Transfert et groupes finis

Gabriel Pallier, gabriel@pallier.org

2 décembre 2014

Résumé

Remarqué par Schur et Artin, l'homomorphisme de transfert d'un groupe dans l'abélianisé de l'un de ses sous-groupe intervient en théorie des groupes et en théorie algébrique des nombres. On se propose de le décrire, et d'en donner deux applications : tout d'abord, une interprétation du lemme de Gauss concernant la réciprocité quadratique ; ensuite, une preuve du théorème du complément normal de Burnside concernant les groupes finis, qui nous permettra d'énumérer les 4 classes d'isomorphismes de groupes d'ordre 2014 et les 2 d'ordre 2015, nombres qui possèdent une complexité arithmétique relativement faible (ce sont des produits de 3 facteurs premiers distincts)

Description Ces notes supportent un exposé au séminaire des élèves de l'Ecole polytechnique, le 2 décembre 2014. La référence majeure est le cours de Serre [3, Chapitre 7], notamment pour la section 1. Les exercices du cours de Perrin sur les groupes [2, Chapitre 1] interviennent dans les sections 3 et 4.

Table des matières

1 L'homomorphisme de transfert

Cette section est pour l'essentiel une réécriture de [3, 7.1].

1.1 Définition

Soient G un groupe, H un sous-groupe d'indice fini n de G. G agit par translation à gauche sur l'ensemble des classes à gauche $X = G/H$; donc sur un système de représentants des classes S de telle manière que pour tout s dans S, $g.s$ est l'unique élément de S tel que $gsH = (g.s)\,H$. On pose alors, pour tout s dans S,

$$gs = (g.s)\,h_{s,g},$$

où $h_{s,g}$ est par définition dans H, puis on définit le **transfert** $V_{G\to H} : G \to H^{\mathrm{ab}} = H/[H,H]$ par

$$V_{G\to H}(g) \equiv \prod_{s\in S} h_{s,g.s} \pmod{[H,H]}. \tag{1}$$

Le théorème suivant détaille les propriétés du transfert :

Théorème 1.1 (Schur, 1902)**.** *L'application $V_{G\to H}$ définie comme précédemment, ne dépend pas du choix de représentants des classes de G/H. De plus, c'est un morphisme de groupes de G dans H^{ab}, appelé homomorphisme de transfert (Verlagerung).*

Démonstration. Soit S' un autre choix de représentants : on note x' le représentant de la classe de x, et h' tel que $gx' = (g.x')\,h'_{x,g}$, V et V' les transferts associés à S et S'. Alors par définition

$$\begin{aligned} h_{s,g.s}\left(h'_{s',g.s'}\right)^{-1} &= (g.s)^{-1}\,gs\,(gs')^{-1}\,(g.s') \\ &= (g.s)^{-1}\,gss'^{-1}g^{-1}\,(g.s'). \end{aligned}$$

Remarquons que ss'^{-1} est dans H. Modulo $[H,H]$, nous pouvons donc écrire :

$$h_{s,g.s}\left(h'_{s',g.s'}\right)^{-1} \equiv (g.s)^{-1}\,(g.s')\,ss'^{-1}.$$

On fait le produit sur tous les $s \in S$:

$$V(g)\,V'(g)^{-1} \equiv \prod_{s\in S}(g.s)^{-1}\,(g.s') \prod_{s\in S} ss'^{-1} \equiv \prod_{s\in S} s^{-1}s' \prod_{s\in S} ss'^{-1}$$

(où l'on a fait le changement de variables $s \leftarrow g.s$ pour la deuxième égalité). Le dernier terme est un produit de commutateurs, donc neutre dans l'abélianisé.

Maintenant, il faut voir que V est un morphisme de groupes. Par définition, pour tous g, g' dans G,

$$h_{g'.s,gg'.s}h_{s,g'.s} \equiv (gg'.s)^{-1}\,g\,(g'.s)\,(g'.s)^{-1}\,g's \equiv (gg'.s)^{-1}\,gg's \equiv h_{s,gg'.s},$$

d'où

$$V(g)\,V(g') \equiv \prod_{s\in S} h_{s,g.s} \prod_{s\in S} h_{s,g'.s} \equiv \prod_{s\in S} h_{g'.s,gg'.s}h_{s,g'.s} \equiv \prod_{s\in S} h_{s,gg'.s} \equiv V(gg').$$

□

Remarque 1.2. D'image abélienne, $V_{G\to H}$ se factorise à gauche par $\pi : G \twoheadrightarrow G^{\mathrm{ab}}$ et donne lieu à un morphisme $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ encore appelé transfert.

