un isomorphisme. Mais, dans cet isomorphisme, l'image du sous-groupe G est le stabilisateur de la classe G, donc contenu dans $\mathfrak{S}_5$, donc il lui est égal pour une raison de cardinal.

2.14 *Remarque.* Une variante de la preuve est la suivante. On reprend le plongement $G \subset \mathfrak{S}_6$. Si G n'est pas contenu dans $\mathfrak{A}_6$ il a un sous-groupe distingué en la personne de $G \cap \mathfrak{A}_6$. Sinon, G est contenu dans $\mathfrak{A}_6$, donc il est d'indice 3 dans ce groupe, ce qui prouve que $\mathfrak{A}_6$ n'est pas simple (car il opère sur $\mathfrak{A}_6/G$ de cardinal 3) et c'est absurde.

2.2.5 Le cas $n = 112 = 2^4 \times 7$

Soit G un groupe d'ordre 112 supposé simple. L'idée est assez voisine du cas $n = 120$.

On considère les 2-Sylow de G. S'ils ne sont pas distingués, il en a 7 de sorte qu'on a un homomorphisme (injectif puisque G est simple) $\varphi : G \to \mathfrak{S}_7$ et on identifie G et son image. Mais le cardinal de $\mathfrak{S}_7$ est $7! = 2^4 \times 3^2 \times 5 \times 7$, donc celui de $\mathfrak{A}_7$ est $2^3 \times 3^2 \times 5 \times 7$. Il en résulte que G n'est pas contenu dans $\mathfrak{A}_7$, et donc $G \cap \mathfrak{A}_7$ est un sous-groupe distingué non trivial de G !

2.15 *Exercice.* On se propose de donner autre preuve du cas $n = 112$. Soit G un groupe de cardinal 112, supposé simple.

1) Montrer que G n'a pas de sous-groupe strict de cardinal > 16.

2) a) Montrer que G a exactement 7 sous-groupes d'ordre 16.

b) Montrer que l'intersection de deux sous-groupes d'ordre 16 est de cardinal ≤ 4 (si l'intersection H est d'ordre 8 on montrera que H est distingué dans G).

3) Soit Σ_2 l'ensemble des 2-Sylow de G et soit $S \in \Sigma_2$.

a) Montrer que Σ_2 est de cardinal 7.

b) On fait opérer S sur Σ_2, puis sur $X = \Sigma_2 - \{S\}$ par conjugaison. Montrer que les orbites de S sur X sont de cardinal 4 (utiliser 2.b) et faire éclater une contradiction.

2.3 Un entier récalcitrant : $n = 144 = 2^4 \times 3^2$

Le lecteur vérifiera que nous avons épuisé les entiers ≤ 168, distincts de 60 et 168, à l'exception de 144 que nous traitons maintenant.

Soit G un groupe d'ordre 144, supposé simple.

On s'intéresse aux 3-Sylow de G. Leurs nombre est congru à 1 modulo 3 et divise 16. C'est donc 1, 4 ou 16. Dans le cas de 1 ou 4 on conclut que le groupe n'est pas simple par l'un des arguments précédents et c'est absurde. Supposons donc $n_3 = 16$. Les groupes d'ordre 9 ne peuvent pas être tous "disjoints" (i.e. se couper seulement sur l'élément neutre). Sinon on aurait $16 \times 8 = 128$ éléments d'ordre 3 ou 9 et il ne resterait la place que pour un unique 2-Sylow qui serait distingué. Il existe donc deux 3-Sylow distincts S_1 et S_2 se coupant en un sous-groupe d'ordre 3 engendré par un élément x d'ordre 3. On considère alors le centralisateur $H = C(x)$. Comme les groupes S_1 et S_2 sont abéliens en vertu de 1.5, H contient S_1 et S_2, donc au moins $6 + 6 + 3 = 15$ éléments. Comme son cardinal est multiple de 9 et diviseur de 144 il est multiple de 18. Si ce cardinal est > 18, l'indice de H est ≤ 4 et on a une opération de G sur G/H qui implique que G n'est pas simple. Il reste le cas où H est d'ordre 18 et contient les deux sous-groupes de Sylow S_1, S_2 d'ordre 9. Mais c'est impossible car ces sous-groupes sont d'indice 2 donc distingués dans H, donc égaux.

