Licence Mathématiques 3ème année

COURS DE THEORIE DES GROUPES

Nicolas JACON

Université de Franche Comté

Table des matières

Chapitre 1

Notions fondamentales sur les Groupes

1.1 Premières définitions

Rappellons tout d'abord qu'une *loi de composition* sur un ensemble E est la donnée d'une application :

$$\begin{array}{rccc} * & : E \times E & \to & E \\ & (x, y) & \mapsto & x * y \end{array}$$

Définition 1.1.1 Un *groupe* G est un ensemble non vide muni d'une loi de composition $* : E \times E \to E$ vérifiant :

1. "$*$" est associative, c'est à dire :

$$\forall (x, y, z) \in E^3,\ (x * y) * z = x * (y * z).$$

2. "$*$" admet un élément neutre e_G, c'est à dire :

$$\exists e_G \in G,\ \forall x \in G,\ e_G * x = x * e_G = x.$$

3. Tout élément x de G admet un inverse noté x^{-1}, c'est à dire :

$$\forall x \in E,\ \exists x^{-1} \in E,\ x * x^{-1} = x^{-1} * x = e_G.$$

On dira de plus que le groupe $(G, *)$ est *commutatif* (ou *abélien*) si la loi de composition " $*$ " est commutative, c'est à dire :

$$\forall (x, y) \in E^2,\ x * y = y * x.$$

Par abus de notation, la plupart du temps, nous noterons G au lieu de $(G, *)$ pour désigner un groupe. Il faut néanmoins bien avoir en tête que la structure de groupe dépend des deux données : celle de l'ensemble G et celle de la loi de composition " $*$ ".

Remarquons que l'élément neutre e_G d'un groupe G est unique ainsi que l'inverse d'un élément. Traditionellement, la loi " $*$ " est souvent notée multiplicativement c'est à dire qu'on remplace " $*$ " par "." dans la définition ci-dessus (on omettra même parfois "." de sorte que $x.y$ sera noté xy), l'élément neutre est alors parfois noté 1. Cependant, dans le cas ou G est commutatif (et seulement dans ce cas !), on utilisera parfois une notation additive : on remplace alors $*$ par $+$ dans la définition ci-dessus, l'élément neutre est alors noté 0 et l'inverse d'un élément $x \in G$ est noté $-x$.

Exemple.

1. $\mathbb{R}$ (rep. $\mathbb{Q}$) muni de l'addition est un groupe commutatif.
2. $\mathbb{R}^*$ (rep. $\mathbb{Q}^*$) muni de la multiplication est un groupe commutatif.
3. $\mathbb{Z}$ muni de l'addition est un groupe commutatif.
4. $\mathbb{Z}^*$ muni de la multiplication n'est pas un groupe, 2 (par exemple) n'ayant pas d'inverse dans $\mathbb{Z}$.
5. Soit $E = \{1, \cdots, n\}$ alors l'ensemble des bijections de E dans E, muni de la loi de composition est un groupe (d'élement neutre l'identité), non commutatif en général, et appelé *groupe symétrique*. On le note $\mathfrak{S}_n$.
6. L'ensemble $GL_n(\mathbb{R})$ des matrices carrées $n \times n$ inversibles à coefficients dans $\mathbb{R}$ et muni de la multiplication est un groupe non commutatif en général. L'élément neutre est la matrice identité.
7. L'ensemble $M_n(\mathbb{R})$ des matrices carrées $n \times n$ à coefficients dans $\mathbb{R}$ et muni de la multiplication n'est pas un groupe en général (la matrice de $M_n(\mathbb{R})$ possedant tous ses coefficents nuls n'est pas inversible).
8. Plus généralement, si V est un espace vectoriel sur un corps k (=$\mathbb{R}$ ou $\mathbb{C}$), l'ensemble des bijections linéaires $GL_k(V)$ muni de la composition est un groupe, non commutatif en général.

Parmi les exemples ci-dessus, le groupe $\mathbb{Z}$ possède des propriétés particulières, entre autre une autre loi : la multiplication qui donne une structure plus riche à cet ensemble : c'est un anneau (cf le cours du 2ème semestre). Nous nous servirons dans la suite particulièrement des propriétés suivantes (il est ici tres important de les maîtriser).

– $\mathbb{Z}$ est muni de la division euclidienne c'est à dire que pour tout $n \in \mathbb{Z}$ et $m \in \mathbb{Z}^*$, il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tel que $0 \leq r < |m|$ et tel que :

$$n = mq + r.$$

– Pour $n \in \mathbb{Z}$ et $m \in \mathbb{Z}$ tous les deux non nuls, on note $\text{pgcd}(m,n)$, le plus grand (au sens de la divisibilité) entier positif divisant m et n. C'est aussi l'entier positif c vérifiant :

$$\forall x \in \mathbb{Z},\ x|m \text{ et } x|n \iff x|c.$$

Si $\text{pgcd}(m,n) = 1$ alors on dit que m et n sont premiers entre eux.
– Le théorème de Gauss : si a est premier avec b et divise bc alors il divise c.

Revenons à la structure de groupe. Donnons quelques règles et remarques relatives aux calculs dans un groupe G.

– On a $e_G^{-1} = e_G$ et pour tout $x \in G$, on a $(x^{-1})^{-1} = x$.
– Pour tout $(x,y,z) \in G^3$, on a :

$$xy = xz \Longrightarrow y = z \qquad \text{et} \qquad yx = zx \Longrightarrow y = z.$$

– Par la règle d'associativité, il est inutile de garder les parenthèses dans une expression. Ainsi, un produit quelconque d'éléments x_i $(i = 1, \cdots, n)$ de G sera noté $x_1 x_2 \cdots x_n$.
– Si x et y sont deux éléments de G alors $xyy^{-1}x^{-1} = e_G$. Il suit que $(xy)^{-1} = y^{-1}x^{-1}$ qui est différent de $x^{-1}y^{-1}$ en général (si le groupe n'est pas commutatif).
– Pour $x \in G$, on notera x^n l'élément $\underbrace{x \cdots xx}_{n \text{ fois}}$ si n est positif avec comme convention $x^0 = e_G$. Pour n négatif, on note $x^n = (x^{-1})^{-n}$. On a alors les regles de calculs :

$$x^m x^n = x^{m+n} \qquad \text{et} \qquad (x^n)^m = x^{mn}.$$

Définition 1.1.2 On dit qu'un groupe G est *fini* si il comporte un nombre fini d'éléments. *L'ordre* de G noté $o(G)$ est par définition le cardinal de G. Si G comporte un nombre infini d'éléments, on dit que G est d'ordre *infini*.

Exemple.