1.2 Evaluation du transfert

L'expression (1) qui définit le transfert n'est pas aisée à calculer telle qu'elle est donnée pour un choix quelconque de représentants, et ce d'autant plus que l'indice de H est grand. Une fois que l'on s'est fixé $g \in G$, il existe cependant un choix de représentants particulièrement adapté pour évaluer $V_{G\to H}(g)$.

Soient $O_1, \dots O_r$ les orbites de G/H sous l'action de $\langle g\rangle$ par translation à gauche ; $s_1, \dots s_r$ des représentants, et $f_1, \dots f_r$ les cardinaux de ces orbites. Posons alors

$$S = \left\{ \begin{array}{c} s_1, gs_1, \dots g^{f_1-1}s_1, \\ s_2, gs_2, \dots, g^{f_2-1}s_2, \\ \dots \\ s_r, gs_r, \dots, g^{f_r-1}s_r \end{array} \right\}.$$

Le système S est conçu de telle sorte que $g.g^{k-1}s_i = g^k s_i$ tant que $k < f_i$ et $g.g^{f_i-1}s_i = s_i = g^{f_i}s_i \left(g^{f_i}s_i\right)^{-1} s_i$. Ainsi,

$$h_{g^k s_i, g.g^k s_i} = \begin{cases} 1 & \text{si } 0 \leqslant k < f_i - 1 \\ s_i^{-1} g^{f_i} s_i & \text{si } k = f_i - 1 \end{cases}.$$

Posant $h_i = s_i^{-1} g^{f_i} s_i$, nous obtenons la formule dite d'évaluation du transfert [3, Proposition 7.2] :

$$V_{G\to H}(g) \equiv \prod_{i=1}^{r} h_i. \tag{2}$$

Un cas particulier important est celui où g^{f_i} commute à s_i. C'est par exemple le cas si H est contenu dans le centre de G :

Corollaire 1.3. *Si H est central d'indice n dans G, alors*[1] *pour tout $g \in G$,*

$$V_{G\to H}(g) = g^n. \tag{3}$$

2 Transfert et réciprocité quadratique

L'objet ici n'est pas de démontrer complètement la loi de réciprocité quadratique mais d'éclairer quelques lemmes techniques qui se retrouvent comme ingrédient dans beaucoup de ses preuves.

2.1 Lemme de Gauss

Soit p un nombre premier impair ; rappelons que pour tout entier relatif a, le symbole de Legendre $\left(\frac{a}{p}\right)$ vaut par définition 0 si $p \mid a$, 1 si a est résidu quadratique modulo p et -1 sinon. Un critère dû à Euler nous dit alors que

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Le lemme de Gauss suivant exprime aussi le symbole de Legendre :

1. Il n'est pas nécessaire de préciser « modulo le dérivé de H » dans l'égalité (3) puisque H étant central dans G, il est déjà abélien.

Proposition 2.1. *Soit p un nombre premier impair, $a \in \mathbb{Z} - p\mathbb{Z}$. Alors*

$$\left(\frac{a}{p}\right) = (-1)^{\epsilon(a)},$$

où

$$\epsilon(a) = \left| \left\{ \overline{a}, \overline{2a}, \ldots, \overline{((p-1)/2) \times a} \right\} \cap \left\{ \overline{\frac{p+1}{2}}, \ldots, \overline{p-1} \right\} \right|$$

est le nombre de classes résiduelles parmi les $\overline{ia}$, $1 \leqslant i \leqslant \frac{p-1}{2}$ qui ont un représentant dans $\mathbb{Z}$ compris entre $\frac{p}{2}$ et p.

Le lemme de Gauss, à l'origine un outil pour démontrer la loi de réciprocité quadratique, s'interprète très bien dans la théorie du transfert.

