Introduction à la théorie des groupes : module licence L3 LM325

S. David

Avertissement : il s'agit de la première version préliminaire de ce polycopié. Merci de signaler les erreurs ou imprécisions que vous remarquerez.

1 Premiers concepts

Définition 1.1 *Soit S un ensemble non vide et $\star$ une application :*

$$\star : S \times S \longrightarrow S \ .$$

On dit que $(S, \star)$ possède un élément neutre *s'il existe un élément $e \in S$ tel que :*

$$e \star x = x \star e = x$$

pour tout élément $x \in S$.

Exemples : 0 est un élément neutre pour l'addition usuelle sur $\mathbb{N}$, sur $\mathbb{Z}$. De même, 1 est un élément neutre pour $\mathbb{R}^*$ muni de la multplication usuelle...

Lemme 1.2 *Si $(S, \star)$ est munie d'un élément neutre, alors ce dernier est unique.*

Démonstration : soient en effet e, e' des éléments neutres pour $(S, \star)$. Alors

$$e = e \star e' = e' \ .$$

D'où le lemme. □

Définition 1.3 *Soit S un ensemble non vide et $\star$ une application comme dans la définition 1.1. On dit que $\star$ est* associative *si pour tous $x, y, z \in S$, on a :*

$$(x \star y) \star z = x \star (y \star z) \ .$$

Exemples : l'addition est associative sur $\mathbb{N}, \mathbb{Z}$; la multiplication usuelle est associative sur $\mathbb{R}^\star$.

Définition 1.4 *Soit S un ensemble non vide et $\star$ une application comme dans la définition 1.1 possédant un élément neutre e, et x un élément de S. On dit que x* possède un inverse *pour $\star$ s'il existe un élément $y \in S$ tel que :*

$$x \star y = y \star x = e \ .$$

L'inverse est souvent noté x^{-1}.

Remarque : si x possède un inverse y, alors y possède un inverse : c'est x. En d'autres termes, $(x^{-1})^{-1} = x$.

Lemme 1.5 *Supposons que $(S, \star)$ possède un élément neutre et soit associative; si $x \in S$ possède un inverse, alors ce dernier est unique.*

Démonstration : soient en effet y, y' des inverses pour x. On a :

$$y' = y' \star e = y' \star (x \star y) = (y' \star x) \star y = e \star y = y \ .$$

D'où le lemme 1.5. □

Exemples : dans $(\mathbb{Z}, +)$ ou $(\mathbb{R}^*, \times)$, tout élément possède un inverse. Par contre, dans $(\mathbb{N}, +)$ seul l'élément neutre 0 possède un inverse. On notera que l'élément neutre possède toujours un inverse (lui même).

Définition 1.6 *Soit $(S, \star)$ comme dans la définition 1.1. On dit que la loi $\star$ est* commutative *ou* abélienne *si pour tous éléments $x, y \in S$, on a :*

$$x \star y = y \star x \ .$$

Exemples : tous les exemples ci-dessus définissent une loi commutative. Par contre si l'on considère l'espace $M_n(\mathbb{C})$ des matrices carrées d'ordre n, muni de la multiplication usuelle des matrices, la loi n'est pas abélienne.

Définition 1.7 *Soit G un ensemble non vide muni d'une loi $\star$ comme ci-dessus. On dit que $(G, \star)$ est* un groupe *si la loi possède un élément neutre, est associative et si tout élément x de G possède un inverse.*

Si de plus la loi est commutative, on parle de groupe commutatif *ou de* groupe abélien.

Exemples :

(i) les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de l'addition usuelle sont des groupes abéliens. Il en est de même pour $\mathbb{Q}^*$, $\mathbb{R}^*$ ou $\mathbb{C}^*$ munis de la multiplication usuelle. L'espace $\mathrm{Gl}_n(\mathbb{C})$ des matrices carrées inversibles d'ordre n muni de la multiplication usuelle des matrices est aussi un groupe, mais il n'est pas abélien;

(ii) soit n un entier. Alors le sous-ensemble de $\mathbb{C}$ formé des racines n-ièmes de l'unité muni de la multiplication usuelle est un groupe abélien *fini*. Son cardinal est n.

(iii) Soit S un ensemble non vide, et $(G, \star)$ un groupe. Alors, l'ensemble :

$$G^S := \{\text{applications} \quad S \longrightarrow G\}$$

muni de la loi

$$\begin{array}{rccl} (f\#g) := S & \longrightarrow & G \\ u & \longmapsto & (f\#g)(u) := f(u) \star g(u) \end{array}$$

est un groupe.

Exercice : déterminer l'élément neutre pour $\#$ et l'inverse f^{-1} d'un élément f de G^S.

(iv) Si S est un ensemble non vide,

$$\mathrm{Perm}(S) := \{\text{bijections} \quad S \longrightarrow S\}$$

muni de la composition usuelle des applications est un groupe. Lorsque $S = \{1, \ldots, n\}$, ce groupe est noté $\mathfrak{S}_n$.

(v) Si k est un corps commutatif, et E un k-espace vectoriel, alors l'ensemble $\mathrm{Gl}(E)$ des applications linéaires de $E \longrightarrow E$ muni de la composition usuelle est un groupe.

Exercice : parmi les exemples (iii)–(v) ci-dessus, déterminer les groupes qui sont abéliens.

Convention : pour alléger l'écriture, nous omettrons le plus souvent la mention de la loi (nous dirons par exemple « soit G un groupe ». De même, nous omettrons le plus souvent le symbole $\star$ pour noter plus simplement la loi comme une multiplication usuelle. Lorsque le groupe est abélien, nous noterons également la loi avec le symbole $+$ comme pour l'addition usuelle.

Définition 1.8 *Soit G un groupe et $a \in G$. On appelle* translation à gauche *(respectivement* translation à droite*) par a l'application :*

$$\begin{array}{rccl} \tau_a : G & \longrightarrow & G \\ x & \longmapsto & \tau_a(x) := ax \ . \end{array}$$

Proposition 1.9 *Soit G un groupe et $a \in G$. La translation à gauche (respectivement à droite) par a est une bijection de G dans lui même.*

Démonstration : soient $x, y \in G$. Supposons $ax = ay$. Par multiplication par a^{-1} de chaque côté, on en déduit $x = y$. Donc τ_a est injective. Soit maintenant $y \in G$; posons $x = a^{-1}y$. Alors

$$\tau_a(x) = a(a^{-1}y) = (aa^{-1})y = ey = y \ ;$$

ainsi, τ_a est surjective. □

1.1 Tables de multiplications

Si G est fini, on peut décrire à l'aide d'une *table* de multiplication la loi $\star$. Pour les groupes de petits cardinal, cette description peut suffire à caractériser entièrement le groupe.

En première ligne, sont énumérés les éléments de G, $x_1, \ldots, x_n$, de même qu'en première colonne. la i-ième ligne, j-ième colonne, on place $x_i \star x_j$.

Nous décrivons ci-dessous l'exemple du cardinal 2. Soit donc G un groupe a deux éléments, $\{e, x\}$. On voit facilement que la seule table possible pour un groupe est :

	e	x
e	e	x
x	x	e

De plus, grâce à l'exemple (ii) ci-dessus, on sait qu'il existe un groupe à deux éléments : $\{1, -1\}$ muni de la multiplication usuelle. On en déduit: *à isomorphisme près, il existe un unique groupe ayant deux éléments.*

Exercice : faire toutes les tables de multiplication possibles de groupes pour $\mathrm{Card}(G) \leq 6$. En déduire une classification complète à isomorphisme près des groupes ayant au plus 6 éléments.

1.2 Sous-groupes, morphismes

Définition 1.10 *Soit G un groupe, et H un sous-ensemble non vide de G. On dit que H est un* sous-groupe *de G, si $e \in H$ et si H est stable par multiplication et passage à l'inverse pour la loi. En d'autres termes, si la restricion $\star_{|H\times H}$ de $\star$:*

$$\star_{|H\times H} \ : \ H \times H \longrightarrow G$$

a en fait pour image H et si $(H, \star_{|H\times H})$ est un groupe.

On dispose d'un critère simple pour vérifier que $H \subset G$ est un sous-groupe :

Proposition 1.11 *Soit H un sous-ensemble non vide d'un groupe G. Si pour tous éléments $x, y \in H$, on a*

$$x.y^{-1} \in H \ ,$$

alors H est un sous-groupe de G.