3 Le groupe simple d'ordre 60

3.1 Du côté de l'algèbre

3.1 Théorème. *Il existe un unique groupe simple d'ordre* 60 *qui est le groupe alterné* $\mathfrak{A}_5$.

Démonstration. Rappelons brièvement pourquoi $\mathfrak{A}_5$ est simple. Outre l'élément neutre, il contient 15 éléments d'ordre 2, doubles transpositions $(ab)(cd)$, tous

conjugués, 20 éléments d'ordre 3, cycles (abc), tous conjugués et 24 éléments d'ordre 5, cycles $\sigma = (abcde)$, se répartissant en deux classes de conjugaison, celle de σ et celle de σ^2. Si N est un sous-groupe distingué de $\mathfrak{A}_5$ non réduit à $\{1\}$, il contient l'un des types d'éléments, donc tous, par conjugaison et multiplication, mais pas seulement car ni $16 = 15 + 1$, ni 21, ni 25 ne divisent 60. Il contient donc au moins deux types d'éléments, donc au moins $15 + 20 + 1 = 36$ éléments et comme son cardinal divise 60, N est égal à $\mathfrak{A}_5$.

Inversement, soit G un groupe simple de cardinal 60. Un tel groupe ne peut opérer non banalement sur un ensemble de cardinal ≤ 4 et, s'il opère sur un ensemble de cardinal 5, il se plonge dans $\mathfrak{S}_5$ comme sous-groupe d'indice 2 donc est isomorphe à $\mathfrak{A}_5$. Dénombrons les différents Sylow. Comme G est simple, n_5, qui divise 6 et est congru à 1 modulo 5, est égal à 6. Cela montre qu'il y a 24 éléments d'ordre 5 dans le groupe. De même, n_3 divise 20, est > 4 et congru à 1 modulo 3, donc vaut 10 et on a 20 éléments d'ordre 3. Enfin, n_3 divise 15, il ne peut valoir 3 et s'il vaut 5 on a gagné, de sorte qu'on peut supposer $n_2 = 15$. Les 2-Sylow sont des groupes à 4 éléments et ils ne peuvent être "disjoints" (i.e. ne se couper que sur le neutre) car on aurait plus que 60 éléments. On considère deux tels Sylow S_1, S_2 se coupant selon un sous-groupe d'ordre 2 engendré par x et on regarde le centralisateur $H = C(x)$. Il contient au moins les 6 éléments de S_1 et S_2 en vertu de 1.5 et il est de cardinal multiple de 4 et diviseur de 60. Son cardinal est donc ≥ 12. S'il était > 12, G aurait une opération transitive sur G/H de cardinal < 5 et c'est impossible. On a donc $|H| = 12$ et l'opération de G sur G/H, de cardinal 5, permet de conclure.

3.2 *Remarque.* L'idée de considérer le centralisateur d'un élément d'ordre 2, utilisée ici dans le cas le plus trivial, est à la racine de la classification des groupes simples finis. Le point de départ de cette méthode est le théorème de Feit-Thomson (1963) qui affirme que tout groupe d'ordre impair est résoluble et dont une conséquence est que tout groupe simple non trivial est d'ordre pair, donc contient un élément d'ordre 2.

3.3 Corollaire. *Soit G un groupe d'ordre 60 qui contient 24 éléments d'ordre 5, 20 d'ordre 3 et 15 d'ordre 2. Alors, G est isomorphe à $\mathfrak{A}_5$.*

Démonstration. Il suffit de montrer que G est simple. Soit N un sous-groupe distingué de G, différent de $\{1\}$. S'il contient un élément d'ordre 5 (resp. 3), il contient le Sylow correspondant, donc il les contient tous puisqu'ils sont conjugués, donc il contient tous les éléments d'ordre 5 (resp. 3). Il contient donc au moins 21 éléments et comme son cardinal divise 60 il vaut 30 ou 60, donc contient à la fois des éléments d'ordre 3 et 5, donc son cardinal vaut au moins $20 + 24 + 1 = 45$ et N est égal à G.