Soit $G = \mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ et son sous-groupe $Q = \{\pm 1\}$, d'indice $(p-1)/2$. Un système de représentants des classes de G/Q est donné par $S = \left\{1, 2, \ldots \frac{p-1}{2}\right\}$. Ainsi, l'application qui à $x \in \mathbb{F}_p^\times$ associe $(-1)^{\epsilon(a)}$ pour $\overline{a} = x$ est le transfert $V_{G \to Q}$: avec les notations du paragraphe précédent, $f_i = 2$ pour tout i et $h_i = 1$ si la classe résiduelle ia admet un représentant dans $\left\{1, \ldots \frac{p-1}{2}\right\}$ et -1 sinon. Comme nous sommes dans le cadre abélien, le corollaire 1.3 à l'évaluation du transfert entraîne

$$(-1)^{\epsilon(a)} = \overline{a}^{\frac{p-1}{2}},$$

l'égalité précédente ayant lieu dans Q. D'après l'identité d'Euler, le terme de droite correspond bien à $\left(\frac{a}{p}\right)$.

2.2 Sur le chemin de la réciprocité quadratique

Notons que l'on peut aussi choisir, en guise de système de représentants des classes de G/Q, l'ensemble

$$S' = \{2, 4, \ldots p-1\}.$$

Au lieu du lemme de Gauss, la propriété d'évaluation du transfert entraîne alors la relation d'Eisenstein, qui mène à une preuve géométrique de la loi de réciprocité quadratique. Cette voie est présenté en tant qu'exercice dans [1, Chapitre 1].

Aussi bien le lemme de Gauss que la relation d'Eisenstein permettent d'obtenir via un calcul direct la loi complémentaire

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod 8 \\ -1 & \text{si } p \equiv \pm 3 \pmod 8. \end{cases}$$

Pour le cas général où l'on remplace 2 par un nombre premier impair ℓ, il faut un peu plus de travail. Une méthode, proposée par Eisenstein (1845) consiste à déduire du lemme de Gauss la relation trigonométrique

$$\left(\frac{\ell}{p}\right) = \prod_{s \in S} \frac{\sin(2\pi \ell s/p)}{\sin(2\pi s/p)}.$$

Cette démarche est suivie dans l'appendice au premier chapitre du cours d'Arithmétique de Serre [4].

Pour finir, signalons qu'à l'occasion de sa nouvelle preuve de la loi de réciprocité quadratique, Zolotarev en 1872 découvrit cet énoncé équivalent au lemme de Gauss (ou à la relation d'Eisenstein) :

Proposition 2.2. *Le caractère de Legendre de $\alpha \in \mathbb{F}_p^\times$ est égal à la signature de la permutation $\sigma(\alpha)$ de*[2] *$\mathbb{F}_p^\times$ associée à la multiplication par α.*

Pour voir que le lemme de Gauss et celui de Zolotarev sont équivalents, remarquons que $\sigma(\alpha)$ est, en réalité, une permutation par blocs des paires $\{x, -x\}$ de $\mathbb{F}_p^\times$. C'est donc, encore, une permutation des couples $(x, -x)$ pour $x \in S$, à la différence près que l'on doit cette fois-ci réordonner les couples qui ont été désordonnés ; autrement dit, appliquer la permutation $\rho(\alpha)$ dont le lemme de Gauss mesure la signature. Ainsi, $\sigma(\alpha)\rho(\alpha)^{-1}$ est une permutation de $\mathbb{F}_p^\times$ en deux blocs S et $\mathbb{F}_p^\times - S$, et les restrictions sur les deux blocs étant conjuguées, ont même signature. $\sigma(\alpha)\rho(\alpha)^{-1}$ est alternée ; ceci conclut.