Démonstration : tout d'abord, puisque H est non vide, il existe un élément $x \in H$. Par hypothèse,

$$e = x.x^{-1} \in H \ .$$

Maintenant, si $x \in H$, par hypothèse, $x^{-1} = e.x^{-1} \in H$. Donc H est stable par passage à l'inverse. Soient enfin x, y des éléments de H. Comme $y^{-1} \in H$,

$$xy = x.(y^{-1})^{-1} \in H$$

par hypothèse et donc H est stable par multiplication, d'où la proposition. □

Remarque : par définition, l'associativité est vraie sur tout sous-ensemble de G.

Exemples : $\mathbb{Z}$ est un sous-groupe de $\mathbb{Q}$ qui est un sous-groupe de $\mathbb{R}$ qui est lui même un sous-groupe de $\mathbb{C}$. L'ensemble des racines n-ièmes de l'unité est un sous-groupe de $\mathbb{C}^*$ etc.

Définition 1.12 *Soient H et G deux groupes et $f : H \longrightarrow G$ une application. On dit que f est un* morphisme de groupes *(ou un* homomorphisme*) si pour tous $x, y \in H$,*

$$f(xy) = f(x)f(y) \ .$$

Si $G = H$ on parle d'endomorphisme. *Si f est bijective, on parle* d'isomorphisme.

Lemme 1.13 *Si $f : H \longrightarrow G$ est un morphisme de groupes, $f(e) = f(e')$ où e' est l'élément neutre de G et e celui de H.*

Démonstration : en effet pour tout $x \in H$,

$$f(x) = f(ex) = f(e)f(x) \ .$$

En multipliant chaque terme par $f(x)^{-1}$, on en tire $e' = f(e)$. D'où le lemme. □

Remarque : pour tout $x \in G$, on a

$$f(x^{-1}) = (f(x))^{-1} \ .$$

En effet,

$$e' = f(e) = f(xx^{-1}) = f(x)f(x^{-1}) \ .$$

Donc $f(x^{-1})$ est l'inverse de $f(x)$, *i. e.* c'est $f(x)^{-1}$.

Exemples : l'identité de G dans lui même est un morphisme de groupes. De même, si H est un sous-groupe de G, l'inclusion est un morphisme de groupes. Si $n \geq 1$ est un entier, l'application

$$\begin{array}{rcl} & [n] : G & \longrightarrow \quad G \\ x \longmapsto [n]x & := x^n & \end{array}$$

est-elle un endomorphisme de G?

Exercice : soit G un groupe et $a \in G$. En général, τ_a est-elle un endomorphisme de G? Peut-t-on mettre des conditions sur a pour que τ_a le soit?

Définition 1.14 *Soit $f : G \longrightarrow H$ un morphisme de groupes. Le* noyau *de f est l'ensemble des $x \in G$ tels que $f(x) = e'$. Il est noté* $\ker(f)$.

Lemme 1.15 *Le noyau d'un morphisme de groupes $G \longrightarrow H$ est un sous-groupe de G.*

Démonstration : tout d'abord, le noyau n'est pas vide puisque $e \in \ker(f)$. Si $x, y \in \ker(f)$

$$f(xy^{-1}) = f(x)f(y^{-1}) = e'.e' = e' \ ;$$

donc $xy^{-1} \in \ker(f)$, d'où le lemme. □

Proposition 1.16 *Soit $f : G \longrightarrow H$ un morphisme de groupes. Si* $\ker(f) = \{e\}$*, alors f est injective et réciproquement.*

Démonstration : supposons que f soit injective. Alors, l'image inverse de e' est réduite à un élément (c'est e), *i. e.* $\ker(f) = \{e\}$. Réciproquement, supposons $\ker(f) = \{e\}$ et soient $x, y \in G$ tels que $f(x) = f(y)$. Alors, $f(xy^{-1}) = e'$, *i. e.* $xy^{-1} \in \ker(f)$. Par hypothèse, $xy^{-1} = e$ *i. e.* $x = y$ d'où la proposition. □

Définition 1.17 *Soit $f : G \longrightarrow H$ un morphisme de groupes. L'*image *de f, notée* $\mathrm{Im}(f)$ *est l'ensemble des $y \in H$ tels qu'il existe $x \in G$ avec $y = f(x)$.*

Proposition 1.18 *L'image d'un morphisme de groupes $f : G \longrightarrow H$ est un sous-groupe de H.*

Démonstration : $\mathrm{Im}(f)$ est non vide puisqu'il contient e'. Maintenant, si $u = f(x)$ et $v = f(y)$ sont dans $\mathrm{Im}(f)$, alors :

$$uv^{-1} = f(x)f(y)^{-1} = f(xy^{-1})$$

et par suite, $\mathrm{Im}(f)$ est un sous-groupe de de H par la proposition 1.11. □

Définition 1.19 *Soit S un sous-ensemble d'un groupe G, on note $< S >$ le plus petit sous-groupe de G contenant S; c'est le* sous-groupe engendré par *S.*

Proposition 1.20 *Soit G un groupe et $a \in G$. Alors $< a >= \{a^n, n \in \mathbb{Z}\}$; c'est un groupe abélien.*

Démonstration : tout d'abord, si H est un sous-groupe de G contenant a, il contient forcément toutes ses puissances, et par suite $< a > \supset \{a^n, n \in \mathbb{Z}\}$; inversement, cet ensemble est non vide puisqu'il contient a et si n, m sont dans $\mathbb{Z}$, $a^n a^{-m} = a^{n-m}$ et par suite $\{a^n, n \in \mathbb{Z}\}$ est un sous-groupe de G par la proposition 1.11. Donc $< a >= \{a^n, n \in \mathbb{Z}\}$. Enfin, $a^n.a^m = a^{n+m} = a^m.a^n$ et donc $< a >$ est abélien. □

Définition 1.21 *On dit qu'un groupe G est* monogène *s'il existe un élément a de G tel que $G =< a >$.*

Scolie 1.22 *Tout groupe monogène est abélien.*

Démonstration : cela résulte de la proposition 1.20. □

Définition 1.23 *Soient H, et K deux groupes. Le* produit *direct de H et K est l'ensemble $H \times K$ muni de la loi :*

$$\begin{array}{rcl} \star : (H \times K)^2 & \longrightarrow & H \times K \\ [(a,b);(x,y)] & \longmapsto & (a,b) \star (x,y) := (ax, by) \ . \end{array}$$

Proposition 1.24 *Le produit direct de deux groupes H et K est un groupe.*

Démonstration : laissée en exercice.

Exemples : $\mathbb{Z}^n$, $\mathbb{R}^n$ etc. sont construits à partir de $\mathbb{Z}, \mathbb{R}$... par produit direct des facteurs.

Proposition 1.25 *Soit G un groupe; soient de plus H, K deux sous-groupes de G tels que $H \cap K = \{e\}$, et tels que pour tout $x \in H$ et tout $y \in K$, $xy = yx$. Alors, l'application :*

$$\begin{array}{rcl} \varphi : H \times K & \longrightarrow & G \\ (a,b) & \longmapsto & \varphi(a,b) := ab \end{array}$$

est un morphisme de groupes injectif.

Démonstration : tout d'abord, si $(a,b),(x,y)$ sont des éléments de $H\times K$

$$\varphi((a,b)(x,y))=\varphi(ax,by)=(ax)(by)=(ab)(xy)=\varphi(a,b)\varphi(x,y)$$

car $xb=bx$ par hypothèse. L'application φ est donc un morphisme de groupes. Soit maintenant $(a,b)\in\ker(\varphi)$. On a donc $ab=e$ et donc $b=a^{-1}$. Donc $b\in K$ est également dans H puisque $a^{-1}\in H$. Donc $b=e$ par hypothèse. Il en va de même pour a. □

Remarque : l'hypothèse que H et K commutent est très forte. Toutefois, lorsque G est abélien, elle est automatique. Ici, cet énoncé sera le plus souvent utilisé dans ce cadre.