1. Le nombre de bijections de $\{1, \cdots, n\}$ dans $\{1, \cdots, n\}$ étant égal à $n!$, on en déduit que le groupe symétrique $\mathfrak{S}_n$ est un groupe fini d'ordre $n!$.
2. On considère l'ensemble $\{\overline{0}, \overline{1}\}$ muni d'une loi interne notée "+" et définie par $\overline{0} + \overline{0} = \overline{0}$, $\overline{0} + \overline{1} = \overline{1} + \overline{0} = \overline{1}$ et $\overline{1} + \overline{1} = \overline{0}$. Il est immédiat de vérifier qu'on obtient une structure de groupe commutatif d'ordre 2. Ce groupe sera noté $\mathbb{Z}/2\mathbb{Z}$ dans la suite.

1.2 Sous-groupes

Définition 1.2.1 Soit G un groupe et $*$ sa loi de composition. On dit que $H \subset G$ est un *sous-groupe* de G si :

1. H est non vide,
2. la restriction de la loi "$*$" à $H \times H$ prend ses valeurs dans H et induit une structure de groupe sur H.

Ainsi, un sous-groupe d'un groupe H est lui-même un groupe pour la loi de composition restreinte à H. Notons que l'ensemble des sous-groupes d'un groupe G est ordonné (partiellement) par l'inclusion. Une notation classique pour "H sous-groupe de G" est $H < G$.

Si G est un groupe alors G et $\{e_G\}$ (où e_G est l'élément neutre de G) sont des sous-groupes de G appelés *sous-groupes triviaux*. Les sous-groupes non triviaux de G sont appelés les *sous-groupes propres* de G et on notera alors $H \lneq G$.

Exemple.

1. $\mathbb{Z}$ est un sous-groupe de $\mathbb{Q}$ lui même sous-groupe de $\mathbb{R}$, lui même sous-groupe de $\mathbb{C}$ pour la loi d'addition.
2. Si $n \in \mathbb{N}_{>0}$, l'ensemble $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$. En effet, $n\mathbb{Z}$ est non vide et si $(x, y) \in n\mathbb{Z} \times n\mathbb{Z}$ alors $x + y \in n\mathbb{Z}$. La loi $+$ est associative, 0 est l'élement neutre et il est dans $n\mathbb{Z}$. De plus, si $x \in n\mathbb{Z}$, on a $-x \in n\mathbb{Z}$. On verra dans le chapitre suivant que ces sous-groupes sont en fait les seuls sous-groupes de $\mathbb{Z}$.
3. Si $n \in \mathbb{N}$, l'ensemble $C_n = \{z \in \mathbb{C} \mid z^n = 1\}$ des racines nièmes de l'unité est un sous-groupe de $\mathbb{C}$ muni de la multiplication. En effet, cet ensemble est non vide car $1 \in C_n$. De plus, si $x^n = 1$ et $y^n = 1$ pour x et y dans $\mathbb{C}$ alors $(xy)^n = 1$: la restriction de la loi de multiplication à $C_n \times C_n$ prend donc ses valeurs dans C_n. Elle est évidemment associative. L'élément neutre 1 est dans C_n et l'inverse d'un élément x dans C_n est dans C_n : si $x^n = 1$ alors $(x^n)^{-1} = 1 = (x^{-1})^n$.

La proposition suivante fournit une définition équivalente à la notion de sous-groupe.

Proposition 1.2.2 *Une partie H d'un groupe G est un sous-groupe de G si et seulement si :*

1. *H est non vide.*
2. *Pour tout x et y dans H, on a $xy^{-1} \in H$.*

Preuve.

- Supposons que H soit un sous-groupe de G. Alors, par définition H est non vide. Soit x et y deux éléments de H. Alors, x et y^{-1} sont dans H d'où $xy^{-1} \in H$.
- Supposons maintenant que H est non vide et vérifie la propriété suivante : $\forall (x, y) \in H^2,\ xy^{-1} \in H$.
  1. Montrons tout d'abord que e_G (l'élément neutre de G) est dans H. Comme H est non vide, il existe un élément x de H, alors on a par hypothèse $xx^{-1} \in H$ d'où $e_G \in H$.
  2. Montrons que si x est dans H, alors x^{-1} est dans H. Soit donc $x \in H$, alors, comme $e_G \in H$, on a par hypothèse $e_G x^{-1} \in H$ d'où $x^{-1} \in H$.
  3. Montrons enfin que si $(x, y) \in H^2$ alors $xy \in H$. Soit donc $(x, y) \in H^2$. Alors, $x \in H$ et $y^{-1} \in H$ d'après (2). Donc, par hypothèse, on a $x(y^{-1})^{-1} \in H$ mais $(y^{-1})^{-1} = y$ donc $xy \in H$.

  Ainsi, la loi de composition restreinte à $H \times H$ prend ses valeurs dans H par (3). Cette loi est associative (car G est un groupe), on a l'existence de l'élément neutre par (1) et de l'inverse par (2). On en déduit que H est bien un sous-groupe de G.

□

En général, pour montrer qu'un sous-ensemble H d'un groupe G est un sous-groupe, on montre tout d'abord que l'élément neutre e_G est dans H ce qui montre que H est non vide. La proposition suivante nous donne un exemple important de sous-groupe.

Proposition 1.2.3 *Si G est un groupe quelconque, l'ensemble suivant :*

$$Z(G) := \{z \in G \mid \forall g \in G,\ zg = gz\}$$

est un sous-groupe de G appelé le centre de G.

Preuve. On va utiliser la proposition 1.2.2. L'élément neutre e_G est dans H, en effet, pour tout $x \in G$, on a $xe_G = e_G x$. On en déduit que H est non vide. Soient maintenant x et y deux éléments de $Z(G)$, on veut montrer que xy^{-1} est dans $Z(G)$ c'est à dire que pour tout $z \in G$, on a $zxy^{-1} = xy^{-1}z$. Soit donc $z \in G$. Comme $x \in Z(G)$, on a $zx = xz$, on a donc $zxy^{-1} = xzy^{-1}$. Ensuite, comme $y \in Z(G)$ et comme $z^{-1} \in G$, il suit que $yz^{-1} = z^{-1}y$. En inversant de chaque coté de l'équation, on obtient $zy^{-1} = y^{-1}z$. Finalement, on conclut que $zxy^{-1} = xzy^{-1} = xy^{-1}z$ ce qu'il fallait montrer.

□

D'autres sous-groupes classiques d'un groupe G sont donnés par les exemples suivants :

Exemple.

1. Si G est un groupe quelconque, A une partie de G, l'ensemble suivant :

$$C_G(A) := \{x \in G \mid \forall a \in A,\ xa = ax\}$$

est un sous-groupe de G (à faire en exercice) appelé le *centralisateur* de A dans G.

2. Si G est un groupe quelconque, B une partie de G, l'ensemble suivant :

$$N_G(B) := \{x \in G \mid xBx^{-1} = B\}$$

est un sous-groupe de G (à faire aussi en exercice) appelé le *normalisateur* de de B dans G. Rappellons la notation $xBx^{-1} := \{xbx^{-1} \mid b \in B\}$.