3 Théorèmes de complément normal

Cette partie concerne spécifiquement la théorie des groupes finis, avec à l'esprit leur classification. Il s'agit en toute généralité d'un problème extrêmement vaste et difficile, même mise à part la classification des groupes finis simples (achevée dans les années 1980). D'une part, les extensions ne sont pas toujours scindées (à la différence des espaces vectoriels où l'on peut invoquer l'existence d'un supplémentaire, ce qui revient à faire vivre le quotient dans l'objet de départ) ; d'autre part les extensions même scindées ne se reconstruisent en général pas comme des sommes directes (hormis le cas abélien, qui relève plus largement de celui des modules). En conséquence, exhiber et même savoir décrire un sous-groupe distingué n'est pas forcément suffisant pour déterminer la structure globale.

3.1 Un premier résultat pour les sous-groupes de Hall

Dans un groupe G fini, le sous-groupe $H \subset G$ est dit sous-groupe de Hall si son ordre et son indice sont premiers entre eux. C'est le cas, des sous-groupes de p-Sylow pour p premier (qui sont les minimaux parmi les sous-groupes de Hall). Le premier résultat de cette partie concerne les sous-groupes de Hall :

Théorème 3.1. *Soit G un groupe fini, H un sous-groupe de Hall. On suppose que H est central dans G. Alors, H admet un complément dans G, c'est-à-dire qu'il existe un sous-groupe $N \subset G$ tel que $G/N \simeq H$.*

Démonstration. Soit V le transfert de G vers H^{ab}. Comme H est central, il est égal à son abélianisé. Il suffit donc de montrer que le transfert est surjectif, le complément sera fourni par son noyau. Plus précisément, on va montrer que $V_{|H} \to H$ est un isomorphisme. D'après le corollaire 1.3 à la formule d'évaluation du transfert, pour tout $u \in H$

$$V(u) = u^{[G:H]}.$$

2. ou plus simplement de $\mathbb{F}_p$, c'est la même signature car 0 est fixe

Donc $\ker V_{|H}$ est formé d'éléments dont l'ordre divise $|H|$ et $[G:H]$. Mais H est un sous-groupe de Hall, donc $V_{|H}$ est injectif. Puisque H est fini, $V_{|H}$ est surjectif. □

Si $H \subset G$ vérifie les hypothèses du théorème précédent, il y a donc une suite exacte

$$1 \to N \to G \to H \to 1$$

qui se scinde[3] par l'inclusion $H \hookrightarrow G$. Comme $|N|$ et $|H|$ sont premiers entre eux,

$$\begin{aligned} N &\lhd G \\ N \cap H &= \{1\} \\ NH &= G, \end{aligned}$$

ce qui permet d'affirmer que G est produit semi-direct de N par H, noté $N \rtimes H$.

Remarque 3.2. Le complément N n'est pas seulement normal ; il est caractéristique, comme tout sous-groupe de Hall normal (noté $N \trianglelefteq G$). Soit en effet $x \in G$; dans G/N, $x^{[G:N]} \equiv 1$, d'où $x^{[G:N]} \in N$. Si de plus $x^{|N|} = 1$ alors $x \in N$; donc N contient tous les éléments dont l'ordre divise $|N|$, et par conséquent, tous les sous-groupe de son ordre. N est l'unique de son ordre parmi les sous-groupes de G, il est stable par tout automorphisme.

3.2 Théorème de Burnside

Le théorème de Burnside proprement dit est le suivant. Il concerne cette fois-ci les sous-groupes de Sylow. La différence principale avec l'énoncé précédent est qu'il intègre l'argument de Frattini, ce qui lui permet de reposer sur une hypothèse un peu plus faible :

Théorème 3.3 (Burnside, 1905 ?)**.** *Soit G un groupe fini, H un p-sous-groupe de Sylow de G central dans son normalisateur. Alors, H admet un p-complément dans G, c'est-à-dire un sous-groupe $N \subset G$ tel que $G/N \simeq H$.*

Preuve du théorème 3.3 de Burnside. Pour la preuve de ce résultat, nous utiliserons le

Lemme 3.4 (Frattini)**.** *Soit H un p-Sylow abélien de G. Alors, pour tous $h \in H$ et $s \in G$ il existe $n \in N_G H$ tel que*

$$s^{-1}hs = n^{-1}hs.$$

Autrement dit, les conjugués de h dans G sont encore conjugués de H dans $N_G H$.