1.3 Classes à gauche, à droite

Définition 1.26 *Soient G un groupe et H un sous-groupe de G; soient de plus x et y des élements de G. On dit que $x\sim_{\mathrm{g}} y$ si*

$$y^{-1}x\in H\ ;$$

de même, on dit que $x\sim_{\mathrm{d}} y$ si

$$xy^{-1}\in H\ .$$

On dit aussi que x est congru *à y* modulo *H (à gauche, respectivement à droite). Toutefois, cette dernière terminologie est plus souvent employée lorsque G est abélien.*

Proposition 1.27 *Les relations $\sim_{\mathrm{g}}$ et $\sim_{\mathrm{d}}$ sont des relations d'équivalences.*

Démonstration : nous faisons la preuve pour $\sim_{\mathrm{d}}$; l'autre étant identique. Soit $x\in G$ comme $e=x.x^{-1}$ est un élément de H, $x\sim_{\mathrm{d}} x$. Par suite, $\sim_{\mathrm{d}}$ est réflexive. Si maintenant $x\sim_{\mathrm{d}} y$, alors $(xy^{-1})^{-1}\in H$ car H est un sous-groupe de G. Mais $(xy^{-1})^{-1}=yx^{-1}$. par suite $y\sim_{\mathrm{d}} x$ et $\sim_{\mathrm{d}}$ est symétrique. Enfin, si $x\sim_{\mathrm{d}} y$ et $y\sim_{\mathrm{d}} z$,

$$xz^{-1}=x(y^{-1}y)z^{-1}=(xy^{-1})(yz^{-1})\in H\ ;$$

par suite $x\sim_{\mathrm{d}} z$ et $\sim_{\mathrm{d}}$ est transitive. C'est donc bien une relation d'équivalence. □

Exemple : si G est abélien, on peut voir que les relations $\sim_{\mathrm{g}}$ et $\sim_{\mathrm{d}}$ concident (cela découle de la définition). Si on pose $G=\mathbb{Z}$ et $H=n\mathbb{Z}$, alors $x\sim_{\mathrm{g}} y$ si et seulement si $x-y$ est un multiple de n c'est-à-dire si et seulement si les restes de la division par n de x et y sont les mêmes. Usuellement, cette propriété est notée $x\equiv y(n)$. Les classes d'équivalences pour $\sim_{\mathrm{g}}$ sont donc les ensembles $i+n\mathbb{Z}$, où i décrit $0,1,\ldots,n-1$.

Rappelons que par définition, les classes d'équivalences forment une *partition* de G. En particulier, et cette remarque sera souvent utilisée, *deux classes d'équivalences sont disjointes ou égales.*

Lemme 1.28 *Supposons que G est fini. Alors, toutes les classes d'équivalences pour $\sim_{\mathrm{g}}$ (ou pour $\sim_{\mathrm{d}}$) ont exactement $|H|$ éléments (si S est un ensemble fini, on note $|S|$ son cardinal).*

Démonstration : soit $x \in G$. Alors pour tout $h \in H$, on a $x \sim_{\mathrm{g}} xh = y$ puisque $y^{-1}x = h^{-1}x^{-1}x = h^{-1} \in H$. Par suite $\tau_x(H)$ est inclu dans la classe de x. Comme τ_x est une bijection de G dans lui même, $|\tau_x(H)| = |H|$. Inversement, si $x \sim_{\mathrm{g}} y$, alors, $y = x(y^{-1}x)^{-1} \in \tau_x(H)$. Donc la classe de x est contenue dans $\tau_x(H)$. □

Définition 1.29 *Soit G un groupe fini et H un sous-groupe de G. On appellera* indice *de H dans G le nombre de classes à gauches (ou à droite) de G relativement à H. Il est noté $|G : H|$. L'ensemble des classes à gauche sera noté G/H.*

Théorème 1.30 *Si G est un groupe fini, et H est un sous-groupe de G,*

$$|G| = |H| \cdot |G : H| \ ;$$

en particulier,

$$|H| \mid |G| \ .$$

Démonstration : comme toutes les classes d'équivalences ont cardinal $|H|$, et comme l'ensemble des classes d'équivalences forme une partition de G, on a $|G| = |H| \times m$, où m est le nombre de classes d'équivalences. □

Définition 1.31 *Si G est un groupe, et $a \in G$,* l'ordre de *a est le cardinal de $< a >$. On le note $O(x)$ (si $< a >$ est isomorphe à $\mathbb{Z}$, $O(x) = \infty$).*

Corollaire 1.32 *(*Lagrange*) Si x est un élément d'un groupe fini G,*

$$O(x) \mid |G| \ .$$

Démonstration : cela résulte du théorème précédent. □

Corollaire 1.33 *Si G est un groupe fini de cardinal premier, alors G est monogène.*

Démonstration : soit $a \in G$, $a \neq e$. Comme $O(a) \mid |G|$ et comme $|G|$ est premier, soit $O(a) = |G|$ et donc $< a >= G$ soit $O(a) = 1$. Mais alors, $< a >= \{e\}$ et donc $a = a^1 = e$ ce que nous avons exclu. □

On peut généraliser le théorème 1.30 de la manière suivante :

Théorème 1.34 *Soit G un groupe fini et soient H, K deux sous-groupes de G tels que $K \subset H$. Alors,*

$$|G : K| = |G : H| \cdot |H : K| \ .$$

Démonstration : écrivons G et H comme des réunions disjointes de classes à gauches :

$$H = \coprod_{1 \leq i \leq |H:K|} x_i K \ , \quad G = \coprod_{1 \leq j \leq |G:H|} y_j H \ .$$

On en déduit que

$$G = \bigcup_{i,j} y_j x_i K \ .$$

Pour montrer le théorème, il suffit de montrer que cette réunion est disjointe. Supposons donc que $abK = xyK$, ou a et x sont deux éléments du système de représentants de G/H que nous avons choisis : $\{y_1, \ldots, y_{|G:H|}\}$ et b, y sont de même deux éléments parmi les $\{x_i\}$. Pour démontrer le théorème, il suffit donc de voir que $a = x$ et $b = y$.

On a donc :

$$x^{-1}abK = yK \ ;$$

notons que $y \in H$. Donc, comme $K \subset H$, $yK \subset H$. De même, $bK \subset H$. Par conséquent,

$$x^{-1}a \in H \ ;$$

Donc, $a \sim_{\mathrm{g}} x$. Comme ils sont choisis parmi un système de représentants de G/H, $a = x$. Le même raisonnement montre maintenant que $y^{-1}b \in K$ et par suite y et b sont dans la même classe modulo K. Ils sont donc égaux. □

Exemple : soit $\mathfrak{S}_n$ le groupe des permutations de $\{1, \ldots, n\}$. On peut voir $\mathfrak{S}_{n-1}$ comme un sous-groupe de $\mathfrak{S}_n$: si $\sigma \in \mathfrak{S}_{n-1}$, on pose $\iota(\sigma)(i) = \sigma(i)$ si $1 \leq i \leq n-1$ et $\iota(\sigma)(n) = n$. On vérifie alors que :

$$\begin{array}{rccc} \iota \ : & \mathfrak{S}_{n-1} & \hookrightarrow & \mathfrak{S}_n \\ & \sigma & \longmapsto & \iota(\sigma) \end{array} \ ,$$

est un morphisme de groupes injectif. En identifiant $\mathfrak{S}_{n-1}$ à $\mathrm{Im}(\iota)$, on voit bien $\mathfrak{S}_{n-1}$ comme un sous-groupe de $\mathfrak{S}_n$ (nous omettrons par la suite d'écrire ι en identifiant σ et $\iota(\sigma)$). Il est facile de voir que via cette identification, $\mathfrak{S}_{n-1}$ est l'ensemble des éléments σ de $\mathfrak{S}_n$ tels que $\sigma(n) = n$. En effet, par construction, $\mathfrak{S}_{n-1}$ est inclu dans cet ensemble. Inversement, si $\sigma(n) = n$, la restriction τ de σ à $\{1, \ldots, n-1\}$ induit une permutation de $1, \ldots, n-1$. C'est donc un élément de $\mathfrak{S}_{n-1}$. Par définition de ι, on a $\iota(\tau) = \sigma$, d'où l'inclusion inverse.

On a alors :

$$|\mathfrak{S}_n : \mathfrak{S}_{n-1}| = n \ .$$

Pour montrer cette relation, introduisons pour $1 \leq i \leq n$ l'élément τ_i de $\mathfrak{S}_n$ défini par $\tau_i(i) = n$, $\tau_i(n) = i$ et si $j \neq i, j \neq n$, $\tau_i(j) = j$. On notera que τ_n est l'identité. On notera également que $\tau_i^{-1} = \tau_i$. Nous allons montrer que les τ_i forment un système de représentants des classes de $\mathfrak{S}_n$ modulo $\mathfrak{S}_{n-1}$.

