Cours de théorie des groupes

20019-2020

Pierre Mounoud

3 septembre 2021

Chapitre 1

Bibliographie

Voici une liste de livres de théorie des groupes, il y aura une autre liste pour la partie théorie de Galois. J'ai mis quelques commentaires pour vous guider.

— Josette Calais ; *Éléments de théorie des groupes*, PUF
(référence classique, un peu ancienne école peut-être)
— Daniel Guin, Thomas Hausberger ; *Algèbre Tome 1. Groupes, corps et théorie de Galois*, EDP Sciences.
(contenu du livre proche du programme de l'UE, contient une partie exercices sur machine)
— Daniel Perrin ; *Cours d'algèbre*, Ellipses.
(référence classique souvent utilisé pour préparer l'agrégation, ne couvre qu'une partie du programme)
— Jean-Pierre Serre ; *Groupes finis, Cours à l'École Normale Supérieure de Jeunes Filles 1978/79*, trouvable sur ArXiv sous la référence : math.GR/0503154
(utile pour les parties théorème de Sylow et groupes résolubles)
— Jean Delcourt ; *Théorie des groupes*, Dunod.
(livre d'exercices corrigés, je ne le connais pas bien, lire des corrigés d'exercices est, à mon avis, une perte de temps)
— Felix Ulmer ; *Théorie des groupes*, Ellipses.
(assez court, ressemble à un poly de cours)
— Joseph Rotman ; *An introduction to the theory of groups*, Graduate Texts in Math
(très différent des autres livres, complet, limite intimidant, pour étudiants en master ou thèse voire chercheurs, ses 5 premiers chapitres couvrent l'essentiel du cours)
— John Meier ; *Groups, graphs and trees*, London Math. Soc. Student Text
(aussi très différent des autres, Rotman compris, ton peu scolaire, colle aussi très (très) peu au programme de l'UE, mais contient plein de jolies maths)

Chapitre 2

Groupes et actions de groupes

Cette section reprend le cours de L2 de théorie des groupes et suppose que le lecteur connaît déjà en partie le sujet. Pour plus de détails on pourra se reporter à son cours de licence ou à son livre de théorie des groupes préféré.

1 Définitions de base

Définition 1.1 *Un ensemble G muni d'une loi de composition interne $\star$ satisfaisant :*

1) (associativité) $\forall x, y, z \in G,\ x \star (y \star z) = (x \star y) \star z$,

2) (existence du neutre) $\exists e \in G, \forall x \in G,\ x \star e = e \star x = x$,

3) (existence inverse) $\forall x \in G, \exists y \in G,\ x \star y = y \star x = e$,

s'appelle un groupe.

Un groupe n'est jamais vide. Un groupe possède un unique élément neutre et tout élément un unique inverse (possiblement lui-même).
Le groupe G est dit commutatif ou abelien si la loi $\star$ est commutative. On appelle ordre d'un groupe son nombre d'éléments (noté $|G|$). Un groupe est dit fini si son ordre est fini.

Notation En général, on notera xy le produit de x et de y, x^{-1} l'inverse de x et 1 l'élément neutre du groupe. C'est la notation multiplicative. Parfois, si le groupe est abélien, on utilisera la notation additive ie on notera $+$ la loi, $-x$ l'inverse de x et 0 le neutre.

Exemples : $(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $\mathrm{Sym}(X)$ le groupe symétrique sur un ensemble X i.e. l'ensemble des bijections de X dans X muni de la loi $\circ$ c'est l'exemple essentiel.

Définition 1.2 *Un sous-groupe de $(G, \star)$ est une partie de G telle $(H, \star)$ est un groupe (la loi est la même). On note $H \leq G$.*

En pratique, $H \subset G$ est un sous-groupe ssi $H \neq \emptyset$ et $(x, y) \in H \Rightarrow xy^{-1} \in H$.
L'ensemble des mouvements d'un *rubik's cube* est un sous-groupe (d'ordre $8!3^7 12!2^{10}$) du groupe symétrique sur les facettes. Le groupe linéaire noté $\mathrm{GL}(V)$ d'un k-espace vectoriel V (consitué des automorphismes d'espace vectoriel de V) est un sous-groupe du groupe symétrique de V. Il a lui-même plein de sous-groupes intéressants (qui préservent ceci ou cela).

Propriété 1.3 [1] *Soit G un groupe. Toute intersection de sous-groupes de G est un sous-groupe de G.*

Définition 1.4 *Soit S une partie d'un groupe G. Le* sous-groupe engendré *par S est le plus petit sous-groupe de G contenant S, c'est l'intersection de tous les sous-groupes contenant S. On le note $\langle S \rangle$.*

1. vous devez savoir montrer rapidement ce qui est indiqué comme *propriété* et non démontré

Si $\langle S\rangle = G$ on dit que S est une partie génératrice *de G.*
Un groupe G est dit monogène *s'il est engendré par un élément et* cyclique *s'il est de plus fini.*
L'ordre d'un élément $x \in G$ (noté $\mathrm{ord}(x)$*) est l'ordre du groupe $\langle x\rangle$.*

Propriété 1.5 *Soit $\in G$,*

$$\mathrm{ord}(x) < \infty \Rightarrow \mathrm{ord}(x) = \min\{k \geq 1, x^k = 1\}.$$

Définition 1.6 *Soient G et H deux groupes. Une application $\Phi : G \to H$ est un morphisme de groupes si*

$$\forall x, y \in G,\ \Phi(xy) = \Phi(x)\Phi(y)$$

Nécessairement, $\Phi(1) = 1$, $\Phi(x^{-1}) = \Phi(x)^{-1}$ et $\mathrm{ord}(\Phi(x))$ divise $\mathrm{ord}(x)$ (ainsi il n'existe pas de morphisme de groupes non constant de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$). Un morphisme de groupes est entièrement déterminé par l'image d'une partie génératrice.

Propriété 1.7 *Si $\Phi : G \to H$ est un morphisme de groupes alors*

1) *l'image directe d'un sous-groupe de G est un sous-groupe de H, en particulier* $\mathrm{Im}\,\Phi = \{\Phi(g), g \in G\}$ *est un sous-groupe de H ;*
2) *l'image réciproque d'un sous-groupe de H est un sous-groupe de G, en particulier* $\ker\Phi = \{g \in G;\ \Phi(g) = 1\}$ *est un sous-groupe de G ;*
3) *Φ est injective si et seulement si* $\ker\Phi = \{1\}$ *(ou si on préfère $\Phi(x) = \Phi(y)$ si et seulement si $xy^{-1} \in \ker\Phi$) ;*
4) *si Φ est bijective alors Φ^{-1} est un morphisme de groupes.*

On peut préciser un peu :

Proposition 1.8 *Si $\Phi : G \to H$ est un morphisme de groupes alors Φ induit une bijection entre les sous-groupes de* $\mathrm{Im}\,\Phi$ *et les sous-groupes de G contenant* $\ker\Phi$.

Preuve On a vu que Φ et Φ^{-1} induisent bien des applications entre nos deux ensembles. Voyons qu'elles sont réciproques l'une de l'autre. Il faut donc vérifier que si $H \leq G$, H contenant $\ker\Phi$ alors $\Phi^{-1}(\Phi(H)) = H$ et que si $L \leq \mathrm{Im}\,\Phi$ alors $\Phi(\Phi^{-1}(L)) = L$.

On a toujours $\Phi^{-1}(\Phi(H)) \supset H$. Réciproquement, si $x \in \Phi^{-1}(\Phi(H))$ alors il existe $h \in H$ tel que $\Phi(x) = \Phi(h)$. On a donc $xh^{-1} \in \ker\Phi \subset H$ et donc $x = (xh^{-1})h \in H$.

On a toujours $\Phi(\Phi^{-1}(L)) = L \cap \mathrm{Im}\,\Phi$. D'où l'égalité cherchée. □

Définition 1.9 *Un morphisme de groupes $\Phi : G \to H$ bijectif est appelé un isomorphisme (de groupes). Si de plus $G = H$, on dit que Φ est un automorphisme,* $(\mathrm{Aut(G)}, \circ)$ *est un groupe.*

Il est clair qu'un morphisme Φ d'un groupe monogène $G = \langle x\rangle$ dans lui-même est un automorphisme ssi $G = \langle\Phi(x)\rangle$. On en déduit les groupes d'automorphismes des groupes monogènes.

Propriété 1.10

$$\mathrm{Aut}(\mathbb{Z}, +) = \{\pm\mathrm{id}\}; \qquad \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}, +) = \{x \mapsto kx;\ 1 \leq k \leq n, k \wedge n = 1\} \simeq (\mathbb{Z}/n\mathbb{Z})^\times$$

2 Classes modulo un sous-groupe

Soit G un groupe et $H \leq G$. Soit $\mathcal{R}_H$ la relation sur G par $x\mathcal{R}_H y$ si $x^{-1}y \in H$

Propriété 2.1 1) *La relation $\mathcal{R}_H$ est une relation d'équivalence (ie reflexive, symétrique et transitive). C'est la relation d'équivalence à gauche modulo H.*
2) *La classe d'équivalence d'un élément $a \in G$ est $aH = \{ah;\ h \in H\}$. On l'appelle la classe à gauche de a modulo H.*

Comme toujours les classes d'équivalences forment *une partition* de G. On note $G/_H$ l'ensemble des classes à gauche de G modulo H .