Proposition 1.2.4 *L'intersection d'une famille quelconque de sous-groupes de G est un sous groupe de G.*

Preuve. Soit G un groupe et $\{H_i\}_{i\in I}$ une famille de sous-groupes de G. On veut montrer que $H := \bigcap_{i\in I} H_i$ est un sous-groupe de G. On utilise pour cela la Prop. 1.2.2.

1. H est non vide car l'élément neutre e_G de G est dans tous les H_i pour $i \in I$, il est donc dans H.
2. Soit $(x, y) \in H^2$. On veut montrer que xy^{-1} est un élément de H. Il suffit de montrer que pour tout $i \in I$, $xy^{-1} \in H_i$. Soit donc $i \in I$, alors x et y sont des éléments de H_i (puisqu'ils sont dans H). H_i étant un sous-groupe de G, on a alors $xy^{-1} \in H_i$ d'après la Prop. 1.2.2. Donc $xy^{-1} \in H$.

□

Attention ! ! ! La réunion de deux sous-groupes n'est pas toujours un sous-groupe. Par exemple, $2\mathbb{Z}$ et $3\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$ mais $2\mathbb{Z} \cup 3\mathbb{Z}$ n'en est pas un : 2 et 3 sont dans $2\mathbb{Z} \cup 3\mathbb{Z}$ mais pas $2 + 3 = 5$, la loi $+$ n'est donc pas interne dans $2\mathbb{Z} \cup 3\mathbb{Z}$! ! !

1.3 Homorphismes de groupes

Définition 1.3.1 Soient G et H deux groupes. Une application $f : G \to H$ est un *homomorphisme* (ou *morphisme*) de groupes si et seulement si elle

vérifie :

$$\forall (x,y) \in G \times G,\ f(x.y) = f(x).f(y).$$

On notera $\mathrm{Hom}(G,H)$ l'ensemble des homomorphismes de G dans H.

Un homomorphisme de groupes est donc une application "compatible" avec les lois de compositions induites par les structures de groupes. Attention encore aux notations de ces lois : dans la définition ci-dessus, les lois internes sont notés multiplicativement.

Exemple.

1. Si G est un groupe, l'application identité est un homomorphisme de groupe (de G dans G).
2. Si G est un groupe et H un sous-groupe de G alors l'application suivante :
$$\begin{array}{rccc} f: & H & \to & G \\ & x & \mapsto & x \end{array}$$
est un homomorphisme de groupes injectif (appelé *injection canonique*).
3. Soit $n \in \mathbb{Z}$ alors l'application suivante :
$$\begin{array}{rccc} f: & \mathbb{Z} & \to & \mathbb{Z} \\ & m & \mapsto & nm \end{array}$$
est un homomorphisme de groupes. En effet, si $(m,m') \in \mathbb{Z}^2$, on a $f(m+m') = nm + nm' = f(m) + f(m')$ (structures additives !!)
4. L'application
$$\begin{array}{rccc} \det: & GL_n(\mathbb{C}) & \to & \mathbb{C}^* \\ & M & \mapsto & \det(M) \end{array}$$
est un homomorphisme entre les groupes $GL_n(\mathbb{C})$ et $\mathbb{C}^*$ (structures multiplicatives).

Remarque 1.3.2 Remarquons que si $f : G \to G'$ est un homomorphisme de groupes, si e_G est l'élément neutre de G et $e_{G'}$ celui de G', on a $f(e_G) = e_{G'}$. En effet, $f(e_G.e_G) = f(e_G).f(e_G)$ d'une part et comme $e_G.e_G = e_G$, on obtient, $f(e_G) = f(e_G).f(e_G)$ d'où $f(e_G) = e_{G'}$.

De plus, si x est un élément de G, on a $e_{G'} = f(e_G) = f(x.x^{-1}) = f(x).f(x^{-1})$ d'où $f(x^{-1}) = f(x)^{-1}$.

Définition 1.3.3 Un homomorphisme de groupes bijectif est appelé un *isomorphisme*. On dit que G et G' sont *isomorphes* si il existe un isomorphisme de G dans G'. On note alors $G \simeq G'$. Un isomorphisme de G dans G est appelé un *automorphisme*.

Exemple.

1. Si G est un groupe, l'application identité est un isomorphisme de groupe (de G dans G) donc un automorphisme.
2. On considère le groupe $\mathbb{R}$ muni de l'addition et l'ensemble $\mathbb{R}_+^*$ qui est un groupe relativement à la loi de multiplication. Soit l'application exponentielle $\exp : \mathbb{R} \to \mathbb{R}_+^*$. C'est un homomorphisme de groupes car pour tout $(a, b) \in \mathbb{R}^2$, on a $\exp(a + b) = \exp(a)\exp(b)$. Cet homomorphisme étant bijectif, c'est même un isomorphisme de groupes.

Bien sûr, si G et G' sont isomorphes, G' et G le sont aussi. Les propriétés des groupes sont "invariantes" par isomorphisme c'est à dire que si $G \simeq G'$, G possède une même propriété de groupes si et seulement si G' la possède aussi. Par exemple, on vérifie facilement que si $G \simeq G'$, G est commutatif si et seulement si G' est commutatif. Ainsi, en théorie des groupes, on cherche à classifier les groupes à isomorphisme près.

Proposition 1.3.4 *Soit $f : G \to G'$ un homomorphisme de groupes. Alors f est un isomorphisme si et seulement si il existe $g : G' \to G$ un homomorphisme de groupes tel que $f \circ g = Id_{G'}$ et $g \circ f = Id_G$.*

Preuve. Si il existe $g : G' \to G$ un homomorphisme de groupes tel que $f \circ g = \mathrm{Id}_{G'}$ et $g \circ f = \mathrm{Id}_G$ alors f admet une application inverse g et donc f est une bijection. f est donc un isomorphisme.

Réciproquement, si f est un isomorphisme alors f est une bijection donc f admet une application inverse g. Montrons que g est un homomorphisme de groupes. Soit x' et y' deux éléments de G', on veut montrer que :

$$g(x'y') = g(x')g(y').$$

Il existe des (uniques) éléments x et y de G tels que $f(x) = x'$ et $f(y) = y'$. Alors, en utilisant le fait que f est un homomorphisme de groupes, il suit :

$$g(x'y') = g(f(x)f(y)) = g(f(xy)) = xy = g(x')g(y').$$

Donc g est bien un homomorphisme de groupes tels que $f \circ g = \mathrm{Id}_{G'}$ et $g \circ f = \mathrm{Id}_G$.

□

Proposition 1.3.5 *Soient G, G' et G'' trois groupes.*

1. *Si $f : G \to G'$ et $g : G' \to G''$ sont deux homomorphismes de groupes. Alors $g \circ f$ est un homomorphisme de groupes.*
2. *Si $f : G \to G'$ est un isomorphisme de groupes alors $f^{-1} : G \to G'$ est un isomorphisme de groupes.*

3. *L'ensemble* $\mathrm{Aut}(G)$ *des automorphismes de* G *est un groupe pour la loi interne donné par la composition* $\circ$.