Ce qui précède montre que si N est différent de G il ne contient que des éléments d'ordre 2 et, comme son ordre divise 60, c'est donc 2 ou 4. Si c'est 4 c'est un 2-Sylow, mais alors N contient tous les 2-Sylow, donc tous les éléments d'ordre 2 et c'est absurde. Si c'est 2, l'unique élément de N distinct de 1 est central. Mais alors il commute aux éléments d'ordre 5 et N contient des éléments d'ordre 10 et c'est absurde.

3.2 Le dodécaèdre

On désigne par τ le nombre d'or, $\tau = \dfrac{1+\sqrt{5}}{2}$, solution positive de l'équation $\tau^2 - \tau + 1 = 0$.

On considère le dodécaèdre régulier D de $\mathbf{R}^3$ défini comme l'enveloppe convexe des 20 sommets suivants :

$$D = \{\ (\pm 1, \pm 1, \pm 1)\ ;\ (0 \pm \tau^{-1}, \pm\tau)\ ;\ (\pm\tau, 0, \pm\tau^{-1})\ ;\ (\pm\tau^{-1}, \pm\tau, 0)\ \}$$

avec tous les signes $\pm$ possibles. On sait [7] qu'il s'agit d'un polyèdre régulier admettant 12 faces, 30 arêtes et 20 sommets.

L'isobarycentre des sommets de D étant l'origine, les rotations qui laissent D invariant fixent le point O et leurs axes passent par O. Nous admettrons [8] que le groupe des rotations est formé des 60 éléments suivants : l'identité, les 24 rotations d'ordre 5 (donc d'angles $\pm\dfrac{2\pi}{5}$ ou $\pm\dfrac{4\pi}{5}$) autour des axes joignant les centres de deux faces opposées de D, les 20 rotations d'ordre 3 (donc d'angles $\pm\dfrac{2\pi}{3}$) autour des axes joignant deux sommets opposés de D et enfin les 15 demi-tours autour des axes joignant les milieux de deux arêtes opposées de D. Le corollaire précédent donne aussitôt :

3.4 Théorème. *Le groupe $G^+(D)$ des rotations de $\mathbf{R}^3$ qui conservent le dodécaèdre est isomorphe à $\mathfrak{A}_5$. Le groupe $G(D)$ des isométries de $\mathbf{R}^3$ conservant D est isomorphe au produit direct $\mathfrak{A}_5 \times \{\pm\mathrm{Id}\}$.*

Démonstration. Pour le groupe $G(D)$ il suffit de noter qu'il contient bien $-\mathrm{Id}$ qui est une homothétie, donc un élément central.

7. Nous allons admettre ici beaucoup de choses sur les polyèdres réguliers, voir en Annexe quelques précisions qui permettent de rendre correct le calcul du groupe de D. Peut-être qu'un jour je mettrai sur ma page web les notes de mon cours de Sèvres d'autrefois. En attendant, le lecteur consultera [Berger].

8. On s'en convainc aussitôt dès qu'on a un dodécaèdre régulier entre les mains !

4 Le groupe simple d'ordre 168

4.1 Théorème. *Il existe un unique groupe simple d'ordre* 168 *qui est isomorphe à* $PSL(2, \mathbf{F}_7)$ *ou à* $PSL(3, \mathbf{F}_2)$.

Démonstration. Voir [DP] Ch. IV, th. 4.1 et Prop. 5.1 pour la simplicité et exercice 5.3 pour l'identification de ce groupe à $PSL(2, \mathbf{F}_7)$.

4.2 *Remarque.* Le groupe simple d'ordre 168 est le groupe des homographies qui conservent la quartique de Klein : $X^3Y + T^3T + T^3X = 0$. L'étude des liens entre cette courbe (ou surface) et le groupe d'ordre 168 est l'une des plus belles choses que je connaisse en mathématiques. On en trouvera un aperçu (et une bibliographie) sur ma page web :

http ://www.math.u-psud.fr/ perrin/conferences.html

à la rubrique *La quartique de Klein et le groupe simple d'ordre 168.*

5 Annexe : à propos du dodécaèdre

Le lecteur qui le souhaite trouvera ci-dessous quelques précisions au sujet du dodécaèdre. Elles permettent de rendre parfaitement correct le théorème 3.4. Cependant, elles sont loin d'épuiser le sujet. En particulier, on passe sous silence tout ce qui concerne la géométrie du dodécaèdre (faces, arêtes), ce qu'on peut à bon droit considérer comme une arnaque. Le premier paragraphe propose une construction du dodécaèdre, le second, sous forme de problème, contient les résultats qui permettent de calculer son groupe d'isométries.