On définit de même la relation d'équivalence à droite modulo H (par $x\mathcal{R}'_H y$ si $xy^{-1} \in H$). La classe à droite de a est$Ha = \{ha;\ h \in H\}$. On note ${}_H\backslash G$ l'ensemble des classes à droite [2].

Il est clair que $a\mathcal{R}_H b$ si et seulement si $a^{-1}\mathcal{R}'_H b^{-1}$. Par conséquent l'application $aH \mapsto Ha^{-1}$ est une bijection de $G/_H$ dans ${}_H\backslash G$. Ces deux ensembles ont donc même cardinal, noté $(G : H)$ et appelé l'indice de H dans G.

Propriété 2.2 *L'application $H \to aH$ (resp. $H \mapsto Ha$) définie par $h \mapsto ah$ (resp. $h \mapsto ha$) est une bijection.*

On a donc une partition de G en classes de cardinal $|H|$. Lorsque G est fini on en déduit :

Théorème 2.3 (théorème de Lagrange) *Si G est un groupe fini et H un sous-groupe de G, alors*

$$|G| = |H|(G : H).$$

L'ordre et l'indice d'un sous-groupe H sont des diviseurs de l'ordre de G. En particulier l'ordre d'un élément divise l'ordre du groupe.

Avertissement : À tout diviseur de $|G|$ ne correspond pas forcément un sous-groupe. Par exemple A_4 (d'ordre 12) ne contient pas de sous-groupes d'ordre 6. Comme souvent dans le monde des groupes cycliques les choses sont beaucoup plus simple.

Propriété 2.4 *Si k est un diviseur de n alors il existe un unique sous-groupe d'ordre k dans $\mathbb{Z}/n\mathbb{Z}$.*

Le théorème de Lagrange implique par exemple qu'il n'existe pas de morphisme de groupes non constants de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ si n et m sont premiers entre eux.

2.1 Sous-groupes distingués, groupes quotient

Définition 2.5 *On dit que H est distingué dans G si*

$$\forall g \in G, gHg^{-1} \subset H,$$

c'est-à-dire si $\forall g \in G, \forall h \in H$, $ghg^{-1} \in H$, ou, de façon équivalente,

$$\forall g \in G, gH \subset Hg.$$

On note $H \triangleleft G$.

Si $H \triangleleft G$ les inclusions ci-dessus sont des égaliltés et $G/_H = {}_H\backslash G$ (c.-à-d. $aH = Ha$ pour tout $a \in G$).

Proposition 2.6 *Soit $H \leq G$. Le sous-groupe H est distingué dans G si et seulement s'il existe une structure de groupe sur G/H telle que la surjection canonique $\pi : G \to G/H$ (qui a x associe xH) est un morphisme de groupes. Cette structure est alors unique.*

Bout de preuve : La condition $H \triangleleft G$ assure que l'application $G/H \times G/H \to G/H$, $(aH, bH) \mapsto abH$ est bien définie (c'est-à-dire ne dépend du choix d'un élément (ici a) dans aH). En effet, si a et b sont dans G et si h et h' sont dans H, alors il existe $h'' \in H$ tel que $ahbh' = abb^{-1}hbh' = abh''$ car $H \triangleleft G$. Le reste marche tout seul. □

Exemples : Le noyau d'un morphisme $\Phi : G \to H$ est distingué (ce qui prouve "la réciproque" dans la proposition ci-dessus) : soit $g \in G$ et $x \in \ker \Phi$, pour savoir si $gxg^{-1} \in \ker \Phi$ on lui applique Φ :

$$\Phi(gxg^{-1}) = \Phi(g)\Phi(x)\Phi(g)^{-1} = 1,$$

2. on note par un quotient à gauche les classes à droite et par un quotient à droite les classes à gauche

donc $gxg^{-1} \in \ker \Phi$. Ainsi $\mathrm{SL}(n,k) \lhd \mathrm{GL}(n,k)$, $A_n \lhd S_n$.

Tout sous-groupe d'un groupe abélien est distingué.

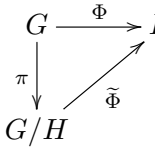
Tout sous-groupe d'indice 2 est distingué (TD). En fait, tout sous-groupe d'indice le plus petit diviseur premier de G est distingué.

Mise en garde La relation « être distingué dans » n'est pas transitive. Par exemple, dans S_4, $\{1,(1,2)(3,4)\} \lhd \langle (1,2)(3,4),(1,3)(2,4)\rangle$ et $\langle (1,2)(3,4),(1,3)(2,4)\rangle \lhd S_4$ MAIS $\{1,(1,2)(3,4)\}$ n'est pas distingué dans S_4.

Propriété 2.7 – *Soient X et Y deux sous-groupes de G. On définit $XY := \{xy;\, x \in X, Y \in Y\}$. L'ensemble XY est un sous-groupe ssi $XY = YX$. Ainsi si $X \lhd G$ alors XY est un sous-groupe de G.*
– L'image directe (resp . l'image réciproque) d'un sous-groupe distingué par un morphisme de groupes $\Phi : G \to H$ est un sous-groupe distingué de $\mathrm{Im}\,\Phi$ (resp. de G qui contient $\ker \Phi$) .
Le morphisme Φ induit une bijection entre l'ensemble des sous-groupes distingués de $\mathrm{Im}\,\Phi$ et ceux de G qui contiennent $\ker \Phi$.

On fera attention qu'un sous-groupe distingué de $\mathrm{Im}\,\Phi$ n'est pas en général un sous groupe distingué de H.
Résultat important :

Théorème 2.8 (1er théorème d'isomorphisme) *Soient $\Phi : G \to K$ un morphisme de groupes et H un sous-groupe distingué de G. Si $H \leq \ker \Phi$ alors il existe un unique morphisme de groupes $\widetilde{\Phi} : G/H \to K$ tel que $\Phi = \widetilde{\Phi} \circ \pi$, où $\pi : G \to G/H$ est la surjection canonique.*
En d'autre termes le diagramme



est commutatif.
En particulier, (pour $H = \ker \Phi$), on voit que Φ induit un isomorphisme entre $G/\ker \Phi$ et $\mathrm{Im}\Phi$.

Preuve en cours. . .□

Ce théorème fait penser au théorème du rang d'algèbre linéaire. Ce dernier peut être vue comme une conséquence de notre théorème.

Pour apprivoiser un théorème, on peut commencer par tester sur les exemples que l'on maîtrise le mieux. On va dire les groupes cycliques. Si $d \in \mathbb{N}$ divise n, alors $n\mathbb{Z} \lhd d\mathbb{Z}$ et on peut former $d\mathbb{Z}/n\mathbb{Z}$. On prend $\Phi = \pi \circ \alpha$, où $\alpha : \mathbb{Z} \to d\mathbb{Z}$ est la multiplication par d et $\pi : d\mathbb{Z} \to d\mathbb{Z}/n\mathbb{Z}$ est la projection canonique. Clairement Φ est surjective et $\ker \Phi = (n/d)\mathbb{Z}$. Le théorème nous dit que $\mathbb{Z}/(n/d)\mathbb{Z}$ est isomorphe à $d\mathbb{Z}/n\mathbb{Z}$.

Une application classique du théorème 2.8. On rappelle qu'un automorphisme intérieur d'un groupe G est une application de la forme $\Phi_g : x \mapsto gxg^{-1}$. On vérifie facilement qu'il s'agit bien d'automorphismes et que l'application de G dans $\mathrm{Aut}(G)$ qui à g associe Φ_g est un morphisme. Son noyau est $Z(G)$, le centre de G, l'ensemble des éléments qui commutent avec tout G. On a donc immédiatement :

Proposition 2.9 *Soit G un groupe. Le* groupe des automorphismes intérieurs de G, *noté $Int(G)$ est isomorphe à $G/Z(G)$.*

Il existe un 2eme et 3eme théorème d'isomorphisme qui sont pour l'essentiel des applications du 1er et dont la preuve sera vue en TD.

Théorème 2.10 (2eme théorème d'isomorphisme) *Soient $H \leq G$, $N \lhd G$. Alors $N \cap H \lhd H$ et $H/N \cap H$ est isomorphe à HN/N.*

Illustration : Prenons $G = \mathbb{Z}$, $H = n\mathbb{Z}$ et $N = m\mathbb{Z}$, on sait que $n\mathbb{Z} \cap m\mathbb{Z} = \text{ppcm}(n,m)\mathbb{Z}$ et que $n\mathbb{Z} + m\mathbb{Z} = \text{pgcd}(n,m)\mathbb{Z}$. Le 2eme théorème d'isomorphisme dit que $n\mathbb{Z}/\text{ppcm}(n,m)\mathbb{Z}$ est isomorphe à $\text{pgcd}(n,m)\mathbb{Z}/m\mathbb{Z}$. On vient de montrer que le premier est isomorphe à $\mathbb{Z}/(\text{ppcm}(n,m)/n)\mathbb{Z}$ et que le deuxième à $\mathbb{Z}/(m/\text{pgcd}(n,m))\mathbb{Z}$. On a donc une preuve compliquée de $nm = \text{ppcm}(n,m)\text{pgcd}(n,m)$.

Si les groupes sont finis, on déduit de ce théorème que $|H||N| = |HN||H \cap N|$.

Théorème 2.11 (3eme théorème d'isomorphisme) *Soient H et K deux sous-groupes distingués de G. Si $K \leq H$ alors $H/K \triangleleft G/K$ et $(G/K)/(H/K)$ est isomorphe à G/H.*

On peut continuer notre jeux. On prend d qui divise n. Le théorème nous dit que $(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$ (ce qu'on pouvait facilement deviner vu que $|d\mathbb{Z}/n\mathbb{Z}| = n/d$ et que le groupe quotient est clairement monogène).