Tout d'abord, supposons $i \neq j$. Alors, $\tau_j^{-1} \circ \tau_i(n) = \tau_j^{-1}(i) = i$ si $i \neq n$ et si $i = n$, $\tau_j^{-1} \circ \tau_i(n) = j \neq n$. En tout état de cause, $\tau_j^{-1} \circ \tau_i(n) \neq n$. Ceci montre que si $i \neq j$, alors

$$\tau_j^{-1} \circ \tau_i \notin \mathfrak{S}_{n-1} \ , \quad i.\,e. \quad \tau_i \not\sim_{\mathrm{g}} \tau_j \ .$$

Pour montrer que les τ_i forment un système de représentants des classes de $\mathfrak{S}_n$ modulo $\mathfrak{S}_{n-1}$, il suffit de montrer que pour tout $\sigma \in \mathfrak{S}_n$, il existe un indice $i \leq n$ tel que :

$$\sigma \sim_{\mathrm{g}} \tau_i \ .$$

Comme σ est une permutation de $1, \ldots, n$, il existe un indice $i \leq n$ tel que $\sigma(n) = i$. Dans ces conditions,

$$\tau_i^{-1} \circ \sigma(n) = \tau_i^{-1}(i) = n \ .$$

En d'autres termes,

$$\tau_i \sim_{\mathrm{g}} \sigma \ .$$

Nous avons donc montré que les n permutations τ_i forment un système de représentants des classes de $\mathfrak{S}_n$ modulo $\mathfrak{S}_{n-1}$; en particulier,

$$|\mathfrak{S}_n : \mathfrak{S}_{n-1}| = n \ .$$

On déduit de cette relation que :

$$|\mathfrak{S}_n| = |\mathfrak{S}_{n-1}| \cdot n \ .$$

Par récurrence sur n, on en déduit en particulier (puisque $\mathfrak{S}_1$ est réduit à l'identité) que :

$$|\mathfrak{S}_n| = n! \ .$$

On retrouve ainsi un résultat de combinatoire bien connu : l'ensemble des bijections d'un ensemble de cardinal n dans lui même est de cardinal $n!$.

Exercices : dans $\mathfrak{S}_3$, on pose $\sigma = (123)$ la permutation telle que $\sigma(1) = 2$, $\sigma(2) = 3$ et $\sigma(3) = 1$. Déterminer un sytème de représentants des classes à gauches de $\mathfrak{S}_3$ modulo $< \sigma >$. Décrire entièrement les classes à gauches. Faire de même pour les classes à droite. Que pouvons nous en conclure?

Les permutations τ_i ci dessus forment elles un système de représentants des classes à droites de $\mathfrak{S}_n$ modulo $\mathfrak{S}_{n-1}$? Les classes à droites et à gauches sont elles égales?

1.4 Sous-groupes distingués

Définition 1.35 *Soient G un groupe et H un sous-groupe de G. On dit que H est* distingué *dans G si pour tout $x \in G$,*

$$x^{-1}Hx = H \ .$$

Définition 1.36 *On dit qu'un groupe G est* simple *si les seuls sous-groupes distingué de G sont $\{e\}$ et lui même.*

Exemples : si G est abélien, tout sous-groupe est distingué. Dans $\mathfrak{S}_3$, le sous-groupe engendré par $\sigma = (123)$ défini ci-dessus est distingué.

Exercice : montrer que H est distingué dans G si et seulement si toute classe à gauche modulo H est une classe à droite.

Lorsque H est un sous-groupe distingué, on sait mettre une structure de groupe sur l'ensemble des classes :

Théorème 1.37 *Soit H un sous-groupe distingué de G. Alors, G/H peut être muni d'une structure de groupe naturelle. De plus, il existe un morphisme de groupes surjectif naturel :*

$$\pi \ : \ G \longrightarrow G/H \ ;$$

le noyau de π est H.

Démonstration : soit $x \in G$; on pose $\pi(x) := \overline{x}$, où $\overline{x}$ est la classe xH de x. L'application π est ainsi bien définie et surjective. Nous allons maintenant construire la loi de groupe sur G/H :

$$\begin{array}{rccc} \star \ : & G/H \times G/H & \longrightarrow & G/H \\ & (\overline{x}, \overline{y}) & \longmapsto & \overline{x} \star \overline{y} := \overline{x.y} \ . \end{array}$$

Avant de montrer que $(G/H, \star)$ est un groupe, il convient de montrer que la loi $\star$ ainsi construite est bien définie. Pour ceci, supposons que x', y' sont des éléments de G tels que $\overline{x'} = \overline{x}$ et $\overline{y'} = \overline{y}$. Il s'agit de montrer que

$$\overline{x'.y'} = \overline{x.y} \ .$$

Par définition, il existe $a, b \in H$ tels que $x' = xa$ et $y' = ya$. Donc,

$$x'.y' = (xa).(yb) = x(yy^{-1})a(yb) = (xy)(y^{-1}ay)b \ .$$

Comme H est distingué, $c := (y^{-1}ay)$ est un élément de H. Par suite,

$$x'.y' = x.y(cb) \ ,$$

et $\overline{x'.y'} = \overline{x.y}$ puisque $cb \in H$. La loi ainsi construite est donc bien définie. Nous allons montrer tout d'abord que $(G/H, \star)$ est un groupe. Nous pourrons ensuite montrer que π est un morphisme de groupes.

(a) Existence d'un neutre : montrons que $\overline{e}$ est un élément neutre. Soit $\overline{x}$ un élément de G/H. Dans ces conditions,

$$\overline{e} \star \overline{x} = \overline{e.x} = \overline{x} = \overline{x.e} = \overline{x} \star \overline{e} \ .$$

(b) Associativité : soient $\overline{x}, \overline{y}, \overline{z}$ des éléments de G/H. On a :

$$\overline{x} \star (\overline{y} \star \overline{z}) = \overline{x} \star (\overline{y.z}) = \overline{x.(y.z)} = \overline{(x.y).z} \ ,$$

car la loi est associative sur G; puis, de façon symétrique,

$$\overline{(x.y).z} = \overline{(x.y)} \star \overline{z} = (\overline{x} \star \overline{y}) \star \overline{z} \ .$$

(c) Existence d'un inverse : soit $\overline{x}$ un élément de G/H. Par définition,

$$\overline{x} \star \overline{x^{-1}} = \overline{x.x^{-1}} = \overline{e} \ .$$

Nous avons donc bien montré que $(G/H, \star)$ est un groupe. Maintenant, vérifions que π est un morphisme de groupes. Soient $x, y \in G$. Par définition de π et de $\star$,

$$\pi(x.y) = \overline{x.y} = \overline{x} \star \overline{y} = \pi(x) \star \pi(y) \ .$$

Pour finir, il reste à calculer le noyau de π. Soit donc $x \in \ker(\pi)$. Par définition,

$$\pi(x) = \overline{x} = \overline{e} \ ,$$

ce qui revient à dire que $x \in H$. D'où le théorème. □

On dispose d'un critère intéressant popur montrer qu'un sous-groupe est distingué :

Théorème 1.38 *Soit $f : G \longrightarrow G'$ un morphisme de groupes. Alors* $\ker(f)$ *est un sous-groupe distingué de G.*

Démonstration : soit $x \in G$ et $a \in \ker(f)$. Nous devons montrer que $x^{-1}ax \in \ker(f)$. Mais,

$$f(x^{-1}ax) = f(x)^{-1}f(a)f(x) = f(x)^{-1}e'f(x) = e' \ .$$

D'où le résultat. □

Remarque : en particulier, la conjonction de ces deux théorèmes nous montre qu'un sous-groupe H de G est distingué si et seulement s'il existe un morphisme de groupes de G vers un groupe G' dont le noyau est H.

Proposition 1.39 *Soit G un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes distingués. Alors,*

$$\bigcap_{i \in I} H_i$$

est distingué.

Démonstration : soit $a \in \cap_i H_i$ et $x \in G$. Comme H_i est distingué pour chaque indice i, $x^{-1}ax \in H_i$ et donc $x^{-1}ax \in \cap_i H_i$. □

Exemple : *soit G un groupe et H un sous-groupe d'indice 2; alors H est un sous-groupe distingué de G.* En effet, supposons qu'il existe un conjugué K de H, avec $H \neq K$. Soit $x \in K \setminus H$. Puisque H est d'indice 2 dans G, on a

$$G = H \coprod xH \ .$$

Soit h un élément de H, et $y \in G$. Nous allons calculer yhy^{-1}. Si $y \in H$, ce produit est dans H car H est un groupe. Sinon, $y \in xH$ par la décomposition ci-dessus et donc il existe $h' \in H$ tel que $y = xh'$. Par conséquent, il existe $h'' \in H$ tel que $yhy^{-1} = xh''x^{-1}$. Comme $x^{-1} \notin H$, et $h'' \in H$, $h''x^{-1} \notin H$. Donc, il existe $l \in H$ tel que $h''x^{-1} = xl$. Donc, $yhy^{-1} = x^2 l$; si $x^2 \in H$, cette quantité est dans H. Sinon, elle est de la forme xk, avec $k \in H$. Mais dans ce cas, $xl = k \in H$, ce qui entraîne $x \in H$. Une contradiction.