5.1 Construction

Rappelons qu'on note τ le nombre d'or $\tau = \dfrac{1+\sqrt{5}}{2} \sim 1,618$ et qu'on a les formules : $\tau^2 = \tau + 1$ et $\tau^{-1} = \tau - 1$.

Une des manières de construire mathématiquement le dodécaèdre consiste à partir d'un cube et à bâtir des "toits" à quatre pentes sur chaque face du cube, de façon à ce que les divers toits se raccordent en donnant des faces pentagonales régulières, comme le montre la figure ci-dessous.

Pour cela, on choisit un repère orthonormé de l'espace. On peut définir analytiquement le cube comme l'enveloppe convexe de ses sommets, à savoir les huit points $(\pm 1, \pm 1, \pm 1)$. On cherche alors, par exemple, les points b, b' formant l'arête du toit située au-dessus de la face du haut. On suppose que cette arête est parallèle à l'axe des y, de sorte que les points b, b' sont de

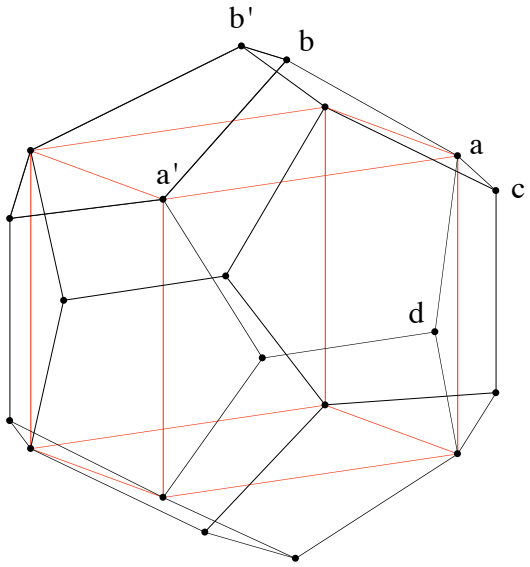

FIGURE 1 – Le dodécaèdre bâti sur le cube

la forme $(0, y, z)$, et qu'elle est symétrique par rapport au plan $y = 0$, donc avec des ordonnées opposées. Rappelons, voir [ME], que le rapport entre la diagonale et le côté d'un pentagone régulier est le nombre d'or τ. Comme l'arête du cube, qui devient la diagonale des faces du dodécaèdre, vaut 2, l'arête du dodécaèdre vaut donc $2\tau^{-1}$ et on en déduit que l'ordonnée de b vaut τ^{-1} et que celle de b' vaut $-\tau^{-1}$. Pour trouver la cote de b et b', il suffit d'écrire que la longueur ab avec $a = (1, 1, 1)$ vaut aussi $2\tau^{-1}$. On a ainsi l'équation $1 + (1 - \tau^{-1})^2 + (z - 1)^2 = 4\tau^{-2}$ qui donne $(z - 1)^2 = \tau^{-2}$ donc $z - 1 = \tau^{-1}$ et $z = \tau$. On a trouvé $b = (0, \tau^{-1}, \tau)$ et $b' = (0, -\tau^{-1}, \tau)$. Les dix autres sommets du dodécaèdre se calculent de la même manière et on obtient en définitive l'ensemble D annoncé ci-dessus.

5.2 Quelques résultats sur le groupe des isométries

L'espace $V = \mathbf{R}^3$ est muni du produit scalaire usuel pour lequel la base canonique $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$ est orthonormée. On note O l'origine, $O = (0, 0, 0)$.