3 Action de groupes

Soient G un groupe et X un ensemble. Faire agir G sur X c'est grosso-modo voir G comme un sous-groupe de $\text{Sym}(X)$.

Définition 3.1 – *Une action de G sur X est la donnée d'une application*

$$G \times X \to X, (g,x) \mapsto g \cdot x$$

vérifiant :

i) $\forall g,h \in G, \forall x \in X,\ g \cdot (h \cdot x) = (gh) \cdot x$

ii) $\forall x \in X, 1 \cdot x = x$

– *De façon équivalente une action de G sur X est la donnée d'un morphisme $\Phi : G \to \text{Sym}(X)$.*

Pour construire Φ à partir d'une action de G sur X, on pose $\Phi(g) : X \to X$ définie par $\Phi(g)(x) = g \cdot x$. On vérifie que $\Phi(g)$ est bien une bijection et que Φ ainsi définie est bien un morphisme. Le lien réciproque se fait de même.

Exemples : – Un sous-groupe H de G agit sur G par translation à gauche en posant $h \cdot g = hg$ ou à droite en posant $h \cdot g = gh^{-1}$ (eh oui !) ;
– un groupe G agit sur lui-même par conjugaison, ie en posant $g \cdot x = gxg^{-1}$, où g et x sont dans G ;
– un groupe G agit sur l'ensemble $\mathcal{G}$ de ses sous-groupes par conjugaison, $g \cdot H = gHg^{-1}$;
– si $H \leq G$, le groupe G agit sur G/H (qui n'est pas forcément un groupe) par $g \cdot xH = gxH$;
– La géométrie du triangle est l'étude des invariant de l'action du groupe des isométries du plan sur celui des triplets de points du plan (cf. définition d'une géométrie due à F. Klein).

Vocabulaire : On dit qu'une action est *fidèle* si le morphisme Φ associé est injectif c.-à-d. si $g \in G$ vérifie $g \cdot x = x$ pour tout x alors $g = 1$.

Ainsi l'action de G sur lui-même par translation est fidèle, ce qui montre :

Théorème 3.2 (Thm de Cayley) *Si G est fini de cardinal n, G est isomorphe à un sous-groupe de S_n (et donc à un sous-groupe de $\text{GL}(n,k)$, quel que soit le corps k) .*

Propriété 3.3 *La relation binaire sur X : $x \sim y$ si $\exists g \in G, g \cdot x = y$ est une relation d'équivalence.*

Ses classes d'équivalences sont les *orbites* de l'action : $\text{Orb}(x) = \{g.x;\ g \in G\}$. *Les orbites forment donc une partition de X.*

Ce n'est pas un hasard si cela rappelle les classes modulo un sous-groupe. Si $H \leq G$, pour l'action définie par $(h,x) \in H \times G, h \cdot x = hx$ (resp. gx^{-1}) on a $\text{Orb}(x) = Hx$ (resp. $= xH$).

Vocabulaire : On dit qu'une action G sur X est *transitive* si tous les points de X sont dans une même orbite, c.-à-d. si $\forall x,y \in X, \exists g \in G, g \cdot x = y$.

L'action de G sur G/H vue plus haut est transitive (en fait toute action transitive est en fin de compte de cette forme là).

Définition 3.4 *Le stabilisateur de $x \in X$ est le sous-groupe de G défini par*

$$\mathrm{Stab}(x) = \{g \in G;\ g.x = x\}.$$

Voir une partie de G comme le stabilisateur d'un élément pour une certaine action montre que cette partie est un sous-groupe de G.

Lorsqu'un groupe agit sur lui-même par conjugaison, le stabilisateur d'un élément est appelé son *centralisateur*. On note $C(x)$ le centralisateur de $x \in G$, $C(x) = \{g \in G |\, gxg^{-1} = x\}$.

Si on considère l'action de G sur ses sous-groupes, le stabilisateur d'un sous-groupe H et appelé son *normalisateur* c'est $N_G(H) = \{g \in G |\, gHg^{-1} = H\}$. Il contient tout sous-groupe K tel que $H \triangleleft K$ et $H \triangleleft G$ ssi $N_G(H) = G$ (i.e. les sous-groupes distingués sont les points fixes de l'action).

On peut maintenant faire agir le sous-groupe $N_G(H)$ sur H par conjugaison. Le morphisme Φ associé à cette action est à valeurs dans $\mathrm{Aut}(H) \leq \mathrm{Sym}(H)$ (a priori l'image de Φ ne contient pas que des automorphismes intérieurs).

Proposition 3.5 *Si $y \in \mathrm{Orb}(x)$ alors $\mathrm{Stab}(x)$ et $\mathrm{Stab}(y)$ sont conjugués. De plus, l'application $\Phi_x : G \to \mathrm{Orb}(x)$, $g \mapsto g.x$ passe au quotient en une bijection $G/\mathrm{Stab}(x) \to \mathrm{Orb}(x)$.*

Preuve Si $y \in \mathrm{Orb}(x)$ alors il existe $g_0 \in G$ tel que $y = g_0 \cdot x$. Dès lors, il est clair que $g \cdot y = y$ implique $(g_0^{-1} g g_0) \cdot x = x$ ce qui donne $g_0 \mathrm{Stab}(y) g_0^{-1} \subset \mathrm{Stab}(x)$. L'inclusion réciproque est obtenue en permutant les rôles de x et y.

Pour le deuxieme point on commence par remarquer que pour tout $g, g' \in G$ on a $g \cdot x = g' \cdot x$ ssi $g^{-1}g' \in \mathrm{Stab}(x)$. Autrement dit deux éléments de G ont même image par Φ_x ssi ils sont dans la même classe modulo à gauche $\mathrm{Stab}(x)$. Par conséquent, Φ_x passe au quotient en une application *injective* $G/\mathrm{Stab}(x) \to \mathrm{Orb}(x)$. Cette application est aussi surjective car Φ_x l'est. □

Application Si X est fini et $x_1, \ldots, x_k$ sont des représentants des orbites de l'action de G (fini lui aussi) sur X (donc k est le nombre d'orbite) alors

$$|X| = \sum_{i=1}^{k} |\mathrm{Orb}(x_i)| = \sum_{i=1}^{k} \frac{|G|}{|\mathrm{Stab}(x_i)|} \qquad (\star).$$

On reconnait là une généralisation du théorème de Lagrange. Par exemple, en faisant agir G (fini) sur lui-même par conjugaison, on obtient (cf. chapitre 4) :

$$|G| = |Z(G)| + \sum_{i=1}^{k} \frac{|G|}{|C(x_i)|},$$

où $Z(G)$ est le centre de G ie l'ensemble des éléments qui commutent avec tout le monde ie (bis) l'ensemble des éléments dont le centralisateur est G, ie (ter) l'ensemble des éléments dont l'orbite est de cardinal 1.

Montrer qu'un sous-groupe d'indice 2 est toujours distingué est élémentaire. Cela s'étend grâce à la formule $(\star)$ en :

Proposition 3.6 *Soit H un sous-groupe de G d'indice p. Si p est le plus petit diviseur premier de $|G|$ alors $H \triangleleft G$.*

On montre aussi que le nombre moyen de points fixes d'une action est ègal au nombre d'orbites.

Proposition 3.7 (formule de Burnside) *Soient G un groupe fini agissant sur un ensemble X fini. Pour tout $g \in G$, on note $\mathrm{fix}(g) = \{x \in X;\ g.x = x\}$. Alors*

$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{fix}(g)| = |\{\text{orbites de } X\}|$$

Ces deux propositions seront montrées en TD.

4 Produit semi-direct

4.1 Construction interne

Définition 4.1 *Soit G un groupe, H et N des sous-groupes de G. Si*

i) $N \triangleleft G$

ii) $N \cap H = \{1\}$

iii) $NH = G$

alors on dit que G est le produit semi-direct de ses sous-groupes N et H, on note $G = N \rtimes H$.

Avertissement Un sous-groupe distingué ne possède pas toujours de "supplémentaire", cf. le groupe des quaternions $H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ muni de la loi vérifiant $(-1)^2 = 1$, $i^2 = j^2 = k^2 = ijk = -1$ (tous les sous-groupes d'ordre 4 contiennent le seul sous-groupe d'ordre 2).