Exercice : soit G un groupe fini et p le plus petit nombre premier divisant $|G|$. Montrer que tout sous-groupe de G d'indice p est distingué.

1.5 Suites exactes, factorisation

Définition 1.40 *Soient*

$$G' \xrightarrow{f} G \xrightarrow{g} G''$$

des morphismes de groupes. On dit que c'est une suite exacte *si :*

$$\ker(g) = \mathrm{Im}(f) \ .$$

Plus généralement, la suite de morphismes

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \cdots \xrightarrow{f_{n-1}} G_n$$

est dite exacte si

$$\ker(f_{i+1}) = \mathrm{Im}(f_i)$$

pour tout i (on notera que la suite peut être infinie).

Exemple : si H est un sous-groupe distingué de G, la suite :

$$H \xhookrightarrow{\iota} G \xrightarrow{\pi} G/H$$

est exacte (*confer* le théorème 1.37).

Proposition 1.41 *Soit $f : G \longrightarrow G'$ un morphisme de groupes. Alors, il existe un unique morphisme $\tilde{f} : G/\ker(f) \longrightarrow G'$ tel que*

$$\tilde{f} \circ \pi = f \ .$$

Plus généralement, si $H \subset \ker(f)$ est un sous-groupe distingué de G, il existe un morphisme $f' : G/H \longrightarrow G'$ tel que $f' \circ \pi = f$, où π est la projection canonique de G vers $G/\ker(f)$ dans le premier cas et vers G/H dans le deuxième.

Démonstration : soit $x \in G$, on définit $\tilde{f}(x) := f(\overline{x})$. De cette manière, on voit que $\tilde{f} \circ \pi = f$; l'application est bien définie car si $\overline{y} = \overline{x}$, alors $xy^{-1} \in H$, et par suite $f(xy^{-1}) = f(x)f(y)^{-1} = e'$. On vérifie facilement que l'application ainsi définie est bien un morphisme de groupes. □

Exemples : si G est un groupe fini, et f est un morphisme de groupes surjectif de G vers G', alors le théorème de factorisation nous assure que f induit un *isomorphisme* $\tilde{f}$ de $G/\ker(f)$ vers G'. En particulier, $|G| = |\mathrm{Im}(f)| \cdot |\ker(f)|$ pour tout morphisme de groupes.

Remarque : à l'aide de f, on a de façon triviale une suite exacte :

$$\{e\} \longrightarrow H \hookrightarrow G \xrightarrow{\pi} G/H \xrightarrow{\tilde{f}} \mathrm{Im}(f') \hookrightarrow G' \ .$$

Exemples : supposons que $K \subset H \subset G$ sont deux sous-groupes distingués de G. Nous pouvons définir l'application f de G/K vers G/H qui à un élément $\overline{x}$ de G/K associe la classe de x modulo H (il est facile de voir que cette application est bien définie). On voit que $\ker(f) = H/K$. Le théorème de factorisation nous fournit donc un morphisme canonique

$$\tilde{f} \ : \ (G/K)/(H/K) \longrightarrow G/K \ ;$$

On voit que $\tilde{f}$ est en fait un isomorphisme.

Soient G un groupe, H, K deux sous-groupes. On suppose que pour tout $x \in H$, $x^{-1}Kx = K$ (*i. e.* H est contenu dans le plus grand sous-groupe de G dans lequel H est distingué, qu'on appelle le *normalisateur* de K, noté N_K). Alors, $H \cap K$ est un sous-groupe distingué de H. En effet, si $x \in H$ et $y \in H \cap K$, $xyx^{-1} \in H$ puisque tous ces éléments sont dans H. De même, il est dans K par hypothèse. De plus l'ensemble $HK = \{hk, h \in H, k \in K\}$ est un sous-groupe de G. En effet, il est non vide (puisque l'élément neutre est dans HK) de plus, si $hk, h'k'$ sont des éléments de HK, $(hk).(h'k')^{-1} = h(kk').h'^{-1}$. Comme $h'Kh'^{-1} = K$, il existe $k'' \in K$ tel que $(kk')h'^{-1} = h'^{-1}k''$. Donc, $(hk).(h'k')^{-1} = (hh^{-1}).k''$ est bien dans HK. On notera aussi que $HK = KH$. Notons aussi que K est un sous-groupe distingué de HK. En effet, si $x = hk \in HK$ et $y \in K$, $xyx^{-1} = hkyk^{-1}h^{-1}$. Par définition, $y' = kyk^{-1} \in K$, donc $xyx^{-1} = hy'h^{-1} \in hKh^{-1} = K$ par hypothèse sur H.

On dispose alors d'un morphisme canonique :

$$\begin{array}{rccc} f \ : & H & \longrightarrow & HK/K \\ & x & \longmapsto & f(x) := xK \ , \end{array}$$

où xK est la classe de x modulo le sous-groupe K de HK. On vérifie (exercice) que f est bien un morphisme de groupes. De plus, f est surjective. En effet, si $y \in HK$, on peut écrire $y = hk$, avec $h \in H$ et $k \in K$ et par suite la classe $yK = hkK = hK$. Conclusion, $f(h) = yK$ et h est un antécédant

de yK par f. Déterminons maintenant le noyau de f : si $x \in H \cap K$, alors $xK = K$ et par suite $f(x) = eK$ est l'élément neutre de HK/K. Donc, $H \cap K \subset \ker(f)$. Inversement, si $x \in \ker(f)$, on a $f(x) = eK$, et cela veut dire que $xK = K$ et donc $x \in K$. Par conséquent, $x \in K$ et donc $\ker(f) \subset H \cap K$.

En conclusion, le théorème de factorisation nous permet d'en déduire un isomorphisme canonique :

$$H/(H \cap K) \simeq HK/K \ .$$

En particulier, lorsque H et K sont finis, on en déduit l'égalité suivante entre cardinaux :

$$|HK| \cdot |H \cap K| = |H| \cdot |K| \ .$$

On notera l'analogie avec la relation bien connue pour les sommes et intersections d'espaces vectoriels :

$$\dim(V) + \dim(W) = \dim(V + W) + \dim(V \cap W) \ .$$

Exercice : soient H et K deux sous-groupes distingués d'un groupe fini G. On suppose $\text{pgcd}(|H|, |K|) = 1$. Montrer que pour tous $x \in H$, $y \in K$, $xy = yx$. En déduire que

$$H \times K \simeq HK \ .$$

2 Opérations, théorèmes de Sylow

2.1 Groupes opérant sur un ensemble

Définition 2.1 *Soit G un groupe et S un ensemble non vide. Une* opération π de G sur S *est un morphisme de groupes $\pi : G \longrightarrow \mathrm{Perm}(S)$.*

En d'autres termes, π associe à chaque élément g de G une *bijection* de S dans lui même. On peut donc aussi voir l'opération π comme une application :

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (g,x) & \longmapsto & \pi(g)(x) \ . \end{array}$$

En général, $\pi(g)(x)$ est simplement noté $g.x$ ou même gx. Le fait que π est un morphisme de groupes se traduit par les conditions

$$(gg').x = g.(g'.x) \ , \quad \text{et} \quad e.x = x \ .$$

Exemples : on prend $G = S$, et l'on pose $\pi(g) = \tau_g$, la translation par g. Toujours avec $G = S$, la conjugaison est aussi une opération de groupes; on pose $\pi(g)(x) := gxg^{-1}$.

Autre exemple : si $S = V$ est un k-espace vectoriel, et si $G = \mathrm{Gl}(V)$, on a une opération de G sur S, en posant $\pi(g)(x) = g(x)$.

Enfin, l'opération triviale : S est quelconque, G aussi, on pose simplement $\pi(g) = \mathrm{Id}$ pour tout $g \in G$.

Définition 2.2 *Soit G un groupe opérant sur un ensemble S. Pour $x \in S$, le* stabilisateur *de x est l'ensemble*

$$G_x := \{g \in G, \ g.x = x\} \ .$$

L'orbite *de x est l'ensemble*

$$G(x) := \{y \in S, \ \exists g \in G, \ g.x = y\} \ .$$

On dit que x est un point fixe *de l'opération si $G_x = G$. On dit enfin que G* opère transitivement *sur S si $G(x) = S$.*

Exemples : si G opère sur lui même par translation, il n'y a pas de points fixes dès que $G \neq \{e\}$. Le stabilisateur de x est réduit à $\{e\}$, et l'opération est transitive. par contre, lorsque G opère sur lui même par conjugaison, le stabilisateur d'un élément x de G est le *commutateur* de x : c'est l'ensemble des $g \in G$ tels que $gx = xg$. Donc, si par exemple G est abélien, l'opération n'est rien d'autre que l'opération triviale (tous les points sont fixes).