Preuve. On prouve (1). Soit $(x, y) \in G^2$, alors $f(xy) = f(x)f(y)$ car f est un homomorphisme de groupes. On obtient $g(f(xy)) = g(f(x)f(y))$. Comme g est un homomorphisme de groupes, il suit $g(f(xy)) = g(f(x))g(f(y))$ ce qu'il fallait montrer.

On prouve (2). La proposition précédente nous montre que $f^{-1} : G \to G'$ est un homomorphisme de groupes. Cet homomorphisme possède un homomorphisme inverse qui est f donc c'est un isomorphisme.

Ces 2 propriétés nous fournissent la preuve de l'existence d'une structure de groupe sur $\mathrm{Aut}(G)$ avec loi interne donnée par la composition, qui est bien associative. L'élément neutre est l'identité.

□

Définition 1.3.6 Soit $f : G \to G'$ un homomorphisme. Le *noyau* de f noté $\mathrm{Ker}\, f$ ou $\mathrm{Ker}(f)$ est l'ensemble $\{x \in G; f(x) = e_{G'}\} \subset G$. L'*image* de f noté $\mathrm{Im}\, f$ ou $\mathrm{Im}(f)$ est l'ensemble $f(G) = \{f(x) \in G' \mid x \in G\} \subset G'$.

Proposition 1.3.7 *Soit* $f : G \longrightarrow G'$ *un homomorphisme de groupes.*

1. *Si* H *est un sous-groupe de* G, $f(H)$ *est un sous-groupe de* G'. *En particulier,* $\mathrm{Im}(f)$ *est un sous-groupe de* G.
2. *Si* H *est un sous-groupe de* G', $f^{-1}(H) := \{x \in G \mid f(x) \in H\}$ *est un sous-groupe de* G. *En particulier,* $\mathrm{Ker}(f)$ *est un sous-groupe de* G.

Preuve. On prouve (1). Tout d'abord, $f(H)$ est non vide car H est non vide. Soit $y_1 \in f(H)$ et $y_2 \in f(H)$. On veut montrer que $y_1 y_2^{-1} \in f(H)$. Il existe $x_1 \in H$ et $x_2 \in H$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$. De plus, d'après la remarque 1.3.2, on a $y_2^{-1} = f(x_2^{-1})$. Comme f est un homomorphisme de groupes, on obtient :

$$y_1 y_2^{-1} = f(x_1)f(x_2^{-1}) = f(x_1 x_2^{-1}).$$

Or, H est un sous-groupe de G, on a donc $x_1 x_2^{-1} \in H$ donc $y_1 y_2^{-1} \in f(H)$. Donc $f(H)$ est un sous-groupe de G'. En particulier $f(G) = \mathrm{Im}(f)$ est un sous-groupe de G'.

On prouve (2). Tout d'abord $f^{-1}(H)$ est non vide car $f(e_G) = e_{G'} \in H$ d'après la remarque 1.3.2. On a donc $e_G \in f^{-1}(H)$. Soit $y_1 \in f^{-1}(H)$ et $y_2 \in f^{-1}(H)$. On veut montrer que $y_1 y_2^{-1} \in f^{-1}(H)$. On a par définition $f(y_1) \in H$ et $f(y_2) \in H$ donc $f(y_1)f(y_2)^{-1} \in H$ car H est un sous-groupe de G. Comme f est un homomorphisme de groupes, on a :

$$f(y_1)f(y_2)^{-1} = f(y_1)f(y_2^{-1}) = f(y_1 y_2^{-1}).$$

Donc $f(y_1 y_2^{-1}) \in H$ ce qui prouve que $y_1 y_2^{-1} \in f^{-1}(H)$ donc $f^{-1}(H)$ est un sous-groupe de G. En particulier $f^{-1}(\{e_{G'}\}) = \mathrm{Ker}(f)$ est un sous-groupe de G car $\{e_{G'}\}$ est un sous-groupe de G'.

□

Théorème 1.3.8 *Soit $f : G \to G'$ un homomorphisme entre G et G'. Alors,*

1. *f est injective si et seulement si $\mathrm{Ker}(f)$ est réduit à l'élément neutre de G.*
2. *f est surjective si et seulement si $\mathrm{Im}(f) = G'$*

Preuve. On prouve (1). Supposons f injective. Soit $x \in \mathrm{Ker}(f)$ alors $f(x) = e_{G'}$. Mais on sait que $f(e_G) = e_{G'}$. Il suit donc $x = e_G$ donc $\mathrm{Ker}(f) = \{e_G\}$. Réciproquement, si x et y sont deux éléments de G tels que $f(x) = f(y)$ alors $f(xy^{-1}) = e_{G'}$ car f est un homomorphisme donc $xy^{-1} = e_G$ et donc $x = y$. Donc f est injective. (2) est évident via la définition de $\mathrm{Im}(f)$.

□

Signalons également le résultat très utile suivant. Soit G et G' deux ensembles finis et $f : G \to G'$ une application, alors :

1. Si f est bijective, G et G' ont même cardinal.
2. Si G et G' ont même cardinal et si f est surjective, f est bijective.
3. Si G et G' ont même cardinal et si f est injective, f est bijective.

En théorie des groupes, ces remarques se traduisent de la façon suivante :

Proposition 1.3.9 *Soit G et G' deux groupes finis et $f : G \to G'$ un homomorphisme de groupes, alors :*

1. *Si f est un isomorphisme, G et G' ont même ordre.*
2. *Si G et G' ont même ordre et si f est surjective, f est un isomorphisme.*
3. *Si G et G' ont même ordre et si f est injective, f est un isomorphisme.*

1.4 Sous-groupes engendrés

Définition 1.4.1 Soit G un groupe et S une partie de G. L'intersection de tous les sous-groupes contenant S est appelé le *sous-groupe engendré par S*. Il est noté $< S >$ et c'est le plus petit (au sens de l'inclusion) sous-groupe contenant S.

Ainsi $< S >= H$ si et seulement si H est un sous-groupe de G vérifiant :

1. $S \subset H$,
2. Si $S \subset H'$ pour un sous-groupe H' de G alors $H \subset H'$.

Si S est une partie d'un groupe G. On notera :

$$S^{-1} := \{x^{-1} \mid x \in S\} \subset G.$$

Proposition 1.4.2 *Soit G un groupe et S une partie de G.*

1. *Si $S = \emptyset$ alors $< S >= \{e_G\}$.*
2. *Si $S \neq \emptyset$ alors on a :*

$$< S >= \{x = x_1 x_2 \cdots x_n \mid \forall i \in \{1, \cdots, n\},\ x_i \in S \cup S^{-1},\ n \in \mathbb{N}\}.$$

Preuve. (1) est évident car $\{e_G\}$ est un sous-groupe de G, il contient $\emptyset$ et est contenu dans tout sous-groupe de G. Montrons (2). Il faut vérifier que l'ensemble $H = \{x = x_1 x_2 \cdots x_n \mid \forall i \in \{1, \cdots, n\},\ x_i \in S \cup S^{-1},\ n \in \mathbb{N}\}$ est le plus petit sous-groupe contenant S.