Analyse
Si G est le produit semi-direct de N et H alors

$$\forall g \in G, \exists!(n,h) \in N \times H, g = nh,$$

l'unicité vient de ii). De fait, le 2eme théorème d'isomorphisme dit $G/N \simeq H$ et donc $|G| = |N||H|$. Comment s'écrit la loi de G dans cette décomposition [3] ?
Si $g = nh$ et $g' = n'h'$, alors

$$gg' = nhn'h' = \underbrace{n(hn'h^{-1})}_{\in N}\underbrace{hh'}_{\in H}$$

Formalisons un peu :
Pour tout $h \in H$, on note Φ_h l'application de N dans lui-même définie par $\Phi_h(n) = hnh^{-1}$. On voit que $\Phi_h \in \mathrm{Aut}(N)$ (c'est un automorphisme intérieur).
Mieux l'application $\Phi : H \to \mathrm{Aut}(N)$, $h \mapsto \Phi_h$ est un morphisme de groupe. On peut écrire

$$(nh)(n'h') = n\Phi_h(n')hh'.$$

Étant donné deux groupes N et H, cette analyse nous dit comment faire pour construire les groupes G tels que $G = N \rtimes H \ldots$

4.2 Construction externe

On se donne deux groupes N et H et un morphisme $\Phi : H \to \mathrm{Aut}(N), h \mapsto \Phi_h$. On définit une loi interne sur l'ensemble $N \times H$ par

$$(n,h)(n',h') = (n\Phi_h(n'), hh').$$

Proposition 4.2 *L'ensemble $N \times H$ muni de la loi ci-dessus est un groupe. Ce groupe est le produit semi-direct (externe) de N et H relativement à Φ, il est noté $N \rtimes_\Phi H$.*

Preuve : On peut vérifier que le neutre est $(1_N, 1_H)$ et l'inverse de (n,h) est $(\Phi_{h^{-1}}(n^{-1}), h^{-1})$. Il reste à vérifier l'associativité. Soient (n_i, h_i), $i = 1,2,3$ des éléments de $N \times H$. On a

$$\begin{aligned}(n_1,h_1)((n_2,h_2)(n_3,h_3)) &= (n_1,h_1)(n_2\,\Phi_{h_2}(n_3), h_2h_3) = (n_1\,\Phi_{h_1}(n_2\,\Phi_{h_2}(n_3)), h_1h_2h_3)\\ &= (n_1\Phi_{h_1}(n_2)\,\Phi_{(h_1h_2)}(n_3)), (h_1h_2)h_3) = ((n_1,h_1)(n_2,h_2))(n_3,h_3) \quad \square\end{aligned}$$

Remarques :
– $N' = N \times \{1_H\}$ est un sous-groupe distingué de $N \rtimes_\Phi H$
– $H' = \{1_N\} \times H$ est un sous-groupe de $N \rtimes_\Phi H$
– $H' \cap N' = \{(1_N, 1_H)\}$
– $N'H' = N \rtimes_\Phi H$ et donc $N \rtimes_\Phi H$ est le produit semi-direct interne de N' et H'. Le morphisme de H' dans $\mathrm{Aut}(N')$ associé (si on identifie N à N' et H à H') est Φ.

3. on fait bien attention à mettre N à gauche sinon c'est un peu plus compliqué à écrire

Proposition 4.3 *Les éléments de N' commutent à ceux de H' ssi Φ est trivial (on obtient alors le produit direct de N et H noté $N \times H$). Cela vient du fait que $H' \triangleleft (N \rtimes_\Phi H)$ ssi Φ est trivial.*

Exemples : Groupes diedraux $\mathbb{Z}/n\mathbb{Z} \rtimes_\Phi \mathbb{Z}/2\mathbb{Z}$ avec $\Phi_1(k) = -k$, A_4 en TD.

Chapitre 3

Présentation par générateurs et relations

1 Un nouveau groupe (ou presque)

Soit X un ensemble non vide (fini ou non) et soit $\widehat{X} = \{\hat{x} | x \in X\}$ une autre copie de X. Il est conseillé dans un premier temps de se limiter au cas où $X = \{a, b\}$.

Étape 1

Pour tout $n \in \mathbb{N}$, on considère W_n l'ensemble des mots de longueur n dans l'alphabet $X \cup \widehat{X}$ ie l'ensemble des $n-$uplets d'éléments de $X \cup \widehat{X}$. On remarque que W_0 ne contient que le mot vide qu'on notera e. On retire des W_n les mots contenant une paire $x, \hat{x}$ (pour le même x) en position adjacente (côte à côte dans un sens ou dans l'autre). Les mots restant sont dits *réduits*. On désigne par $\widetilde{W}_n$ l'ensemble des mots réduits de longueur n.

Enfin on pose

$$F_X = \bigcup_{n \in \mathbb{N}} \widetilde{W}_n,$$

F comme *free*.

Étape 2

On définit une loi binéaire sur F_X de la façon suivante : étant donnés

$$a = (a_1, \ldots, a_k) \in \widetilde{W}_k \quad \text{et} \quad b = (b_1, \ldots, b_\ell) \in \widetilde{W}_\ell,$$

on pose

$$a \cdot b = (a_1, \ldots, a_{k-r}, b_{r+1}, \ldots, b_\ell),$$

où r est le plus grand des entiers $j \geq 0$ tels que aucun des $(a_k, b_1), (a_{k-1}, b_2) \ldots, (a_{k-j+1}, b_j)$ n'est réduit (on voit les $\hat{x}$ comme les inverses de x et on simplifie) [1]. Il est clair que $a \cdot b$ est réduit (possiblement vide).

On voudrait vérifier que cette loi fait de F_X un groupe. On a bien un neutre, c'est le mot vide e, chaque élément a un inverse :

$$(a_1, \ldots, a_k)^{-1} = (\hat{a}_k, \ldots, \hat{a}_1),$$

en posant $\hat{\hat{x}} = x$ pour tout $x \in X$.

Il ne reste plus qu'à montrer que cette loi est bien associative pour avoir un groupe. Hélas la vérification directe est pénible. On remet cette question à plus tard.

Pour finir (pour des raisons esthétiques) on enlève les parenthèses et les virgules (on note les mots comme des mots non plus comme des n-uplets et on écrit x^{-1} au lieu de $\hat{x}$. Avec cette convention on voit que tout élément de F_X s'écrit de manière unique $x_1^{\epsilon_1} \ldots x_k^{\epsilon_k}$, avec $k \in \mathbb{N}$ (variable), $\epsilon_j = \pm 1$, $x_1, \ldots, x_k \in X$, tels que $x_j^{\epsilon_j} \neq x_{j+1}^{-\epsilon_{j+1}}$, e étant obtenu pour $k = 0$.
Pour éviter les confusions on notera encore "$\cdot$" la loi de F_X.

1. on peut aussi définir r comme plus petit entier tel que $(a_1, \ldots, a_{k-r}, b_{r+1}, \ldots, b_\ell)$ est réduit

2 Une propriété universelle

Définition 2.1 *Soit F un groupe et X une partie de F. On dit que F est libre de base X si pour tout groupe G et toute application de $f : X \to G$ il existe un* unique *morphisme $\Phi : F \to G$ étendant f (ie tel que $\Phi|_X = f$).*

On pourra remarquer que les bases des espaces vectoriels possèdent une propriété similaire.

Théorème 2.2 *L'ensemble F_X muni de la loi donnée plus haut est un groupe libre de base X.*

Preuve : Pour éviter d'avoir à montrer directement l'associativité de la loi précédemment construite, on utilise *l'astuce de van der Waerden* qui envoie F_X dans le groupe symétrique sur F_X.

Pour tout $x \in X$, on définit les fonctions $|x| : F_X \to F_X$ et $|x^{-1}| : F_X \to F_X$ par, avec $\epsilon = \pm 1$,

$$|x^\epsilon|(x_1^{\epsilon_1} \dots x_k^{\epsilon_k}) = \begin{cases} x^\epsilon x_1^{\epsilon_1} \dots x_k^{\epsilon_k} & \text{si } x^\epsilon \neq x_1^{-\epsilon_1} \\ x_2^{\epsilon_2} \dots x_k^{\epsilon_k} & \text{si } x^\epsilon = x_1^{-\epsilon_1} \end{cases}$$

Il s'agit clairement de deux bijections, réciproques l'une de l'autre, ie d'éléments du groupe symétrique sur F_X, que l'on notera S_F.

On note $\mathcal{F}$ le sous-groupe de S_F engendré par $[X] = \{|x|, x \in X\}$. Tout élément $g \in \mathcal{F}$ s'écrit $g = |x_1^{\epsilon_1}| \circ \dots \circ |x_k^{\epsilon_k}|$ avec $x_i \in X$ et $\epsilon_i = \pm 1$, de plus on peut supposer qu'un $|x^\epsilon|$ et un $|x^{-\epsilon}|$ ne sont jamais adjacents, sinon on les simplifie. L'écriture obtenue est alors unique, vu que $g(e) = x_1^{\epsilon_1} \cdots x_k^{\epsilon_k}$.

On voit donc que l'application $\zeta : \mathcal{F} \to F_X$ donnée par $g \mapsto g(e)$ est bijective et vérifie $\zeta(g \circ f) = \zeta(g) \cdot \zeta(f)$ (le point correspondant ici à la multiplication dans F_X). On en déduit que F_X est un groupe et ζ un isomorphisme de groupes.

Montrons que F_X est libre de base X. Soit G un groupe et $f : X \to G$ une fonction. Comme tout élément de F_X s'écrit de manière unique $x_1^{\epsilon_1} \dots x_k^{\epsilon_k}$, $x_j^{\epsilon_j} \neq x_{j+1}^{-\epsilon_{j+1}}$, l'application Φ donnée par $\Phi(x_1^{\epsilon_1} \dots x_k^{\epsilon_k}) = f(x_1)^{\epsilon_1} \dots f(x_k)^{\epsilon_k}$ est bien définie.

L'application Φ est un morphisme de groupes. Soient v et w dans F_X (des mots réduits donc). Si le mot wv (obtenu en juxtaposant les 2 mots) est lui aussi réduit ie si $w \cdot v = wv$ et donc il est évident que $\Phi(w \cdot v) = \Phi(w)\Phi(v)$. Dans la cas général il existe des mots réduits w', v' et u tels que $w = w' \cdot u$ et $v = u^{-1} \cdot v'$ et tels que $w \cdot v = w'v'$. On a alors

$$\Phi(w)\Phi(v) = \Phi(w')\Phi(u)\Phi(u^{-1})\Phi(v') = \Phi(w')\Phi(v') = \Phi(w'v') = \Phi(w \cdot v).$$

Il s'agit donc bien d'un morphisme.