Preuve du lemme 3.4 de Frattini. Nous savons que $s^{-1}C_G\{h\}s = C_G\left\{s^{-1}hs\right\}$ et H étant abélien, $H \subset C_G\{h\}$ d'où en posant $H' = s^{-1}Hs$

$$H,\ H' \subset C_G\left\{s^{-1}hs\right\}.$$

3. De manière générale toutes les extensions de H' par N' finis sont scindées dès que N' et H' sont d'ordres premiers entre eux : c'est le théorème de Schur-Zassenhaus [3, Théorème 4.10], qui correspond à l'annulation d'un second groupe de cohomologie, qui encode une partie de la classification des extensions.

H et H' sont deux p-Sylow de G et a fortiori de $C_G\left\{s^{-1}hs\right\}$. D'après les théorèmes de Sylow ils sont conjugués par $k \in C_G\left\{s^{-1}hs\right\}$:

$$H = k^{-1}H'k.$$

Posons $n = sk$. Nous obtenons que $n \in N_G H$ conjugue h à $s^{-1}hs$. □

A présent, démontrons le théorème. Par évaluation du transfert, pour $u \in H$ nous pouvons écrire avec les notations de la première partie

$$V(u) = \prod_{i=1}^{r} s_i^{-1} u^{f_i} s_i.$$

D'après le lemme 3.4 de Frattini, pour tout $i \in \{1, \ldots, r\}$ il existe $n_i \in N_G H$ tel que $s_i^{-1}u^{f_i}s_i = n_i^{-1}u^{f_i}n_i$. De plus, par hypothèse H est central dans son normalisateur, donc $V(u) = u^{[G:H]}$. La conclusion est la même que dans la preuve du théorème 3.1. □

Dans la pratique, le théorème 3.3 est plus utile que le théorème 3.1, ceci parce qu'on dispose d'énoncés d'existence pour les sous-groupes de Sylow, à la différence des sous-groupes de Hall généraux. Voyons une première application, qui découle du

Lemme 3.5. *Soit G un groupe fini, p le plus petit facteur premier de $|G|$, H un sous-groupe d'ordre p, distingué dans G. Alors, H est central.*

Démonstration. G opère sur H par conjugaison ; les orbites pour cette action ont pour cardinaux des diviseurs de G ; donc elles sont de cardinaux 1 ou $\geqslant p$, et la somme des cardinaux vaut p. Par ailleurs, l'identité est fixée. Donc tous les éléments de H sont fixés. □

Proposition 3.6. *Soit G un groupe de cardinal $m = p_1 p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ avec $p_1 < \cdots < p_s$ des nombres premiers, $s \geqslant 2$. Alors G n'est pas simple.*

Démonstration. G possède un p_1-sous groupe de Sylow S. Le cardinal de $N_G(S)$ est un multiple de p_1 et un diviseur de $|G|$; donc p_1 est son plus petit diviseur premier. D'après le lemme 3.5 S est central dans $N_G(S)$. En vertu du théorème 3.3 il possède un complément normal N dans G. En particulier G n'est pas simple. □

Remarque 3.7. Il existe d'autres théorème de complément normal. Celui de Cayley par exemple : si un 2-Sylow est cyclique alors il possède un complément normal.

4 Groupes d'ordre 2014 et 2015

La démarche générale de preuve est celle du « dévissage » qui relève de l'analyse-synthèse ; nous commençons par décrire les sous-groupes d'un groupe général d'ordre 2015 (resp. 2014) puis nous recherchons leurs extensions possibles, et finalement lesquelles sont isomorphes entre elles.

4.1 Quelques lemmes préliminaires

On démontre ici quelques résultats classiques sur les groupes finis. Ils font tous l'objet (sauf le lemme 4.2) d'exercices dans le livre de Perrin [2, Chapitre 1].