1. H est bien un sous-groupe de G. En effet, il est non vide car S est non vide. De plus, si $x \in H$ et $y \in H$ alors il existe une suite d'éléments $x_i \in S \cup S^{-1}$ avec $i \in \{1, \cdots, n\}$ $(n \in \mathbb{N})$ et une suite $y_j \in S \cup S^{-1}$ avec $j \in \{1, \cdots, m\}$ $(m \in \mathbb{N})$ telles que $x = x_1 x_2 \cdots x_n$ et $y = y_1 y_2 \cdots y_m$. Alors on a $xy^{-1} = x_1 \cdots x_n (y_1 \cdots y_m)^{-1} = x_1 \cdots x_n y_m^{-1} \cdots y_1^{-1}$ avec $x_i \in S \cup S^{-1}$ pour $i \in \{1, \cdots, n\}$ et $y_j^{-1} \in S \cup S^{-1}$ avec $j \in \{1, \cdots, m\}$. On a donc $xy^{-1} \in H$. Par la Proposition 1.2.2, H est bien un sous-groupe de G.
2. H contient S : c'est évident par la définition de H.
3. Soit H' un sous-groupe de G contenant S. On veut montrer que $H \subset H'$. Soit donc $x = x_1 \cdots x_n \in H$ avec $x_i \in S \cup S^{-1}$ pour $i \in \{1, \cdots, n\}$ $(n \in \mathbb{N})$. Soit $i \in \{1, \cdots, n\}$, si $x_i \in S$ alors x_i est dans H' par hypothèse. Sinon, $x_i \in S^{-1}$ mais alors $x_i^{-1} \in S$ donc $x_i^{-1} \in H'$ par hypothèse et comme H' est un sous-groupe $(x_i^{-1})^{-1} = x_i \in H'$. Il suit $x_i \in H'$ pour tout $i \in \{1, \cdots, n\}$. Mais comme H' est un sous-groupe, le produit d'éléments de H' est dans H' donc $x = x_1 \cdots x_n \in H'$. On en déduit donc $H \subset H'$.

Donc H est le plus petit sous-groupe de G contenant H, on en déduit donc $H =< S >$.

□

Définition 1.4.3 Soit G un groupe et S une partie de G. Si $G =< S >$, on dira que S est une *partie génératrice* de G (ou que S engendre G). On dira que G est de *type fini* si une partie finie de G engendre G.

Exemple. :

1. Le groupe $\mathbb{Z}$ muni de l'addition est engendré par un élément : 1. En effet si $n \in \mathbb{Z}$, alors $n = \underbrace{1+1+\cdots+1}_{n \text{ fois}}$ si n est positif et $n = \underbrace{-1-1-\cdots-1}_{-n \text{ fois}}$ si n est négatif. Donc $\mathbb{Z}$ est de type fini.
2. Soit C_n le groupe des racines nième de l'unité muni de la multiplication. Alors, C_n est engendré par l'élément $\exp(\frac{2i\pi}{n})$. En effet, si $z \in C_n$ alors $z^n = 1$ donc il existe $k \in \{1, \cdots n-1\}$ tel que $z = \exp(\frac{2ik\pi}{n}) = \underbrace{\exp(\frac{2i\pi}{n}) \cdots \exp(\frac{2i\pi}{n})}_{k \text{ fois}}$. Donc C_n est de type fini.

Si G est un groupe et g_1, g_2, ..., g_n des éléments de G on notera souvent $< g_1, \cdots, g_n >$ au lieu de $< \{g_1, \cdots, g_n\} >$ pour le sous-groupe engendré par la partie $\{g_1, \cdots, g_n\}$ de G.

Remarque 1.4.4 Si G est un groupe alors $G =< G >$. En particulier tout groupe fini est de type fini. La réciproque est fausse : $\mathbb{Z}$ est un groupe infini ... de type fini.

Bien sûr, si G est de type fini, il n'y a pas unicité de la partie génératrice : $\mathbb{Z}$ est engendré par $\mathbb{Z}$ mais aussi par par $\{1\}$ par exemple.

Définition 1.4.5 Soit G un groupe et soit x un élément de G. On dit que x est d'*ordre fini* si il existe $n \in \mathbb{N}$ tel que $x^n = e_G$. On note alors

$$o(x) = \min(n \in \mathbb{N}_{>0} \mid x^n = e_G\},$$

l'*ordre* de l'élément x.

Exemple.

1. Considérons le groupe C_n des racines nièmes de l'unité alors $\exp(\frac{2i\pi}{n})$ est d'ordre n.
2. Soit le groupe $GL_2(\mathbb{C})$ des matrices inversibles à 2 lignes et 2 colonnes. On considère la matrice $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. On a $A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $A^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. La matrice A est donc d'ordre 4 dans $GL_2(\mathbb{C})$.

Proposition 1.4.6 *Soit G un groupe et soit x un élément d'ordre fini dans G. Alors le sous-groupe $< x >$ est fini et :*

$$o(x) = o(< x >).$$

Ainsi, le sous-groupe $< x >$ comporte $o(x)$ éléments. De plus,

$$< x >= \{e_G, x, x^2, \cdots, x^{n-1}\}.$$

Preuve. Soit x un élément d'ordre fini dans un groupe G. On note $n = o(x)$. Si $n = 1$ alors $x = e_G$ et le résultat est evident. Supposons donc $n > 1$.

Nous allons tout d'abord montrer que $\{e_G, x, x^2, \cdots, x^{n-1}\} =< x >$. L'inclusion $\subset$ est immédiate car $< x >= \{x^k \mid k \in \mathbb{Z}\}$. Soit $a \in < x >$. Il existe $k \in \mathbb{Z}$ tel que $a = x^k$. On effectue la division euclidienne de k par n. Il existe $q \in \mathbb{Z}$ et r tel que $0 \leq r < n$ tels que $k = nq + r$. Alors :

$$x^k = x^{nq+r} = (x^n)^q x^r = e_G^q x^r = x^r$$

Donc $a = x^r \in \{e, x, x^2, \cdots, x^{n-1}\}$. Il reste à montrer que $\{e_G, x, x^2, \cdots, x^{n-1}\}$ possède n éléments distincts. Supposons qu'il existe i et j tels que $0 \leq i < j < n$ et tels que $x^i = x^j$. Alors, on a $x^{j-i} = e_G$ avec $0 < j - i < n$ ce qui est une contradiction car x est d'ordre n. Ainsi $\{e_G, x, x^2, \cdots, x^{n-1}\}$ possède n élément distincts et on a bien $o(x) = o(< x >)$.