Si Φ' est un autre morphisme qui étend f alors Φ et Φ' coïncident sur X et comme X engendre F_X, forcément $\Phi = \Phi'$. D'où l'unicité de l'extension. □

Proposition 2.3 *Soient F_1 et F_2 deux groupes libres de bases respectivement X_1 et X_2. Les groupes F_1 et F_2 sont isomorphes si et seulement si X_1 et X_2 ont même cardinal. En particulier, toutes les bases d'un groupe libre ont même cardinal.*

Preuve dans le cas où les X_i sont au plus dénombrables (ou les F_i c'est pareil) :
Si $F_1 \simeq F_2$ alors $|\mathrm{Hom}(F_1, \mathbb{Z}/2\mathbb{Z})| = |\mathrm{Hom}(F_2, \mathbb{Z}/2\mathbb{Z})|$. D'après la propriété universelle il y a autant de morphisme de F_i dans $\mathbb{Z}/2\mathbb{Z}$ que d'application de X_i dans $\mathbb{Z}/2\mathbb{Z}$. Or le nombre d'application de X_i dans $\mathbb{Z}/2\mathbb{Z}$ est égal au nombre de parties de X_i, c'est-à-dire $2^{|X_i|}$. On en déduit que X_1 et X_2 ont même cardinal. [2]

Réciproquement, X_1 et X_2 ont même cardinal alors il existe une bijection $\kappa : X_1 \to X_2$. Nos groupes étant libres, il existe un unique morphisme de groupe F_1 dans F_2, noté α, étendant κ et un unique morphisme de groupe β de F_2 dans F_1 étendant κ^{-1}. La restriction de $\alpha \circ \beta$ à X_2 est l'identité et donc par unicité des extensions $\alpha \circ \beta = \mathrm{id}_{F_2}$ et de même $\beta \circ \alpha = \mathrm{id}_{F_1}$. □

2. c'est là qu'on utilise notre hypothèse de dénombrabilité

On parle donc **du** groupe libre de base X, le cardinal de X est appelé le rang du groupe. On notera F_k le groupe libre de rang k (on se limitera à $k \leq \aleph_0$).

L'importance des groupes libres vient notamment du théorème suivant :

Théorème 2.4 *Tout groupe est isomorphe à un quotient d'un groupe libre.*

Preuve : Soit G un groupe et S une partie génératrice de G. L'inclusion de S dans G se prolonge en un morphisme surjectif de F_S dans G. Le 1er théorème d'isomorphisme finit le travail.

Ce théorème permet de montrer qu'il existe une infinité de groupes à 2 générateurs (cf. [Meier]).

Avertissement : Le rang des groupes libres se comporte très mal. Ainsi F_2 possède un sous-groupe isomorphe à F_3 (et donc de tout rang $k \in \mathbb{N}$ et en fait il en existe même de rang $\aleph_0$).

Exercice : Pour tout $w \in F_j$ on note $\ell(w)$ la longueur de w càd le nombre de lettres du mot réduit donnant w (ie $\ell(x_1^{n_1} \dots x_k^{n_k}) = |n_1| + \dots + |n_k|$ si $x_i \neq x_{i+1}$ quel que soit i) .

1) Soit f le morphisme de groupe de $F_{\{a,b\}}$ dans $\mathbb{Z}/2\mathbb{Z}$ tel que $f(a) = f(b) = 1$. Montrer que $w \in \ker(f)$ ssi $\ell(w)$ est pair. Montrer que $\ker(f) = \langle a^2, b^2, ab \rangle$.
2) Soit g le morphisme de $F_{\{x,y,z\}}$ dans $F_{\{a,b\}}$ qui envoie x sur a^2, y sur b^2 et z sur ab. Montrer que pour tout $w \in F_{\{x,y,z\}}$, $\ell(g(w)) \geq \ell(w)$ (on montrera que l'image d'un mot réduit ne peut pas trop se simplifier). En déduire que $\langle a^2, b^2, ab \rangle \simeq F_3$.

Il est cependant vrai que tout sous-groupe d'un groupe libre est libre, c'est le théorème de Nielsen-Schreier (qui n'est pas facile à montrer).

3 Présentation par générateurs et relations

Une fois qu'on s'est donné un ensemble de générateurs d'un groupe G, une relation entre ces générateurs est un mot réduit (en tant que mot) qui est égal à 1 dans G. Par exemple, un groupe cyclique d'ordre n a un générateur x qui vérifie la relation $x^n = 1$. Clairement il est inutile de se donner toutes les relations pour décrire complètement le groupe.

Définition 3.1 *Si S est une partie d'un groupe G, le sous-groupe normal de G engendré par S, qu'on notera (S), est l'intersection de tous les sous-groupes normaux de G contenant S. Si $S = \emptyset$, on pose $(S) = \{1\}$, où 1 est l'élément neutre de G.*

Définition 3.2 *Soit X un ensemble et R une partie de F_X le groupe libre de base X. On dit que $\langle X \,|\, R \rangle$ est une présentation d'un groupe G par générateurs et relations si G est isomorphe au groupe $F_X/(R)$, où (R) est le sous-groupe normal de F_X engendré par R.*

Exemples : $\langle \{x\} \,|\, x^n \rangle$ est une présentation de $\mathbb{Z}/n\mathbb{Z}$ (dans la pratique on écrit plutôt $\langle x \,|\, x^n \rangle$.
$\langle x, y \,|\, xyx^{-1}y^{-1} \rangle$ est une présentation de $\mathbb{Z}^2$.
Souvent, on cherche X et R les plus petits possible. Par exemple, $\langle a, b |\, a^2, b^3, aba^{-1}b^{-1} \rangle \simeq \mathbb{Z}/6\mathbb{Z}$ ne semble pas être une bonne présentation.

Proposition 3.3 *Soient $G = \langle X|R \rangle$ et G' un groupe. Pour définir un morphisme de groupes $f : G \to G'$, il suffit de définir $f(x)$ pour $x \in X$ et de vérifier que, pour tout $r \in R$, $f(r) = 1_{G'}$.*

Par contre il est souvent très difficile de vérifier si un tel morphisme est injectif. Pour les groupes finis on contourne souvent cette difficulté avec des arguments de cardinalité.

Exercice : Montrer que $\langle a, b \,|\, a^4, b^2, abab \rangle$ est une présentation du groupe diédral D_4.

Chapitre 4

Théorèmes de Sylow

Définition 0.1 *Soit p un nombre premier (dans tout le chapitre p désignera un nombre premier). Un p-groupe est un groupe fini de cardinal une puissance de p.*

Les p-groupes jouent un rôle important dans la compréhension des groupes finis.

Lemme 0.2 *Soit X un ensemble fini sur lequel opère un p-groupe P et soit X^P l'ensemble des éléments de X fixés par P . Alors $|X| \equiv |X^P| \mod p$.*

Preuve On se donne un ensemble T de représentants de chaque orbite (ie tq tout élément de G est dans l'orbite d'un unique élément de T). On a donc

$$X = \coprod_{x \in T} \mathrm{Orb}(x).$$

Un élément $x \in X$ est dans X^P ssi $\mathrm{Orb}(x) = \{x\}$, d'où : $|X| = |X^P| + \sum_{x \in T \setminus X^P} |\mathrm{Orb}(x)|$. Or le cardinal d'une orbite divise l'ordre du groupe, d'où p divise le cardinal de $\mathrm{Orb}(x)$ pour tout $x \in T \setminus X^P$. D'où $|X| \equiv |X^P| \mod p$.□

Proposition 0.3 *Le centre d'un p-groupe n'est pas trivial. Il contient toujours un élément d'ordre p.*

Preuve On fait agir G sur lui-même par conjugaison. On a $G^G = Z(G)$ et d'après le lemme 0.2

$$0 \equiv |G| \equiv |Z(G)| \mod p.$$

Soit $x \in Z(G)$, $x \neq 1$. L'ordre de x est p^a avec $a \geq 1$ et donc $x^{p^{a-1}} \in Z(G)$ est d'ordre p.□

On verra en TD que cela implique :

Corollaire 0.4 *Un groupe d'ordre p^a possède des sous-groupes d'ordre p^b pour tout $0 \leq b \leq a$.*

Définition 0.5 *Soit p un nombre premier et G un groupe d'ordre $p^a m$ avec $p \wedge m = 1$. Un sous-groupe de G d'ordre p^a s'appelle un p-sous-groupe de Sylow (ou p-Sylow) de G.*

Remarque : si p n'est pas un diviseur de $|G|$ alors $\{1\}$ est un p-Sylow de G.

Exemple : Soit H le sous-groupe de $G = \mathrm{GL}(n, F_p)$ composé des matrices triangulaires supérieures avec des 1 sur la diagonale. Il est clair que $|H| = p\,p^2 \dots p^{n-1} = p^{n(n-1)/2}$. Comme (cf. TD)

$$|\mathrm{GL}(n, F_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1}) = p\,p^2 \dots p^{n-1}[(p^n - 1)(p^{n-1} - 1) \dots (p - 1)]$$

et que $(p^n - 1)(p^{n-1} - 1) \dots (p - 1) \equiv (-1)^n \mod p \not\equiv 0 \mod p$, on voit H est un $p-$Sylow de G. Cet exemple nous permet de montrer le premier théorème de Sylow.