4.1.1 Groupes d'ordre pq

Lemme 4.1. *Soit G un groupe d'ordre pq avec p et q premiers distincts, $p < q$ et $p \nmid q - 1$. Alors G est cyclique.*

Démonstration. Le nombre de p-Sylow de G est congru à 1 modulo p et divise q ; G possède donc un unique p-Sylow, qui est distingué. Si P est le p-Sylow de G et Q un q-Sylow, on dispose donc d'une action $Q \rightsquigarrow P$ par conjuguaison, obtenue par restriction de celle de G. L'équation aux classes pour cette action donne

$$p = \sum_{x \in \Omega} \frac{q}{|\mathrm{C}_N x|},$$

où Ω est l'ensemble des orbites et $|\mathrm{C}_N x|$ le cardinal du centralisateur [4] d'(un représentant de) x. Par $p < q$, on déduit que tous les centralisateurs sont totaux et donc $[P, Q] = \{1\}$. Comme $P \simeq \mathbb{Z}/p\mathbb{Z}$ et $Q \simeq \mathbb{Z}/q\mathbb{Z}$, on finalement $G \simeq \mathbb{Z}/pq\mathbb{Z}$. □

4.1.2 Homomorphismes entre groupes cycliques

Lemme 4.2. *La classe des groupes cycliques est stable par $Hom\,(-,-)$; plus précisément*

$$Hom\,(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/d\mathbb{Z},$$

où d est le pgcd de n et de m.

Démonstration. Soit $\varphi \in \mathrm{Hom}\,(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$; alors φ est complètement déterminé par $\varphi(1)$. Il y a une restriction sur l'image de φ, puisque ses éléments sont d'ordre divisant à la fois n et m. Les éléments d'ordre divisant d dans $\mathbb{Z}/m\mathbb{Z}$ forment un sous-groupe isomorphe à $\mathbb{Z}/d\mathbb{Z}$; donc

$$\mathrm{Hom}\,(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \simeq \mathrm{Hom}\,(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/d\mathbb{Z})\,.$$

Pour finir, on vérifie que

$$\begin{array}{rcl} \mathrm{Hom}\,(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/d\mathbb{Z}) & \to & \mathbb{Z}/d\mathbb{Z} \\ \varphi & \mapsto & \varphi(1) \end{array}$$

est un isomorphisme. □

4.1.3 Isomorphismes entre produits semi-directs

Pour finir, le lemme suivant donne un critère simple d'isomorphisme pour les produits semi-directs :

4. On s'est autorisé l'écriture $\mathrm{C}_N x$ qui ne veut en soi rien dire, parce que les centralisateurs de deux éléments d'une même orbite sont conjugués et que seul nous importe le cardinal.

Lemme 4.3. *Soient φ, ψ des opérations de H sur N qui diffèrent d'un automorphisme au départ, c'est-à-dire qu'il existe $\alpha \in Aut(H)$ tel que*

$$\varphi = \psi \circ \alpha.$$

Alors, les produits semi-directs $N \rtimes_\psi H$ et $N \rtimes_\varphi H$ sont isomorphes, via l'application donnée sur les couples par

$$\begin{array}{rcl} \Phi : N \rtimes_\varphi H & \to & N \rtimes_\psi H \\ (n, h) & \mapsto & (n, \alpha(h)). \end{array}$$

En particulier, le lemme implique que si tous les morphismes non triviaux de H vers $\mathrm{Aut}(N)$ diffèrent d'un automorphisme au départ, la notation $N \rtimes H$ ne désigne qu'une seule classe d'isomorphismes de groupes, et n'est pas ambigüe.

Démonstration. Calculons

$$\begin{aligned} \Phi(n, h)\,\Phi(n', h') &= (n, \alpha(h))\,(n', \alpha(h')) \\ &= (n \cdot \psi \circ \alpha(h)(n'), \alpha(h)\,\alpha(h')) \\ &= (n\varphi(h)(n'), \alpha(hh')) \\ &= \Phi[(n, h)(n', h')]. \end{aligned}$$

□

4.2 Groupes d'ordre 2015

Le nombre 2015 se factorise sous la forme

$$2015 = 5 \times 13 \times 31.$$

Théorème 4.4. *Il existe exactement deux classes d'isomorphisme de groupes d'ordre 2015, à savoir : le groupe cyclique $\mathbb{Z}/2015\mathbb{Z}$ et un unique produit semi-direct non direct $(\mathbb{Z}/31\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/13\mathbb{Z}$.*