On considère l'ensemble D formé des 20 points ci-dessous (le signe $\pm$ prend toutes les valeurs possibles) :

$$D = \{\ (\pm 1, \pm 1, \pm 1)\ ;\ (0, \pm\tau^{-1}, \pm\tau)\ ;\ (\pm\tau, 0, \pm\tau^{-1})\ ;\ (\pm\tau^{-1}, \pm\tau, 0)\ \}$$

On désigne par G le sous-groupe de $O(V)$ formé des éléments g qui laissent invariant D, c'est-à-dire vérifient $g(D) = D$ et on pose $G^+ = G \cap O^+(V)$.

1) Montrer que les points de D sont sur une même sphère de centre l'origine. Déterminer l'isobarycentre des points de D. Montrer que le groupe des isométries affines qui conservent D est isomorphe à $G(D)$.

Soit σ une permutation **paire** de l'ensemble $\{1,2,3\}$ et soit $\epsilon = (\epsilon_1, \epsilon_2, \epsilon_3)$ un élément de $\{1,-1\}^3$. On considère la transformation $u_{\sigma,\epsilon}$ définie par la formule :

$$u_{\sigma,\epsilon}(e_i) = \epsilon_i e_{\sigma(i)} \qquad \text{pour} \quad i = 1,2,3.$$

Soit H l'ensemble des transformations $u_{\sigma,\epsilon}$ pour $\sigma \in \mathfrak{A}_3$ et $\epsilon \in \{1,-1\}^3$.

2) Montrer que H est contenu dans $O(V)$, déterminer $|H|$ et $H^+ = H \cap O^+(V)$. Montrer qu'on a $H \simeq H^+ \times \{1,-1\}$. Montrer que H est contenu dans G, de sorte que H opère sur D. Montrer que H admet sur D deux orbites que l'on précisera.

3) On pose $a = (1,1,1)$, $b = (0,\tau^{-1},\tau)$, $m = (\tau^{-1},1,\tau)$. On considère le demi-tour d'axe Om, que l'on note v_m. Montrer que l'on a $v_m(a) = b$, puis que v_m est dans G. (Il sera utile de préciser l'effet de v_m sur tous les éléments de D.)

4) Déduire de 3) que G opère transitivement sur D. Montrer que $|G|$ est multiple de 20 et de 24, donc de 120.

5) Montrer que G^+ opère transitivement sur D. (On utilisera un point $z \in D$ tel que $v_m(z) = -z$.)

6) On reprend les notations de 3) et on pose, de surcroît, $c = (\tau, 0, \tau^{-1})$ et $d = (\tau^{-1}, \tau, 0)$, voir figure ci-dessus.

a) Soit $g \in G$. On suppose que g laisse fixe b, c, d. Montrer que g est l'identité.

b) Soit G_a le stabilisateur de a. Montrer que G_a permute les points b, c, d (on pourra considérer la position des points de D par rapport au plan d'équation $x + y + z = \sqrt{5}$).

c) Montrer qu'on a $|G_a| \leq 6$ et en déduire qu'on a $|G| = 120$ et $|G^+| = 60$.

7) Montrer que G^+ contient 20 éléments d'ordre 3, 15 d'ordre 2 et 24 d'ordre 5.

Indication : Il y a mille et une manières d'aboutir au résultat. Voici quelques pistes. Pour montrer que G^+ contient au moins 20 éléments d'ordre 3 on utilisera les conjugués des sous-groupes G_a. Pour montrer qu'il contient au moins 15 éléments d'ordre 2, on montrera qu'il y a 15 éléments d'ordre 2 dans G^-, toujours en utilisant les sous-groupes G_a. Enfin, pour les sous-groupes

d'ordre 5, qui existent en vertu de Sylow et sont formés de rotations de même axe, on montrera qu'il n'y en a pas qu'un seul (donc qu'il y en a six, toujours par Sylow) en conjuguant un tel sous-groupe par une rotation d'ordre 3. Le lecteur ne manquera pas de trouver sa propre voie, éventuellement plus géométrique.

6 Références

[Berger] BERGER Marcel, *Géométrie*, Nathan, 1990.

[DP] PERRIN Daniel, *Cours d'Algèbre*, Ellipses, 1996.

[ME] PERRIN Daniel, *Mathématiques d'école*, Cassini, 2011.