Plus généralement, les points fixes pour la conjugaison sont les éléments de G *qui commutent à tous les éléments de G* : c'est le *centre* du groupe G, noté Z_G :

$$Z_G := \{x \in G, \ \forall\, u \in G, \ xu = ux\} \ .$$

La nature des orbites peut donc varier fortement en fonction de G. Enfin, $\mathfrak{S}_n$ opère transitivement sur $\{1, \ldots, n\}$ *via* l'opération identité $\mathrm{Id} : \mathfrak{S}_\mathrm{n} \longrightarrow \mathfrak{S}_\mathrm{n}$.

Lemme 2.3 *Soient G opérant sur un ensemble S, et $x \in S$. Alors, le stabilisateur G_x est un sous-groupe de G.*

Démonstration : G_x n'est pas vide puisque $e \in G_x$. Ensuite, si $g, g' \in G_x$, notons tout d'abord que $g^{-1}.x = x$ puisque $x = e.x = g^{-1}(g.x) = g^{-1}.x$. Maintenant, $(gg'^{-1}).x = g.(g'^{-1}.x) = g.x = x$ par définition. Donc $gg'^{-1} \in G_x$ qui est donc un sous-groupe de G. □

Définition 2.4 *Soient G un groupe opérant sur un ensemble S et $x, y \in S$. On dit que $x \sim y$ si $y \in G(x)$.*

Lemme 2.5 *La relation $\sim$ est une relation d'équivalence.*

Démonstration : puisque $e.x = x$, $x \in G(x)$ et donc $x \sim x$, et $\sim$ est réflexive. Si $x \sim y$, alors, il existe $g \in G$ tel que $y = g.x$. Par suite, $x = g^{-1}.y$ et $x \in G(y)$. Donc, $\sim$ est symétrique. Enfin, si $x \sim y$ et $y \sim z$, alors il existe $g, h \in G$ tels que $y = g.x$ et $z = h.y$. Donc, $(h.g).x = h.(g.x) = h.y = z$ et donc $z \in G(x)$ et $\sim$ est transitive. En particulier, l'ensemble des orbites forme une partition de S. □

Théorème 2.6 *Soit G un groupe fini opérant sur un ensemble S. Alors,*

$$|G : G_x| = |G(x)| \ .$$

*En particulier, si S est fini, on a (*formule des classes*) :*

$$|S| = \sum_x |G : G_x| \ ,$$

où la somme est étendue à un système de représentants de l'ensemble des orbites de S pour l'action de G.

Démonstration : soit $g \in G$ et $h = gk \in gG_x$. Alors,

$$h.x = (g.k).x = g(k.x) = g.x \ ,$$

car $k \in G_x$. Donc si g, h sont dans la même classe de G modulo G_x, $g.x = h.x$. Inversement, si $g.x = h.x$, alors, $(h^{-1}.g).x = x$ et donc $(h^{-1}.g) \in G_x$ c'est-à-dire $h \in gG_x$. L'application f qui à $\overline{g} \in G/G_x$ associe $f(\overline{g}) = g.x$ est donc bien définie et injective. ceci donne déjà $|G/G_x| \leq |G(x)|$. Inversement, si $y \in G(x)$, soit $g \in G$ tel que $y = g.x$, on voit facilement par définition que $f(\overline{g}) = y$ donc f est surjective et par suite $|G/G_x| \geq |G(x)|$. ceci montre le théorème, la formule des classes découlant immédiatement du fait qu'une relation d'équivalence induit une partition. □

Définition 2.7 *Soit G un groupe et $x \in G$. Le* centralisateur *de x est*

$$\{g \in G,\ gx = xg\}\ .$$

Lemme 2.8 *Soient G un groupe et $x \in G$. Alors le centralisateur de x est un sous-groupe de G.*

Démonstration : C_x est non vide puisque $e \in C_x$. Si $g, h \in C_x$,

$$(gh).x = g.(hx) = g.(xh) = (gx).h = x.(gh)\ .$$

D'où le lemme. □

On notera aussi que le centralisateur de x est le stabilisateur de x lorsque G opère sur lui même par conjugaison.

Corollaire 2.9 *Soit G un groupe fini, et I un système de représentants des orbites pour l'action de G sur lui même par conjugaison. Alors,*

$$|G| = \sum_{x \in I} |G : C_x|\ .$$

Démonstration : c'est ce que donne la formule des classes dans ce cas particulier. □

Lemme 2.10 *Soient G un groupe opérant sur S, $x \in S, g \in G$ et $y = g.x \in G(x)$. Alors,*

$$G_y = gG_xg^{-1}\ .$$

Démonstration : soit $ghg^{-1} \in gG_xg^{-1}$, on a $(ghg^{-1}).y = (gh).g^{-1}y = (gh).x = g.x = y$. Inversement, si $k.y = y$, alors $k.(g.x) = g.x$ et donc, $(g^{-1}kg).x = x$. En conclusion, $(g^{-1}kg) \in G_x$ et donc $k \in gG_xg^{-1}$. □

Lemme 2.11 *Soient $\pi : G \longrightarrow S$ une opération de G sur S, et $K = \ker(\pi)$. Alors,*

$$K = \bigcap_{x \in S} G_x\ .$$

Démonstration : si $g \in \bigcap_{x \in S} G_x$, alors, pour tout $x \in S$, $g.x = x$. Par suite, $\pi(g)$ est la permutation identité sur S, *i. e.* $g \in \ker(\pi)$. Inversement, si $\pi(g)$ est la permutation identité sur S, $g.x = x$ pour tout $x \in S$ et donc $g \in \bigcap_{x \in S} G_x$. □

Définition 2.12 *On dit que G opère* fidèlement *sur S si* $\ker(\pi) = \{e\}$.

Exemples : si G opère sur lui même par translation, il opère fidèlement.

Nous donnons maintenant quelques exemples d'utilisation de la notion d'opération d'un groupe G sur un ensemble pour étudier les propriétés de G.

(i) Soit G un groupe fini, et H un sous-groupe. Rappelons que le *normalisateur* N_H de H dans G est le plus grand sous-groupe de G dans lequel H est distingué (qui est égal à $\{g \in G, gHg^{-1} = H\}$). Alors, *le nombre de conjugués distincts de H est égal à l'indice de N_H dans G* (on notera que par définition, H est distingué si et seulement si $N_H = G$, ou si et seulement si tous ses conjugués sont égaux; dans le cas où $|G : N_H| = 1$, nous connaissons donc déjà cette propriété). On fait opérer G par conjugaison sur l'ensemble des sous-groupes de G (exercice : vérifier que c'est bien une opération de groupe sur un ensemble). Le nombres de conjugués distincts de H est donc égal par définition à $|G(H)|$ (le cardinal de l'orbite de H pour cette opération). Mais, G_H (le stabilisateur de H) est par définition, l'ensemble des $g \in G$ tels que $gHg^{-1} = H$, qui n'est rien d'autre que N_H. Par le théorème 2.6, $|G(H) = |G : N_H|$, ce que l'on voulait.

(ii) Nous avons déjà vu que tout sous-groupe d'indice 2 dans un groupe fini G est distingué. Nous allons donner une autre preuve de cette propriété. Il s'agit de montrer que $N_H = H$. Comme $H \subset N_H \subset G$, l'indice $|G : N_H|$ vaut 1 ou 2. S'il vaut, 1, il n'y a rien à démontrer. On peut donc supposer qu'il vaut 2, c'est-à-dire que $N_H = H$, et que H possède deux conjugués distincts : lui même et un autre groupe de même cardinal K. Dans ce cas, l'application :

$$\begin{array}{rcccl} \varphi : & G & \longrightarrow & \mathrm{Perm}(H,K) & \\ & g & \longmapsto & \varphi(g) : \{H,K\} & \longrightarrow \{H,K\} \\ & & & H & \longmapsto \varphi(g)(H) := gHg^{-1} \\ & & & K & \longmapsto \varphi(g)(K) := gKg^{-1} \ , \end{array}$$

est un morphisme de groupes (excercice : vérifier que $\varphi(g)$ est bien une permutation de l'ensemble $\{H, K\}$ et que c'est un morphisme de groupes). De plus, c'est un morphisme de groupes surjectif puisque K est un conugué de H. Donc $\mathrm{Im}(\varphi)$ est de cardinal $|\mathrm{Perm}(H,K)| = 2$ et $\ker(\varphi)$ est un sous-groupe de G d'indice 2 puisque $|G| = |\ker(f)| \cdot |\mathrm{Im}(f)|$ pour tout morphisme par le théorème de factorisation. On notera que $\ker(\varphi)$ contient H et donc $H = \ker(\varphi)$ puisque H est d'indice 2. Mais $\ker(\varphi)$ est distingué. Donc, H l'est aussi, une contradiction.