Soit donc G un groupe d'ordre 2015, S un sous-groupe de 5-Sylow (on peut simplement invoquer le lemme de Cauchy pour son existence). D'après le lemme 3.5, S est central dans son normalisateur [5] D'après le lemme du complément normal de Burnside, S possède un complément N dans G, d'ordre $2015/5 = 403 = 13 \times 31$ avec $13 \nmid 31$. D'après le lemme, N est cyclique, soit :

$$N \simeq \mathbb{Z}/403\mathbb{Z} \simeq \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/31\mathbb{Z}.$$

On cherche à présent les extensions scindées de N par S ; autrement dit les morphismes de S vers $\mathrm{Aut}(N)$. Le lemme des restes chinois (version anneaux) nous dit que

$$\mathrm{Aut}(N) \simeq (\mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/31\mathbb{Z})^\times \simeq (\mathbb{Z}/13\mathbb{Z})^\times \times (\mathbb{Z}/31\mathbb{Z})^\times \simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}.$$

5. On peut aussi retrouver ce résultat directement. Le normalisateur $N_G(S)$ agit sur S par conjuguaison, ce qui donne lieu à

$$\psi : N_G(S) \to \mathrm{Aut}(S) \simeq \mathbb{Z}/4\mathbb{Z}.$$

Comme d'une part $|\mathrm{Im}\,\psi|$ divise $|\mathbb{Z}/4\mathbb{Z}| = 4$ et d'autre part $|\mathrm{Im}\,\psi| = |N_G(S)| / |\ker\psi|$ qui divise $|G|$, $|\mathrm{Im}\,\psi|$ divise $\mathrm{pgcd}(4, 2015) = 1$. Donc l'action $N_G(S) \rightsquigarrow S$ par conjuguaison est triviale, autrement dit $S \subset Z(N_G(S))$.

Soit donc $\varphi \in \mathrm{Hom}\,(\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z})$. Notons π_{12} et π_{30} les projections respectives du produit sur $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/30\mathbb{Z}$. Alors

$$\pi_{12} \circ \varphi \in \mathrm{Hom}\,(\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}) \simeq \{0\}\,.$$

Donc l'image de φ est contenue dans $\{0\} \times \mathbb{Z}/30\mathbb{Z}$; d'autre part

$$\pi_{30} \circ \varphi \in \mathrm{Hom}\,(\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/30\mathbb{Z}) \simeq \mathbb{Z}/5\mathbb{Z}$$

Il y a donc a priori 5 tels φ possibles ; cependants tous ceux qui sont non nuls ne diffèrent que d'un automorphisme au départ, et donnent lieu à des produits semi-directs isomorphes d'après le lemme 4.3.

4.3 Groupes d'ordre 2014

C'est un peu plus difficile. 2014 se factorise sous la forme

$$2014 = 2 \times 19 \times 53.$$

Théorème 4.5. *Il existe exactement quatre classes d'isomorphisme de groupes d'ordre* 2014*, à savoir : le groupe cyclique* $\mathbb{Z}/2014\mathbb{Z}$*, le groupe dihédral* D_{2014} *et deux produits semi-directs non directs non isomorphes entre eux et non isomorphes à* D_{2014}*, de la forme :*

$$G_{53} = (\mathbb{Z}/19\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/53\mathbb{Z}, \text{ ou}$$

$$G_{19} = (\mathbb{Z}/53\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/19\mathbb{Z}.$$

Soit G d'ordre 2014 et D un 2-Sylow ; D est central dans son normalisateur, puisque d'ordre 2, en vertu du lemme 3.5, et d'après le théorème de Burnside il admet un complément normal N d'ordre 1007. Comme $1007 = 19 \times 53$ et $19 \nmid 53$, N est cyclique. La principale difficulté consiste ici à distinguer les produits semi-directs $N \rtimes D$. Nous avons

$$\mathrm{Aut}\,(N) \simeq \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/52\mathbb{Z}.$$

Soit $\varphi \in \mathrm{Hom}\,(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/52\mathbb{Z})$. Alors (avec les mêmes notations que dans la section précédente et le lemme 4.2)

$$\pi_{18} \circ \varphi \in \mathrm{Hom}\,(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/18\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}, \text{ et}$$

$$\pi_{52} \circ \varphi \in \mathrm{Hom}\,(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/52\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