Théorème 0.6 *Tout groupe fini possède au moins un p-Sylow.*

Preuve : On a vu que tout groupe fini peut etre vu comme un sous-groupe de $\mathrm{GL}(n, F_p)$. Le théorème se déduit de l'exemple ci-dessus et du lemme suivant :

Lemme 0.7 *Si G a des p-Sylow et si H est un sous-groupe de G, alors H a aussi des p-Sylow. Plus précisément, si S est un p-Sylow de G alors il existe $g \in G$ tel que $H \cap gSg^{-1}$ est un p-Sylow de H.*

Preuve du lemme Le groupe G opère sur G/S par translation à gauche et le stabilisateur de aS est aSa^{-1}. Mais H opère lui aussi sur G/S par restriction, avec comme stabilisateur de aS, $aSa^{-1} \cap H$.

Il reste à. voir que l'un de ces groupes est un p-Sylow de H. Ce sont déjà des p-groupes et il suffit donc que, pour un $a \in G$, $|H/(aSa^{-1} \cap H|$ soit premier à p.

Mais $|H/(aSa^{-1} \cap H|$ est le cardinal de l'orbite de aS dans G/S sous l'action de H. Si tous ces nombres étaient divisibles par p, il en serait de même de $(G : S) = |G/S|$. Mais ceci contredit le fait que S est un p-Sylow de G. □

Corollaire 0.8 *Soit G un groupe fini et $a \geq 0$ tel que p^a divise $|G|$. Alors il existe un sous-groupe de G d'ordre p^a. En particulier, si p divise $|G|$ alors G possède un élément d'ordre p (thm de Cauchy).*

Le deuxième théorème de Sylow étudie la conjugaison des p-Sylow.

Théorème 0.9 *Soit G un groupe, de cardinal $|G| = p^a m$, avec $p \wedge m = 1$.*

1) Si H est un sous-groupe de G qui est un p-groupe, il existe un p-Sylow S, avec $H \subset S$;

2) Les p-Sylow sont tous conjugués ;

3) On a $n_p \equiv 1 \mod p$ (donc n_p divise m).

Corollaire 0.10 *Soit S un p-Sylow de G. On a $n_p |N_G(S)| = |G|$ et donc notamment*

$$S \triangleleft G \Leftrightarrow S \text{ est l'unique } p-\text{Sylow de } G \Leftrightarrow n_p = 1$$

Preuve : Les points 1 et 2 sont des conséquences directes du lemme 0.7 ci-dessus (details en cours)

Pour le point 3), on fait opérer G par conjugaison sur l'ensemble X de ses p-Sylow. Soit S un p-Sylow, S opère lui aussi sur X.

Si T est un point fixe de cette action, c'est-à-dire si S normalise T, on considère alors N le sous-groupe de G engendré par $S \cup T$. Comme S normalise T, on a $T \triangleleft N$. Or T est un p-Sylow de N et donc T est l'unique p-Sylow de N et $S = T$.

On conclut avec le lemme 0.2 que $n_p = |X| = |G/N_G(S)| \equiv 1 \mod p$. □

Exemples d'utilisation des théorèmes de Sylow

— Un groupe d'ordre 63 n'est jamais simple. On a $63 = 3^2.7$. On a donc n_7 divise 9 et $n_7 \equiv 1 \mod 7$ donc $n_7 = 1$!

— Un groupe G d'ordre 300 non plus. On a $300 = 2^2.3.5^2$, d'où $n_5 = 1$ ou 6. Si G est simple alors $n_5 = 6$ et l'action de G sur l'ensemble de ses 6-Sylow induit un morphisme injectif (car non trivial et G simple) dans S_6. Or 300 ne divise pas $6! = 720$! !

— Soit G un groupe d'ordre pq (nombres premiers distincts $p < q$). On a $n_q = 1$ (sinon $n_q > q > p$). Il n'existe qu'un q-Sylow, H, et $H \triangleleft G$. Soit K un q-Sylow. On a forcément $H \cap K = \{1\}$ et $G = HK$ et donc $G = H \rtimes K$. Qu'en est-il de n_p ?

On sait que n_p divise que q et que $n_p \equiv 1 \mod p$. On en déduit que $n_p = 1$ ou p divise $q - 1$.

Si p ne divise pas $q-1$, on a donc K distingué lui-aussi. Par conséquent $[h, k] = 1, \forall (h, k) \in H \times K$ et

$$G \simeq \mathbb{Z}/pZ \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}.$$

Si p divise $q-1$, sachant que $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$, il existe un morphisme de groupe non trivial de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ et donc des produits semi-directs non abéliens (on peut montrer qu'à isomorphisme près il existe un unique groupe non abélien d'ordre pq dans ce cas).

Terminons avec quelques propriétés supplémentaires des p-Sylow.

Proposition 0.11 *1) Soit H un sous-groupe normal de G et soit S un p-Sylow de G. Alors $S \cap H$ est un p-Sylow de H et SH/H, l'image de S dans G/H, est un p-Sylow de G/H (et on les obtient tous ainsi)*

2) Soit S un p-Sylow de G. Si $N_G(S) \leq K \leq G$ alors $N_G(K) = K$ (en particulier $N_G(N_G(S)) = N_G(S)$).

Preuve : Pour tout $g \in G$, $|S \cap H| = |g(S \cap H)g^{-1}| = |gSg^{-1} \cap gHg^{-1}| = |gSg^{-1} \cap H|$ (H distingué). Les p-Sylow étant tous conjugués, cela signifie que $|S \cap H|$ ne dépend pas du choix du p-Sylow S. Le lemme 0.7 implique donc $S \cap H$ est un p-Sylow de H.

L'ordre de S divise l'ordre de SH et donc $(G : SH)$ est premier à p. Or,

$$(G/H : SH/H) = \frac{|G/H|}{|SH/H|} = \frac{\frac{|G|}{|H|}}{\frac{|SH|}{|H|}} = (G : SH).$$

De plus, SH/H est un p-groupe (il est d'ordre $|S|/|S \cap H|$), il s'agit donc d'un p-Sylow de G/H. Soit R un p-Sylow de G/H et K son image réciproque par la projection canonique, $(G : K) = (G/H, R = K/H)$ est premier avec p. Soit S un p-Sylow de K, S étant aussi un p-Sylow de G son image dans G/H est un p-Sylow de G/H (on vient de la montrer) contenu dans R, elle est forcément ègale à R (et $K = SH$).

Pour tout $x \in N_G(K)$, on a $xSx^{-1} \leq K$ vu que $S \leq K$. C'est encore un p-Sylow de K. Or les p-Sylow de K sont K-conjugués, i.e. il existe $h \in K$ tel que $xSx^{-1} = hSh^{-1}$. Par conséquent $xh^{-1} \in N_G(S) \leq K$. Comme $h \in K$, on a $x \in K$. L'autre inclusion est évidente.□

Chapitre 5

Groupes symétriques

1 Rappels rapides

Soit $n \geq 1$ un entier, on note S_n le groupe des permutations de $\{1, \ldots, n\}$ c'est à dire l'ensemble des bijection de $\{1, \ldots n\}$ dans lui-même muni de l'opération $\circ$. Il est bien connu que $|S_n| = n!$.

Définition 1.1 *Soit $\sigma \in S_n$. La signature de σ noté $\epsilon(\sigma)$ est l'élément de $\{\pm 1\}$ défini par*

$$\epsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Proposition 1.2 *La signature est un morphisme de groupes surjectif de S_n dans $(\{\pm 1\}, \times)$. On note A_n son noyau (le groupe alterné), $A_n \lhd S_n$ et $|A_n| = n!/2$.*

Preuve : Soient σ et σ' dans S_n. On a

$$\begin{aligned} \epsilon(\sigma\sigma') &= \prod_{1<j} \frac{\sigma\sigma'(i) - \sigma\sigma'(j)}{\sigma'(i) - \sigma'(j)} \frac{\sigma'(i) - \sigma'(j)}{i - j} \\ &= \epsilon(\sigma)\epsilon(\sigma') \end{aligned}$$ □

Définition 1.3 *1) Soit $\sigma \in S_n$. L'ensemble $\{i \in \{1, \ldots, n\} \,|\, \sigma(i) \neq i\}$ est appelé le support de σ.*

2) Une permutation σ est un k-cycle, s'il existe des éléments $a_1, \ldots a_k$ distincts tels que σ envoie chaque élément a_i sur a_{i+1}, a_k sur a_1 et que le support de σ est égal à $\{a_1, \ldots, a_k\}$. On le note $(a_1, \ldots, a_k)$.
Un 2-cycle est appelé une transposition.

Propriété 1.4 *Toute permutation s'écrit comme un produit de cycles à supports disjoints. Cette décomposition est unique à permutation des facteurs près (deux cycles à supports disjoints commutent).*

Cette décomposition correspond à la partition de $\{1, \ldots, n\}$ en orbites sous l'action de $\langle\sigma\rangle$. La signature d'un k-cycle est -1^{k-1}.

2 Engendrement et conjugaisons

En remarquant que $(a_1, \ldots, a_k) = (a_1, a_2)(a_2, a_3) \ldots (a_k, a_{k-1})$, on montre facilement que :

Proposition 2.1 *Le groupe S_n est engendré par $\{(i, j), i < j\}$.*

On peut faire beaucoup mieux :
– $S_n = \langle (1,i), 2 \leq i \leq n \rangle$
– $S_n = \langle (i,i+1), 1 \leq i \leq n-1 \rangle$
– $S_n = \langle (1,2), (1,2,\ldots,n) \rangle$.