□

Notons en particulier le fait remarquable suivant : si $x^s = e_G$ dans un groupe G alors $o(x)$ divise s. En effet, toujours en utilisant la division euclidienne de s par $o(x)$, on a $s = o(x)k + r$ avec $r \in \{0, 1, \cdots, o(x) - 1\}$ d'où $x^r = e_G$ et donc $r = 0$ par la définition de l'ordre (car $r < o(x)$).

Définition 1.4.7 On dit qu'un groupe G est *monogène* si il contient une partie génératrice à un élément. Un groupe est dit *cyclique* si il est monogène et fini.

Théorème 1.4.8 (Classification des groupes monogènes) *Soit G un groupe monogène.*

1. *Si G est infini, G est isomorphe à $\mathbb{Z}$.*
2. *Si G est fini d'ordre n, G est isomorphe à $C_n := \{z \in \mathbb{C} \mid z^n = 1\}$.*

Preuve. Soit G un groupe monogène et soit x un générateur de G.

1. Si G est infini. Soit $f : \mathbb{Z} \to G$ défini par $f(n) = x^n$ pour tout $n \in \mathbb{Z}$. f est un morphisme de groupes car $f(n + m) = x^n x^m = f(n)f(m)$ pour tout $(n, m) \in \mathbb{Z}^2$. f est surjective car tout élément de G est de

la forme x^n pour $n \in \mathbb{N}$ car G est monogène. Enfin, f est injective : supposons qu'il existe $n \in \mathbb{Z}$ tel que $f(n) = e_G$. On obtient alors $x^n = e_G$. Supposons $n \neq 0$, il existe $m \in \mathbb{N}_{>0}$ tel que $x^m = e_G$ (ce m étant égale à n ou $-n$ selon que n est positif ou négatif). D'après la proposition précédente, x serait alors d'ordre fini ce qui est absurde car G est infini. Donc $\mathrm{Ker}(f) = \{e_G\}$ et donc f est injective. Il suit que f est un isomorphisme.

2. Si G est fini. Alors, on a vu dans la proposition précédente que

$$G = \{e, x, x^2, \cdots, x^{n-1}\},$$

où $n = o(x)$. Posons $\omega = \exp(\frac{2i\pi}{n})$. On sait que

$$C_n := \{1, \omega, \cdots, \omega^{n-1}\}.$$

On définit alors l'application $h : C_n \to G$ défini par $h(\omega^k) = x^k$ pour tout $k \in \{0, 1, \cdots, n-1\}$. Montrons que f est un homomorphisme de groupes. Soit $(k, l) \in \{0, 1, \cdots, n-1\}^2$.
– Si $k + l \leq n - 1$. Alors :

$$h(\omega^k \omega^l) = h(\omega^{k+l}) = x^{k+l} = x^k x^l = h(\omega^k) h(\omega^l).$$

– Si $k + l > n - 1$ alors $0 \leq k + l - n \leq n - 1$. Alors :

$$h(\omega^k \omega^l) = h(\omega^{k+l}\omega^{-n}) = h(\omega^{k+l-n}) = x^{k+l}x^{-n} = x^k x^l = h(\omega^k) h(\omega^l),$$

car $\omega^n = 1$ et $x^n = e_G$.
Donc f est un homomorphisme de groupes. De plus, f est surjective par définition de G donc bijective car les 2 groupes ont même ordre (voir la proposition 1.3.9).

Proposition 1.4.9 *Tout groupe monogène est commutatif.*

Preuve. Ceci résulte de la classification des groupes monogènes et du fait que $\mathbb{Z}$ et C_n sont des groupes commutatifs.

□

Exemple. On considère le groupe $\mathfrak{S}_3$ des bijections de $\{1, 2, 3\}$ dans $\{1, 2, 3\}$. Ce groupe possède 6 éléments. $\sigma \in \mathfrak{S}_3$ est entièrement déterminé par la donnée de $\sigma(1) \in \{1, 2, 3\}$, $\sigma(2) \in \{1, 2, 3\} \setminus \{\sigma(1)\}$ et $\sigma(3) \in \{1, 2, 3\} \setminus \{\sigma(1), \sigma(2)\}$. On notera alors :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix}$$

Les 6 éléments de $\mathfrak{S}_3$ sont :

$$Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Déjà $\mathfrak{S}_3$ n'est pas monogène car il n'est pas commutatif : $\sigma_1 \circ \sigma_2 = \sigma_4$ et $\sigma_2 \circ \sigma_1 = \sigma_5$. On vérifie que l'identité est d'ordre 1, σ_1, σ_2 et σ_3 sont d'ordre 2, σ_4 et σ_5 d'ordre 3.

En fait, $\mathfrak{S}_3$ est engendré par σ_1 et σ_2. En effet, on vérifie que $\sigma_4 = \sigma_1 \circ \sigma_2$, $\sigma_5 = \sigma_2 \circ \sigma_1$ et $\sigma_3 = \sigma_4 \circ \sigma_1 = \sigma_1 \circ \sigma_2 \circ \sigma_1$.

Chapitre 2

Groupes quotients

2.1 Relations d'équivalence

Dans cette première partie, on étudie les intéractions entre un groupe G et ses sous-groupes. On va pour cela définir une certaine relation d'équivalence.

Rappellons qu'une relation d'équivalence $\mathcal{R}$ sur un ensemble S est une relation binaire possédant les propriétés suivantes :

1. $\mathcal{R}$ est reflexive, c'est à dire :

$$\forall x \in S,\ x\mathcal{R}x.$$

2. $\mathcal{R}$ est symétrique, c'est à dire :

$$\forall (x,y) \in S^2,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x.$$

3. $\mathcal{R}$ est transitive, c'est à dire :

$$\forall (x,y,z) \in S^3,\ (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z.$$

Nous allons maintenant définir deux relations d'équivalence sur un groupe arbitraire à l'aide de la loi interne définie sur celui-ci.

Proposition 2.1.1 *Soient G un groupe et H un sous-groupe de G. On définit les deux relations ci-dessous :*
- *$x\mathcal{R}_1 y$ si et seulement si $xy^{-1} \in H$,*
- *$x\mathcal{R}_2 y$ si et seulement si $y^{-1}x \in H$.*

Alors, $\mathcal{R}_1$ et $\mathcal{R}_2$ sont des relations d'équivalences.

Preuve. On fait la démonstration pour $\mathcal{R}_1$, la démonstration pour $\mathcal{R}_2$ étant identique.