Exercices : soit G opérant sur un ensemble S, de cardinal $|S| \geq 2$. On suppose qu'il n'y a qu'une seule orbite. Montrer qu'il existe $g \in G$ tel que pout tout $x \in S$, $g.x \neq x$.

Montrer qu'un groupe fini ne peut pas être la réunion des conjugués d'un sous-groupe $H \neq G$ de G.

2.2 Sous-groupes de Sylow

Dans ce paragraphe, tous les groupes seront supposés *finis*.

Définition 2.13 *Soit p un nombre premier. On dit que G est un p-*groupe *si G est un groupe dont le cardinal est une puissance de p. De même, pour un p* sous-groupe*. Enfin, on dit qu'un sous-groupe H de G est un p* un sous-groupe de Sylow *si $|H| = p^{v_p(|G|)}$ où $v_p(|G|)$ est l'unique entier tel que $|G| = p^{v_p(|G|)}m$ avec p ne divisant pas m.*

Théorème 2.14 *Soit G un groupe fini; alors pour tout nombre premier p divisant $|G|$, il existe un p sous-groupe de Sylow de G.*

Démonstration : nous allons procéder par récurrence sur $|G|$ (notons aussi qu'il n'y a rien à démontrer si $|G|$ est une puissance d'un nombre premier). Supposons le théorème vrai pour tout groupe de cardinal $< n$ (pour $n \geq 2$) et soit G de cardinal n. Nous allons provisoirement admettre le lemme suivant[1] :

Lemme 2.15 *Soit G un groupe abélien et p un nombre premier divisant $n = |G|$. Alors, il existe un sous-groupe H de G d'ordre exactement p.*

Soit H un sous-groupe strict de G (il en existe puisqu'il suffit de prendre par exemple $H = \{e\}$). Si $(|G : H|, n) = 1$, tout sous-groupe de Sylow de H est un sous-groupe de Sylow de G, ce qui permet de conclure par l'hypothèse de récurrence. On peut donc supposer que $p \mid |G : H|$ pour *tout* sous-groupe strict H de G.

Faisons opérer G sur lui-même par conjugaison. La formule des classes nous donne :

$$|G| = |Z_G| + \sum_{i \in I} |G : G_i| \ ,$$

où Z_G est le centre de G et les G_i sont différents de G. Par hypothèse, $p \mid |G : G_i|$ puisque G_i est un sous-groupe strict de G pour tout $i \in I$ (dire que $G_i = G$ revient à dire que l'orbite associée à cette classe de conjugaison est réduite à un seul élément, c'est-à-dire que ce point appartient au centre Z_G de G, ce que nous avons exclu). Comme p divise aussi $|G|$, on en déduit que $p \mid |Z_G|$. Soit donc $a \in Z_G$ un élément de Z_G d'ordre exactement p (il en existe au moins un par le lemme 2.15). Posons alors $H =< a >$. Le sous-groupe H est distingué dans G puisqu'il est contenu dans Z_G. Considérons la projection

$$\pi \ : \ G \longrightarrow G/H \ ;$$

par hypothèse de récurrence, G/H contient un p-Sylow K'. Posons $K = \pi^{-1}(K')$. Comme a est d'ordre p, le cardinal de K' est

$$p^{v_p(|G/H|)} = p^{v_p(|G|) - v_p(o(a))} = p^{v_p(|G|)-1} \ .$$

[1] Une démonstration de ce lemme sera fournie au chapitre suivant sur les groupes abéliens.

Par le théorème de factorisation, la projection $K \xrightarrow{\pi} K'$ se factorise à travers K/H , et l'on a une bijection $\tilde{\pi} : K/H \simeq K'$. Donc, le cardinal de K vaut $|K| = |K'| \cdot p = p^{v_p(|G|)}$. Donc, K est un p-Sylow de G. □

Lemme 2.16 *Soit H un p-groupe opérant sur un ensemble fini S. Alors,*

(i) le nombres de points fixes de l'action est $\equiv |S| \bmod (p)$;

(ii) si l'action de H a exactement un point fixe, alors $|S| \equiv 1 \bmod (p)$;

(iii) si $p \mid |S|$, le nombre de points fixes de l'action est divisible par p.

Démonstration : bien entendu, les points *(ii)* et *(iii)* découlent de *(i)*. Soit I un système de représentants des orbites de S non triviales sous l'action définie par H. La formule des classes s'écrit :

$$|S| = |\{\text{points fixes}\}| + \sum_{i \in I} |H : H_i| = |\{\text{points fixes}\}| + p(\star) \ ,$$

en effet, puisque H est un p-groupe, $|H : |H_i|$ est un multiple de p sauf si $H_i = H$, ce que l'on a exclu puisque l'on a mis séparément les points fixes. D'où le point *(i)* et par suite le lemme. □

Théorème 2.17 *Soit G un groupe fini, et p un nombre premier divisant $|G|$. Alors :*

(i) si H est un p sous-groupe de G, il est contenu dans un p-sous groupe de Sylow de G;

(ii) tous les p-Sylow sont conjugués;

(iii) le nombre de p-Sylow est un diviseur de $|G|$. De plus, il est $\equiv 1 \bmod (p)$.

Démonstration : montrons tout d'abord *(i)*. Soit H un p sous-groupe de G et P un p-Sylow[2]. Nous allons tout d'abord supposer que $H \subset N_P$. En particulier, $HP \subset N_P$. Au vu de l'exemple traité page 16, nous savons que

$$|HP : P| = |H : H \cap P| \ .$$

Si $H \not\subset P$, $|HP : P| \neq 1$ et donc, la formule ci-dessus montre que l'ordre de HP est une puissance de p, strictement supérieure à $|P|$ ce qui contredit le fait que P est un p-Sylow. Donc, $HP = P$ et par suite, $H \subset P$.

[2]L'existence de P est assurée par le théorème précédent. Une nouvelle preuve sera fournie lors de la preuve du point (iii) du théorème, qui n'utilise pas les précédents.

Nous allons maintenant montrer que l'on peut se ramener au cas $H \subset N_P$. Considérons l'ensemble :

$$S := \{\text{conjugués de } P\} \ .$$

Le groupe G opère sur S par conjugaison, et, par restriction à H de cette opération, H opère sur S. Notons que le cardinal de S est exactement $|G : N_P|$ (voir l'exemple (i), page 20). Comme $P \subset N_P$, on a donc $(|S|, p) = 1$ et donc, par le lemme 2.16, l'action de H sur S admet au moins un point fixe, disons Q. Notons que puisque Q est un conjugué de P, c'est aussi un p-Sylow de G. Puisque Q est fixé par l'action de H, on a :

$$\forall h \in H, \ \forall x \in Q, \quad hxh^{-1} \in Q \ .$$

Ceci revient à dire que $H \subset N_Q$. Par la première partie de la preuve, on en déduit donc que $H \subset Q$. Ceci démontre le point (i), mais aussi le point (ii), en faisant $H = P$.

Montrons maintenant le point (iii). Notons r la valuation en p de $|G|$ et soit $\mathcal{F}$ l'ensemble des sous-ensembles de G de cardinal p^r. On fait agir G sur $\mathcal{F}$ par translation à gauche. Soit H un p-Sylow de G; l'orbite de H pour cette action est l'ensemble des classes à gauches de H. Le stabilisateur de H est égal à H.

Soit maintenant $\mathcal{X}$ une orbite de $\mathcal{F}$ pour cette action et X un élément de $\mathcal{X}$. Notons G_X le stabilisateur de X. On a donc :

$$\forall g \in G, \ gX = X \ .$$

Par suite, $G_X.X = X$ et donc,

$$\forall x \in X, \ G_X \cdot x \subset X \ ,$$

et donc,

$$|G_X| \leq |X| = p^r \ .$$

Inversement, on a

$$|\mathcal{X}| = |G : G_X| = \frac{mp^r}{|G_X|} \ .$$

Supposons que $(|\mathcal{X}|, p) = 1$. La relation précédente nous assure alors que $|G_X|$ est un multiple de p^r. En particulier, $|G_X| \geq p^r$. Ceci assure que $|G_X| = p^r$. Donc, il existe un élément $x \in G$ tel que

$$X = G_X \cdot x \ .$$

Puisque G opère sur $\mathcal{F}$ par translation à gauche, $x^{-1}G_X x = x^{-1} \cdot X \in \mathcal{X}$ est un sous-groupe de G d'ordre p^r.