Proposition 2.2 *Pour $n \geq 3$, le groupe A_n est engendré par les 3-cycles*

Preuve Les éléments de A_n s'écrivent comme le produit d'un nombre pair de transpositions. Or

$$(a,b)(c,d) = (a,b)(a,c)(a,c)(c,d) = (a,c,b)(a,c,d).$$

Proposition 2.3 *1) Pour tout $\sigma \in S_n$ et tous $a_1, \ldots a_k$ distincts, on a*

$$\sigma(a_1, \ldots, \ldots a_k)\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k))$$

2) Dans S_n tous les cycles d 'ordre k sont conjugués entre eux.

3) Si $n \geq 5$ les cycles d'ordres 3 sont conjugués dans A_n.

Dans 1) la transformation est « la même » seul le nom des éléments de $\{1, \ldots, n\}$ a changé (cf. Perrin p.16). On déduit de 2) que la classe de conjugaison d'une permutation est déterminée par la suite des cardinaux des supports des cycles disjoints qui la compose.. . .

Preuve : 1) clair

2) On prend σ qui envoie a_i sur i et on applique 1)

3) On montre que si $k \leq n-2$ alors $(a_1, \ldots, a_k)$ est conjugué à $(1, \ldots, k)$ par un élément de A_n. D'après 2), il existe σ tel que $\sigma(a_1, \ldots, \ldots a_k)\sigma^{-1} = (1, \ldots, k)$ si $\sigma \in A_n$ on a fini sinon on reconjugue par $(n-1, n)$.□

Corollaire 2.4 *Si $n \geq 3$ alors $Z(S_n) = \{1\}$*

Preuve Soit $\sigma \neq 1$. Il existe i tel que $j = \sigma(i) \neq j$. Comme $n \geq 3$, il existe k différents de i et j. On pose $\tau = (j,k)$ et on remarque $\tau\sigma\tau^{-1}(i) = k$ et donc $\tau\sigma\tau^{-1} \neq \sigma$ et $\sigma \notin Z(S_n)$.□

3 Structure

Le théorème principal de cette section est le suivant :

Théorème 3.1 *Si $n \geq 5$ alors le groupe A_n est simple.*

Remarque : On a déjà vu que A_4 n'est pas simple (il s'écrit comme le produit semi-direct du sous-groupe des produits de transpo à supports disjoints par un sous-groupe engendré par un 3-cycle). $|A_3| = 3 \ldots$

On va commencer par montrer le cas $n = 5$ et voir ensuite commence se ramener à ce cas.

3.1 Preuve de la simplicité de A_5.

Le groupe A_5 a 60 éléments : le neutre, 15 éléments d'ordre 2 (produit de deux transpositions disjointes), 20 d'ordre 3 (3-cycles), 24 d'ordre 5 (5-cycles).

On a vu que les cycles d'ordre 3 sont conjugués dans A_5. Les éléments d'ordre 2 le sont aussi : si $\sigma = (ab)(cd)(e)$ et $\sigma' = (a'b')(c'd')(e')$ il existe $\tau \in A_5$, tel que $\tau(a) = a'$, $\tau(b) = b'$, $\tau(e) = e'$ et on a alors $\sigma' = \tau\sigma\tau^{-1}$. Les éléments d'ordre 5 ne sont pas tous conjugués (impossible vu que 24 ne divise pas 60) mais les 5-Sylow le sont.

Soit $H \lhd A_5$. Étant invariant par conjugaison, si H contient un élément d'ordre 3 (resp. 4 / 5) il les contient tous. Mais ni 16, ni 21, ni 25 ne divise 60. Donc si $H \neq \{1\}$, il contient au moins deux types de permutations et donc au moins 36 éléments. Donc $|H| = 60$ et $H = A_5$.

3.2 Preuve pour $n > 5$

Soit $H \neq \{1\}$ distingué dans A_n. On va commencer par trouver un élément de H ayant $n-5$ points fixes. Pour cela on considère un commutateur $[\tau, \sigma]$ avec $\tau \in A_n$ avec un maximum de points fixes (ie $n-3$) et $\sigma \in H$. On a alors $[\tau, \sigma] \in H$ car $H \lhd A_n$ et $[\tau, \sigma] = \tau(\sigma\tau^{-1}\sigma^{-1})$ a beaucoup de points fixes (à la louche deux fois moins que τ c'est encore beaucoup).

On met en forme :
Soit $\sigma \neq 1 \in H$ et $a \in \{1, \ldots, n\}$ tel que $b = \sigma(a) \neq a$. Bien sûr, on choisit pour τ un 3-cycle de sorte que $\rho = [\tau, \sigma] \neq 1$ et $[\tau, \sigma]$ laisse fixe $n-5$ points. Pour cela on prend $\tau = (a, c, b)$ où $c \neq a, c, \sigma(b)$. On a donc $\rho = (a, b, c)(\sigma(a), \sigma(b), \sigma(c))$. Comme $b = \sigma(a)$, l'ensemble $F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ a au plus 5 éléments et $\rho(F) = F$, $\rho|_{E-F} = \mathrm{Id}_{E-F}$
On note que ρ est distinct de 1, car $\rho(b) = \tau\sigma(b) \neq b$ puisque $\sigma(b) \neq \tau^{-1}(b) = c$. Enfin quitte à rajouter des éléments à F, on peut supposer $|F| = 5$.

Soit alors $A(F)$ l'ensemble des permutations paires de F, $A(F)$ est un sous-groupe de A_n isomorphe à A_5. Le sous-groupe $H_0 = H \cap A(F)$ est distingué dans $A(F)$. Comme $A(F) \simeq A_5$ est simple et $H_0 \neq \{1\}$, on a $H_0 = A(F)$. Par conséquent H_0 contient un 3-cycle et donc H les contient tous. Ceux-ci engendrent A_n et donc $H = A_n$. □

Corollaire 3.2 *Si $n \geq 5$, les sous-groupes distingués de S_n sont $\{1\}$, A_n et S_n.*

Preuve Soit $H \lhd S_n$. Comme $H \cap A_n \lhd A_n$ et que $(S_n : A_n) = 2$, on a $A_n \leq H$ ou $|H| \leq 2$ (1er ou 2eme thm d'isom.). Tout sous-groupe distingué d'ordre 2 est contenu dans le centre. Or celui est trivial.

Corollaire 3.3 *Tout sous-groupe G de S_n d'indice n est isomorphe à S_{n-1}.*

Preuve : Soit $\Phi : S_n \to \mathrm{Sym}(S_n/G) \simeq S_n$ l'action habituelle. On commence par remarquer que le sous-groupe de $\mathrm{Sym}(S_n/G)$ laissant fixe un point (par exemple G) est isomorphe à S_{n-1}. Le stabilisateur de $G \in S_n/G$ est égal à G (vu que $g \cdot G = G$ ssi $g \in G$) et donc $\Phi(G)$ est contenu dans un sous-groupe isomorphe à S_{n-1}. Pour conclure il suffit de voir que Φ est injectif. L'action est transitive donc le noyau de Φ est d'indice au moins n. Ce qui implique qu'il est trivial par le corollaire 3.2. □

Chapitre 6

Groupes résolubles

Les groupes résolubles forment une famille de groupes « plus abéliens » que la moyenne (les groupes nilpotents en forment une encore plus abélienne mais on n'en parlera pas faute de temps). Ils interviennent en théorie de Galois, on le verra plus tard, c'est de là que vient leur nom.

1 Groupe(s) dérivé(s)

Soit G un groupe et $x, y \in G$. On appelle commutateur de x et y l'élément

$$[x, y] := xyx^{-1}y^{-1} \in G.$$

On voit facilement que $xy = [x, y]yx$. Le commutateur mesure le défaut de commutativité de x et y. En particulier x et y commutent ssi $[x, y] = 1$.

Notation Si H et K sont deux sous-groupes de G, on note $[H, K]$ le sous-groupe de G engendré par les $[x, y]$ avec $x \in H$ et $k \in K$.

Définition 1.1 *Le sous-groupe $D(G) = [G, G]$ (noté aussi parfois G') est appelé le groupe dérivé de G :*

$$D(G) = \langle [x, y];\ x, y \in G \rangle.$$

On défini par récurrence le ieme groupe dérivé de G noté $D^i(G)$ par $D^i(G) = [D^{i-1}(G), D^{i-1}G] = D(D^{i-1}G)$ et $D^0(G) = G$.

Proposition 1.2 *1) Le sous-groupe $D(G)$ est invariant par tout automorphisme de G (on dit que $D(G)$ est caractéristique). En particulier $D(G) \triangleleft G$ et même $D^i(G) \triangleleft G$.*

2) Pour tout $H \leq G$ sont équivalents :

(a) H contient $D(G)$,

(b) $H \triangleleft G$ et G/H est abélien.

Preuve : 1) Pour tout automorphisme φ, on a $\varphi([x, y]) = [\varphi(x), \varphi(y)] \in D(G)$.

2) –>

Pour tout $h \in H$ et $g \in G$, $ghg^{-1}h^{-1} \in D(G) \subset H$ donc $ghg^{-1} \in H$. Donc H est distingué.

Pour tout $x, y \in G$, on a (on utilisant pour une fois des classes à droite) :

$$HxHy = Hxy = H[x, y]yx = Hyx = HyHx.$$

<–

Soit $\pi : G \to G/H$ la projection canonique.Pour tout $x, y \in G$

$$\pi([x, y]) = [\pi(x), \pi(y)] = H = 1_{G/H}$$

et donc $D(G) \leq \ker \pi = H$.□

Remarque Si $H \triangleleft G$ et que K est un sous-groupe caractéristique de H alors $K \triangleleft G$.