1. $\mathcal{R}_1$ est reflexive. Soit $x \in G$ alors $xx^{-1} = e_G \in H$ car H est un sous-groupe de G. Donc on a $x\mathcal{R}_1 x$.
2. $\mathcal{R}_1$ est symétrique. Soit $x \in G$ et $y \in G$ tels que $x\mathcal{R}_1 y$ alors $xy^{-1} \in H$. Il suit $(xy^{-1})^{-1} \in H$ et donc $yx^{-1} \in H$. Donc on a $y\mathcal{R}_1 x$.
3. $\mathcal{R}_2$ est transitive. Soit $(x, y, z) \in G^3$ tel que $x\mathcal{R}_1 y$ et $y\mathcal{R}_1 z$. On a donc $xy^{-1} \in H$ et $yz^{-1} \in H$. Le produit de ces deux éléments est donc dans H. On obtient donc $xy^{-1}yz^{-1} = xz^{-1} \in H$. Ceci implique $x\mathcal{R}_1 z$.

□

Définition 2.1.2 Soit G un groupe et H un sous-groupe de G.
- La relation $\mathcal{R}_1$ est appelée *congruence à droite modulo* H. L'ensemble des classes d'équivalence est noté $H \setminus G$.
- La relation $\mathcal{R}_2$ est appelée *congruence à gauche modulo* H. L'ensemble des classes d'équivalence est noté G/H.

Le cardinal de l'ensemble G/H est appelée *l'indice* de H dans G et il est noté $[G : H]$.

Proposition 2.1.3 *Soit G un groupe et H un sous-groupe de G. Les classes de congruence à droite et à gauche d'un élément $x \in G$ modulo H sont respectivement égales à Hx et xH.*

Preuve. Soit $x \in G$ et soit $y \in G$ un élément dans la classe de congruence à droite modulo H de x. On a donc $y\mathcal{R}_1 x$ c'est à dire $yx^{-1} \in H$. Il suit donc $y \in Hx$. Réciproquement, si $y \in Hx$ alors $yx^{-1} \in H$ et donc $y\mathcal{R}_1 x$ donc y est un élément dans la classe de congruence à droite modulo H de x. La démonstration pour $\mathcal{R}_2$ est identique.

□

Ces remarques nous permettent de démontrer le résultat important suivant.

Théorème 2.1.4 (Théorème de Lagrange) *Soit G un groupe fini et H un sous-groupe de G. Alors on a :*

$$o(G) = [G : H]o(H).$$

En particulier, l'ordre de H divise l'ordre de G.

Preuve. La proposition précédente nous montre que le cardinal d'une classe d'équivalence de G/H est égale au cardinal de xH c'est à dire à l'ordre de H. Les classes d'équivalence réalisent une partition de G c'est à dire que tout élément de G est dans une et une seule classe d'équivalence (c'est une propriété générale des classes d'équivalence). On a donc $[G : H]$ classes

d'équivalence, chacune de cardinal $o(H)$. Il en résulte que le cardinal de G est égal à $[G : H]o(H)$ d'où le résultat.

□

On en déduit quelques résultats remarquables.

Corollaire 2.1.5 *Soit G un groupe fini et $x \in G$ alors $o(x)$ divise $o(G)$ et on a $x^{o(G)} = e_G$.*

Preuve. Le sous-groupe $< x >$ est d'ordre $o(x)$ et d'après la proposition précédente, cet ordre divise l'ordre de G. On note $p := [G :< x >]$. On a donc $o(G) = po(x)$. Par définition de l'ordre, on a $x^{o(x)} = e$ donc $x^{o(G)} = (x^{o(x)})^p = e_G$.

□

Corollaire 2.1.6 *Un groupe fini G dont l'ordre est un nombre premier est cyclique.*

Preuve. Soit x un élément de G distinct de l'élément neutre. Ceci implique que l'ordre de x est plus grand que 1. D'après le corollaire précédent, cet ordre divise l'ordre de G. Cet ordre étant premier, on en déduit que $o(x) = o(G)$. Le sous-groupe $< x >$ de G comporte donc $o(G)$ éléments distincts, il est donc égale à G. Donc G est monogène et fini, G est donc cyclique.

□

2.2 Sous-groupes normaux

Avant d'étudier plus précisement les structures de ces classes de congruence attachées à un sous-groupe, nous nous intéressons à certains sous-groupes particuliers.

Définition 2.2.1 Soit G un groupe, un sous-groupe H est dit *normal* (ou *distingué*) si et seulement si :

$$\forall x \in G,\ xHx^{-1} = H.$$

On note alors $H \lhd G$.

On rappelle que $xHx^{-1} := \{xgx^{-1} \in G \mid g \in H\}$.

Proposition 2.2.2 *Soient G un groupe et H un sous-groupe de G. Alors :*

$$H \lhd G \iff \forall x \in G,\ xHx^{-1} \subset H.$$

Preuve. Le sens $\Rightarrow$ est trivial. Réciproquement, supposons $\forall x \in G,\ xHx^{-1} \subset H$. Soit $x \in G$, on veut montrer $xHx^{-1} = H$. On a déjà $xHx^{-1} \subset H$ par hypothèse. Soit $y \in H$ alors $x^{-1}yx \in x^{-1}H(x^{-1})^{-1} \subset H$ par hypothèse. Donc $y = x(x^{-1}yx)x^{-1} \in xHx^{-1}$. On a donc $H \subset xHx^{-1}$.

□

Exemple.

1. Si G est un groupe, ses deux sous-groupes triviaux, G et $\{e_G\}$, sont normaux.
2. Si G est un groupe commutatif, il est clair que tout sous-groupe de G est normal.
3. Soit $G := GL_2(\mathbb{R})$ le groupe des matrices inversibles à deux lignes et deux colonnes. On considère $K := \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \ | a \in \mathbb{R} \right\}$. On montre facilement que K est un sous-groupe de G. Posons $x = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in G$. Alors on a $x^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$. Soit $a \in \mathbb{R}$, alors :

$$x \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} x^{-1} = \begin{pmatrix} 1-a & a \\ -a & a+1 \end{pmatrix}.$$

   Cet élément n'étant clairement pas contenu dans K en général, K n'est pas normal.

Proposition 2.2.3 *Soient G et G' deux groupes et soit $f : G \to G'$ un morphisme de groupes.*

1. *Soit $H' \lhd G'$, alors $f^{-1}(H') \lhd G$. En particulier* $\mathrm{Ker}(f) \lhd G$.
2. *Soit $H \lhd G$ et supposons que f est surjective alors $f(H) \lhd G'$.*

Preuve.