En conclusion, $\mathcal{X}$ contient un sous-groupe K de G d'ordre p^r. Inversement, puisque $\mathcal{X}$ est l'ensemble des classes à gauches de K, l'orbite $\mathcal{X}$ contient un sous-groupe de G d'ordre p^r et un seul : c'est K.

Nous avons donc démontré le résultat intermédiaire suivant : *l'ensemble des sous-groupes de G d'ordre p^r est en bijection avec l'ensemble des orbites $\mathcal{X}$ de $\mathcal{F}$ pour l'action de G d'ordre premier à p.* Le cardinal de l'ensemble des p sous-groupes de Sylow est donc égal au cardinal de l'ensemble de telles orbites qu'il s'agit maintenant d'estimer pour établir le point (iii).

Nous allons maintenant montrer le lemme combinatoire suivant :

Lemme 2.18 *Soit p un nombre premier et m un entier premier à p. Soit de plus r un entier ≥ 1. Alors,*

$$\left(\begin{array}{c} mp^r - 1 \\ p^r - 1 \end{array} \right) \equiv 1 \bmod (p) \ ,$$

et

$$\left(\begin{array}{c} mp^r \\ p^r \end{array} \right) \equiv m \bmod (p) \ .$$

Démonstration : par définition,

$$\left(\begin{array}{c} mp^r - 1 \\ p^r - 1 \end{array} \right) = \frac{mp^r - 1}{1} \times \frac{mp^r - 2}{2} \times \cdots \times \frac{mp^r - p^r + 1}{p^r - 1} \ .$$

Pour chaque entier i compris entre 1 et $p^r - 1$, remarquons maintenant que

$$v_p(mp^r - i) = v_p(i)$$

puisque la valuation de i est plus petite que r. Après simplification par $p^{v_p(i)}$, le quotient $\frac{mp^r - i}{i}$ est donc premier à p. On peut donc considérer sa réduction dans $\mathbb{Z}/p\mathbb{Z}$ qui vaut -1. Au total, on a donc

$$\left(\begin{array}{c} mp^r - 1 \\ p^r - 1 \end{array} \right) \equiv (-1)^{p^r - 1} \bmod (p) \ ,$$

si p est impair, $p^r - 1$ est pair, ce qui montre bien que

$$\left(\begin{array}{c} mp^r - 1 \\ p^r - 1 \end{array} \right) \equiv 1 \bmod (p) \ .$$

Si $p = 2$, $1 = -1$ et l'on a aussi le résultat. Pour la deuxième égalité, on remarque que

$$\left(\begin{array}{c} mp^r \\ p^r \end{array} \right) = \frac{mp^r}{p^r} \left(\begin{array}{c} mp^r - 1 \\ p^r - 1 \end{array} \right) \ ,$$

et le lemme suit. □

Revenons maintenant à la preuve du théorème 2.17. Séparons les orbites de $\mathcal{F}$ en deux parties : $\mathcal{E}$ étant l'ensemble des orbites dont le cardinal est premier à p et $\mathcal{E}'$ l'ensemble des orbites dont le cardinal est un multiple de p. Notons que si $\mathcal{X} \in \mathcal{E}$, alors $|\mathcal{X}| = m$. En effet, on a vu que $\mathcal{X}$ contient un sous-groupe K d'ordre p^r et donc $\mathcal{X}$ est l'ensemble des classes à gauches de K. Le cardinal de $\mathcal{X}$ vaut donc :

$$|G : K| = \frac{mp^r}{p^r} = m \ .$$

Ecrivons maintenant la formule des classes :

$$|\mathcal{F}| = \sum_{\mathcal{X} \in \mathcal{E}'} |\mathcal{X}| + \sum_{\mathcal{X} \in \mathcal{E}} |\mathcal{X}| \ .$$

En tenant compte de la remarque précédente, cette formule entraîne en particulier :

$$|\mathcal{F}| \equiv \sum_{\mathcal{X} \in \mathcal{E}} |\mathcal{X}| \bmod (p) \equiv m|\mathcal{E}| \bmod (p) \ .$$

Mais, $\mathcal{F}$ est l'ensemble des parties de G à p^r éléments. Par suite,

$$|\mathcal{F}| = \left(\begin{array}{c} mp^r \\ p^r \end{array} \right) \ .$$

Par le lemme 2.18, on a donc :

$$\left(\begin{array}{c} mp^r \\ p^r \end{array} \right) \equiv m|\mathcal{E}| \bmod (p) \equiv m \bmod (p) \ .$$

Comme m est premier à p, on en déduit que

$$|\mathcal{E}| \equiv 1 \bmod (p) \ .$$

Mais, on a vu que le nombre de p-sous-groupes de Sylow de G est égal à $|\mathcal{E}|$. On a donc montré que le nombre de p-sous-groupes de Sylow de G est[3]

$$\equiv 1 \bmod (p) \ .$$

Pour conclure la preuve du point (iii), rappelons que comme par le point (ii) les sous-groupes de Sylow sont tous conjugués, leur nombre est égal à

$$|G : N_H| \ .$$

Ce nombre divise donc $|G|$, d'où le théorème 2.17. □

[3]En particulier, il existe des p-sous-groupes de Sylow.

Exemples : (i) tout groupe d'ordre 15 est commutatif. Pour le montrer, considérons les 3-Sylow et les 5-Sylow de G. Le nombre de 3-Sylow divise 15 (c'est donc $1, 3, 5$ ou 15) et est $\equiv 1 \bmod (3)$. Ce ne peut donc que 1. Il existe donc un et un seul 3-sous-groupe de Sylow de G. Notons ce groupe H_3. De même, le nombre de 5-Sylow divise 15 est est $\equiv 1 \bmod (15)$, c'est donc 1. Notons H_5 l'unique 5-Sylow de G. Comme H_3 et H_5 sont d'ordre premier, ce sont des groupes abéliens. Soit x un générateur de H_3 et y un générateur de H_5. Il suffit de montrer que x et y commutent. Comme H_5 est distingué, $xyx^{-1} \in H_5$ et donc, il existe un entier a, $0 \leq a \leq 4$ tel que :

$$xyx^{-1} = y^a \ .$$

Par itération,

$$x^2yx^{-2} = x(xyx^{-1})x^{-1} = xy^ax^{-1} = (xyx^{-1})^a = y^{a^2} \ ,$$

et, de même,

$$x^3yx^{-3} = y^{a^3} \ .$$

Mais, $x^3 = e$ et donc,

$$y = y^{a^3} \ .$$

Comme y est d'ordre 5, on en déduit que

$$5 \mid a^3 - 1 \ .$$

Mais, cette relation n'est possible que si $a = 1$ (vérification numérique pour les 5 valeurs possibles de a). En d'autres termes, x et y commutent.

(ii) Soit G un groupe d'ordre 12. Alors, soit un 2-Sylow soit un 3-Sylow de G est distingué (un tel sous-groupe est alors unique). Supposons que les trois sous-groupes de Sylow ne sont pas distingués. Il y a alors exactement 4 3-sous-groupes de Sylow de G (en effet, ce nombre divise 12, c'est donc 1, 2, 3, 4, 6 ou 12 et il est $\equiv 1 \bmod (3)$ donc c'est 1 ou 4; puisqu'on a supposé que ce n'est pas 1, c'est 4). Soient H et K deux 3-sous-groupes de Sylow distincts. L'intersection $H \cap K$ est un sous-groupe strict de H dont le cardinal divise 3, donc $H \cap K = \{e\}$. Les 3-sous-groupes de Sylow n'ont donc deux à deux qu'un seul élément en commun : l'identité. En conclusion, leur réunion est de cardinal 9, et G contient exactement 1 élément d'ordre 1 et 8 éléments d'ordre 3. Il y a donc au plus $12 - 8 = 4$ éléments de G dont l'ordre divise 4. Mais un 2-sous-groupe de Sylow de G a exactement 4 éléments d'ordre divisant 4. En conclusion, le groupe G ne peut avoir qu'un seul 2-sous-groupe de Sylow, ce qu'il fallait démontrer.

Exercice : (i) montrer que tout groupe d'ordre 35 est abélien (on s'inspirera de l'exemple (i) ci-dessus).

(ii) Soit G un groupe d'ordre 40. Montrer que soit les 2-Sylow soit les 5-Sylow de G sont distingués (on s'inspirera de l'exemple (ii) ci-dessus).