On a bien sûr $D^iG \triangleleft D^{i-1}(G)$ et même $D^iG \triangleleft G$

Corollaire 1.3 *$G/D(G)$ est le plus grand quotient abélien de G (on l'appelle l'abélianisé de G) dans la mesure où tout quotient abélien de G est isomorphe à un quotient de $G/D(G)$.*

Preuve : Si G/H est abélien alors $D(G) \leq H$ mais alors par le 3eme thm d'isomorphisme $(G/D(G))/(H/D(G)) \simeq G/H$.□

Exemples :
– Si G est simple alors $D(G) = \{1\}$ ou G. Si G est simple et d'ordre non premier alors $D(G) = G$ (et son abélianisé est trivial).

– Dans S_n, $n \geq 3$ tous les 3-cycles sont conjugés. Donc pour tout 3-cycle σ il existe $\rho \in S_n$ tel que $\sigma^2 = \rho\sigma\rho^{-1}$ et donc $\sigma = [\rho, \sigma] \in D(S_n)$. On en déduit $A_n \subset D(S_n)$ (ce qu'on savait déjà pour $n \geq 5$). La signature de tout commutateur est 1 donc $D(S_n) \subset A_n$.

– Soit F_2 est le groupe libre à 2 générateurs. On sait qu'il existe un morphisme de groupe surjectif de F_2 dans $\mathbb{Z}^2$ (vu que $\mathbb{Z}^2$ est engendré par deux éléments). Ainsi $F_2/D(F_2)$ est un groupe abélien à deux générateurs qui possède un quotient isomorphe à $\mathbb{Z}^2$. C'est donc que $F_2/D(F_2) \simeq \mathbb{Z}^2$. On peut montrer que le groupe dérivé de F_2 est un groupe libre avec une infinité (dénombrable) de générateurs mais c'est plus compliqué.

2 Groupes résolubles

Définition 2.1 *Un groupe G est dit résoluble s'il existe un entier $n > 0$ tel que $D^nG = \{1\}$. On appelle alors classe de résolubilité de G et on note* $\mathrm{cl}(G)$ *le plus petit entier n positif pour lequel $D^nG = \{1\}$.*

Ainsi, $\mathrm{cl}(G) = 0$ équivaut à $G = \{1\}$ et $\mathrm{cl}(G) \leq 1$ équivaut à dire que G est abélien. Tout groupe résoluble non trivial contient un sous-groupe abélien normal $\neq \{1\}$, c'est $D^{\mathrm{cl}(G)-1}(G)$.

Un groupe simple non abélien n'est pas résoluble (par exemple les A_n, $n \geq 5$).

Théorème 2.2 *Soit G un groupe.*

1) *Si G est résoluble de classe n alors tout sous-groupe de G est résoluble de classe $\leq n$.*
2) *Si H est un sous-groupe normal de G, alors G est résoluble si et seulement si H et G/H sont résolubles.*
   On a alors $\mathrm{cl}(G) \leq \mathrm{cl}(H) + \mathrm{cl}(G/H)$, $\mathrm{cl}(G) \geq \mathrm{cl}(G/H)$ *et* $\mathrm{cl}(G) \geq \mathrm{cl}(H)$.

Preuve : 1) Pour tout $i \in \mathbb{N}$, on a $D^iH \leq D^iG$. Si $D^nG = \{1\}$ alors $D^nH = \{1\}$.

Lemme 2.3 *Si $\varphi : G \to G'$ est un morphisme de groupes surjectif alors $\varphi(D(G)) = D(G')$.*

Preuve du lemme L'image d'un commutateur est un commutateur d'où une inclusion. Pour l'autre, comme φ est surjective tout commutateur de G' est de la forme $[\varphi(x), \varphi(y)] = \varphi([x, y])$ avec $x, y \in G$. Ce qui montre l'autre inclusion

On déduit par application succésive du lemme ci-dessus que pour tout $i \in \mathbb{N}$, $D^i(G/H) = \pi(D^i(G))$, où π est la projection canonique.

Si G est résoluble, il est maintenant immédiat que G/H l'est aussi.

Supposons H et G/H résolubles. On sait qu'il existe n tel que $\pi(D^nG)$ est trivial ie $D^n(G) \leq H$ et donc il existe k tel que $D^{n+k}(G) = \{1\}$ et donc G est résoluble. □

Applications : – Le produit semi-direct de deux groupes abéliens est résoluble de classe ≤ 2. Ainsi A_4 est résoluble et donc S_4 est résoluble.

– Tout p-groupe est résoluble (par récurrence en utilisant que le centre est non trivial).

– On voit que $G/D^{\mathrm{cl}(G)-1}(G)$ est résoluble de classe $\mathrm{cl}(G) - 1$.

– Le groupe F_k, $k \geq 2$ n'est pas résoluble. Si c'etait le cas, tout groupe à k générateurs serait résoluble d'après le théorème 2.2. Or les S_n, $n \geq 5$ ne sont pas résolubles et sont engendrés par 2 (et donc k) éléments.

Proposition 2.4 *Soit G un groupe et soit n un entier ≥ 1. Les propriétés suivantes sont équivalentes :*

1) G est résoluble de classe $\leq n$,

2) Il existe une suite $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ de sous-groupes normaux de G tels que G_i/G_{i+1} soit abélien pour tout $0 \leq i \leq n-1$,

3) Il existe une suite $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ de sous-groupes de G tels que G_i soit normal dans G_{i-1} et que G_{i-1}/G_i soit abélien, pour tout $1 \leq i \leq n$.

Preuve : (1) $\Rightarrow$ (2) Posons $G_i = D^i(G)$ pour tout $i > 0$. Puisque $D(G)$ est stable par tout automorphisme (même non intérieur !) de G, $D^i(G)$ est normal dans G pour tout i. La suite $(G_i)_{i>0}$ ainsi définie vérifie donc (2).

(2) $\Rightarrow$ (3) est trivial.

(3) $\Rightarrow$ (1) Par récurrence sur k on voit que $D^k G \subset G_k$ pour tout k, d'où $D^n G = \{1\}$. $\square$

Exemple essentiel : Soit K un corps. Le sous-groupe G de $\mathrm{GL}(n, K)$ constitué des matrices triangulaires supérieures (inversibles) est résoluble.

Soit $(e_1, \ldots, e_n)$ la base canonique de K^n. Si on pose $V_i = \mathrm{Vect}\{e_1, e_2, \ldots, e_{n-i}\}$ pour tout $0 \leq i \leq n$, on obtient une famille de sous-espace vectoriel vérifiant $\mathrm{codim}\, V_i = i$ et

$$V = V_0 \supset V_1 \supset \cdots \supset V_n = 0.$$

On a alors $G = \{s \in GL(n, K) |\, sV_i = i, \forall i, 0 \leq i \leq n\}$.
On définit alors une suite de sous-groupes $(B_i)_{0 \leq i \leq n}$ de G par

$$B_i = \{s \in G |\, (s-1)V_j \subset V_{i+j}, 0 \leq j \leq n-i\}.$$

En particulier, $B_0 = G$, B_1 est composé des matrices avec des 1 sur la diagonale, B_2 des matrices ayant des 1 sur la diagonale et des 0 sur la 1ere sur diagonale ..., $B_n = \{id\}$. On vérifie que les B_i sont bien des sous-groupes

Montrons que $[B_j, B_k] \leq B_{\min(j+k,n)}$:

Soient en effet $s \in B_j$, $t \in B_k$ et $x \in V_i$. Il existe $v_{i+k} \in V_{i+k}$ et $w_{i+j} \in V_{i+j}$ (on convient que $V_m = 0$ si $m \geq n$) tels que

$$tx - x = v_{i+k} \quad \text{et} \quad sx - x = w_{i+j}$$

d'où

$$stx = sx + sv_{i+k} = x + w_{i+j} + v_{i+k} + y_{i+j+k}$$

(avec $y_{i+j+k} \in V_{i+j+k}$). De même

$$tsx = t(x + w_{i+j}) = x + v_{i+k} + w_{i+j} + y'_{i+j+k}$$

(avec $y'_{i+j+k} \in V_{i+j+k}$). Donc

$$stx \equiv tsx \mod V_{i+j+k}$$

ou encore

$$s^{-1}t^{-1}st\, x \equiv x \mod V_{i+j+k}$$

d'où le résultat !

En particulier :

• $[B_0, B_i] \subset B_i$ pour $0 \leq i \leq n$, donc les B_i sont normaux dans $B_0 = G$.

• $[B_i, B_i] = D(B_i) \subset B_{2i} \subset B_{i+1}$ pour $1 \leq i \leq n$, donc les quotients B_i/B_{i+1} sont abéliens pour $1 \leq i \leq n-1$.

• Enfin, $B_0/B_1 = G/B_1$ s'identifie au groupe des matrices diagonales (abélien car K est commutatif). Donc la suite $B_0 = G \supset B_1 \supset \cdots \supset B_n = \{1\}$ vérifie la condition (2) et G est résoluble.

Mieux

— Tout groupe d'ordre $p^a q^b$ (où p et q sont premiers) est résoluble (Burnside).

— Le (très difficile : 250 pages de preuve) théorème de Feit-Thompson dit : tout groupe d'ordre impair est résoluble (ou encore : l'ordre d'un groupe simple non abélien est pair).