On trouve donc, au plus 4 groupes d'ordre 2014, dont 3 non abéliens. Si $\pi_{18} \circ \varphi\,(1)$ et $\pi_{52} \circ \varphi\,(1)$ sont non nuls, $\varphi\,(1)$ est le morphisme d'inversion $\iota : N \to N$ et $N \rtimes_{\varphi} D$ est le groupe dihédral D_{2014}, soit le groupe des isométries d'un polygone à 1007 côtés. D_{2014} n'a pas de sous-groupe abélien d'ordre pair strictement plus grand que 2 : un tel sous-groupe contiendrait un élément d'ordre 2, donc une symétrie s, dont le commutant dans D_{2014} est réduit à $\{1, s\}$.

Par contre, G_{53} et G_{19} ont des sous-groupes abéliens « rectangles » (produits de sous-groupes), d'ordre respectifs 106 et 38. Donc ils ne sont pas isomorphes à D_{2014}. Il reste à voir qu'ils ne sont pas isomorphes entre eux.

D'après les théorèmes de Sylow, le nombre de 53-Sylow de G_{53} est congru à 1 modulo 53 et divise 38 ; G_{53} possède donc un unique 53-Sylow. De plus, comme

par définition $G_{53} \simeq G' \times \mathbb{Z}/53\mathbb{Z}$, le 53-Sylow de G_{53} est central. De même, le 19-Sylow de G_{19} est central. Si donc $G_{53} \simeq G_{19}$ alors leur centre serait d'ordre au moins 19×53, donc 1007 ou 2014. En fait, 1007 est exclu puisqu'alors on aurait $G_{19}/Z(G_{19}) \simeq \mathbb{Z}/2\mathbb{Z}$, ce qui est impossible (le quotient par le centre est trivial dès qu'il est monogène). Le cas où le centre est d'ordre 2014 est aussi exclu puisque G_{19} et G_{53} sont non abéliens. Donc G_{19} et G_{53} sont bien non isomorphes, ce qui termine la classification des groupes d'ordre 2014.

5 Epilogue (2017)

Inexorablement, l'année 2016 est arrivée, et il a fallu se résoudre à l'évidence : les groupes d'ordre 2016 sont très nombreux, trop nombreux. Ceci notamment parce que 32 divise le nouveau venu, et déverse un formidable réservoir de 2-Sylow dans les groupes d'ordre 2016. Il était temps de s'adresser aux spécialistes. La SmallGroup Library du projet GAP, d'accès un peu retiré, mais agréablement intégrée au moteur de recherche Wolfram Alpha (Posez-lui la question « *How many groups of order 2016 are there ?* ») nous indique qu'il existe 6538 groupes d'ordre 2016. Parmi eux figure un invité d'honneur, le groupe classique $\mathrm{GL}(2, \mathbf{F}_7)$, un intime du groupe simple d'ordre $168 = 2016/12$. Au delà, les groupes d'ordre inférieur ou égal à 2047 sont repertoriés (la plupart [6] sont d'ordre 1024), ce qui nous laisse encore, à l'heure où j'écris ces lignes, un peu de répit avant la survenue du prochain multiple de 32.

Note *Complément à la bibliographie d'une republication de [3] parue en 2016, considérablement augmentée (le transfert est toujours au chapitre 7).*

Références

[1] Gaëtan Chenevier, *Théorie algébrique des nombres*, cours de M1 à l'Ecole polytechnique, 2013.

[2] Daniel Perrin, *Cours d'Algèbre*, Ellipses, 1996 — issu d'un polycopié de l'ENSJF vers 1980.

[3] Jean-Pierre Serre, *Groupes finis* — issu d'un polycopié de cours de l'ENSJF 1978-1979. Republié sous le titre *Finite Groups : An introduction*, International Press Volume : 100, 2016.

[4] Jean-Pierre Serre, *Cours d'arithmétique*, PUF, 1970 — issu des « cours au carrés » à l'ENS vers 1965-1970.

6. D'un point de vue strictement comptable, on peut défendre que la plupart des groupes finis sont des 2-groupes (donc en particulier nilpotents).