1. Soit $H' \lhd G'$. On sait déjà que $f^{-1}(H')$ est un sous-groupe de G (voir la proposition 1.3.7). Montrons que ce sous-groupe est normal. Soit $x \in G$, on veut montrer que $xf^{-1}(H)x^{-1} \subset f^{-1}(H)$. Soit $y \in f^{-1}(H)$. Il faut montrer que $xyx^{-1} \in f^{-1}(H)$ c'est à dire que $f(xyx^{-1}) \in H$. Or, comme f est un morphisme de groupes, on a $f(xyx^{-1}) = f(x)f(y)f(x)^{-1}$. Comme $f(y) \in H$ et que H est normal, on conclut que $f(x)f(y)f(x)^{-1} \in H$. Donc $f^{-1}(H')$ est un sous-groupe normal de G.
2. Soit $H \lhd G$ et supposons que f est surjective. On sait déjà que $f(H)$ est un sous-groupe de G'. Montrons qu'il est normal. Soit $x \in G'$. On veut

montrer $xf(H)x^{-1} \subset H$. Comme f est surjective, il existe $z \in G$ tel que $f(z) = x$. Alors, $f(z^{-1}) = x^{-1}$. Soit $y \in H$, on a $xf(y)x^{-1} = f(zyz^{-1})$ car f est un homomorphisme de groupes. Comme H est normal on sait que $zyz^{-1} \in H$. Il suit $xf(y)x^{-1} \in f(H)$. $f(H)$ est donc bien un sous-groupe normal de G'.

□

Exemple. Soit $GL_n(\mathbb{C})$ le groupes des matrices à n lignes et n colonnes à coefficients dans $\mathbb{C}$. Soit $SL_n(\mathbb{C}) := \{M \in GL_n(\mathbb{C}) \mid \det(M) = 1\}$. On a $SL_n(\mathbb{C}) = \mathrm{Ker}(\det)$ (on rappelle que le déterminant est un morphisme de $GL_n(\mathbb{C})$ dans $\mathbb{C}^*$). Il suit que $SL_n(\mathbb{C})$ est un sous-groupe normal de $GL_n(\mathbb{C})$ appelée le *groupe spécial linéaire*.

2.3 Groupes quotients

Dans la première section de ce chapitre, à un groupe G et un sous-groupe H, on a associé un certain ensemble G/H, ensemble des classes de congruence à gauche modulo H. On se pose maintenant la question suivante : est-il possible de mettre une structure de groupe sur cet ensemble qui serait "compatible" avec la structure de groupe sur G ? le théorème suivant répond par l'affirmative à ce problème lorsque $H \lhd G$. Das ce cas, les classes de congruence à droite où à gauche sont les mêmes puisque $xH = Hx$ pour tout $x \in G$. On parlera donc seulement ici de classe de congruence et on note G/H l'ensemble de ses classes.

Théorème 2.3.1 *Soit G un groupe et soit $H \lhd G$. Soit $\pi : G \to G/H$ la surjection canonique qui associe à un élément de G sa classe de congruence modulo H. Alors, il existe sur G/H une unique structure de groupe tel que π soit un morphisme de groupe. Le groupe ainsi obtenu est appelé le groupe quotient G/H.*

Preuve. Soit $x \in G$. La surjection canonique π est définie par $\pi(x) = xH$. Supposons qu'on ait une loi interne " $*$ " sur G/H induisant une structure de groupe sur cet ensemble et tel que π soit un homomorphisme de groupes. Alors, pour $(x, y) \in G^2$, on a :

$$\pi(x.y) = (x.y)H = xH * yH = \pi(x) * \pi(y).$$

La seule structure de groupe possible sur G/H tel que π soit un homomorphisme est donc celle définie par la formule $xH * yH := (xy)H$. Vérifions maintenant que cette loi confère bien une structure de groupe à G/H.

Il faut tout d'abord vérifier que cette loi est bien définie, c'est à dire qu'elle ne dépend pas des choix de x et de y dans les classes de congruences. Soit donc $x' \in G$ et $y' \in G$ tels que $xH = x'H$ et $yH = y'H$. On veut montrer qu'alors $(xy)H = (x'y')H$ c'est à dire que $y^{-1}x^{-1}x'y'H = H$. On a :

$$y^{-1}x^{-1}x'y' = y^{-1}y'y'^{-1}x^{-1}x'y'.$$

On a $x^{-1}x' \in H$ car $xH = x'H$ donc, comme H est normal, on obtient $y'^{-1}x^{-1}x'y' \in H$. De plus, comme $y^{-1}y' \in H$, on obtient $y^{-1}x^{-1}x'y' \in H$. On en déduit donc $y^{-1}x^{-1}x'y'H = H$. Donc la loi $xH * yH := (x.y)H$ définit une loi interne sur G/H. Elle est associative car la loi inerne de G l'est. On a un élément neutre qui est $e_G H$ et chaque classe xH possède un inverse qui est $x^{-1}H$. On a donc bien une structure de groupe sur G/H tel que π est un homomorphisme.

□

Ainsi, il est possible de mettre une structure de groupe sur le quotient G/H lorsque H est un sous-groupe normal de G. Réciproquement, on peut montrer que si une telle structure de groupe existe sur G/H alors H est normal.

De la démonstration, on retient en particulier que la loi interne définie sur le groupe quotient est donnée par $xH * yH := (xy)H$ pour $xH \in G/H$ et $yH \in G/H$. Par abus de notation, on notera cette loi interne de la même manière que la loi du groupe G c'est à dire "." en général et parfois " + " lorsque le groupe est commutatif. Un élément de la classe de congruence sera parfois noté $\overline{x}$ pour $x \in G$ au lieu de xH. Si deux éléments x et y de G sont dans la même classe de congruence modulo H, c'est à dire si $\overline{x} = \overline{y}$ (ce qui équivaut à $x^{-1}y \in H$), on note $x \equiv y (\text{mod } H)$ et on dit que x est congrue à y modulo H.

En résumé, le groupe quotient G/H est composé des classes de congruence $\overline{x}$ ($x \in G$) avec, pour $(x, y) \in G^2$, $\overline{x} = \overline{y}$ si et seulement si $x \equiv y (\text{mod } H)$ ou encore $xy^{-1} \in H$. La loi interne est donnée par :

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

Il faudra bien avoir en tête que pour définir une application f de G/H dans un ensemble S, il faudra associer à chaque élément de G/H (et non de G) un élément de S. Ainsi, si $x \equiv y (\text{mod } H)$ c'est à dire si $xH = yH$ on devra avoir $f(\overline{y}) = f(\overline{x})$ sinon f n'est pas bien définie.

Corollaire 2.3.2 *Un sous-groupe normal est le noyau d'un homomorphisme de groupes.*

Preuve. Soit H un sous-groupe normal de G. On a donc un homomorphisme π entre G et le groupe quotient G/H. Comme π est la surjection canonique, le noyau de π est H. En effet, si $\pi(x) = e_{G/H} = \overline{e_G}$ alors $\overline{x} = e_{G/H}$ et $x \in H$. Réciproquement, si $x \in H$, $\pi(x) = e_{G/H}$. Donc H est le noyau de π.

□

Théorème 2.3.3 (Théorème de correspondance) *Soit G un groupe et soit $H \lhd G$. Alors, on a une bijection*

$$\begin{array}{ccc} \{\textit{Sous-groupes de } G \textit{ contenant } H\} & \to & \{\textit{Sous-groupes de } G/H\} \\ K & \mapsto & \pi(K) \end{array}$$

Preuve. Soit K un sous-groupe de G contenant H. Comme la surjection canonique π est un homomorphisme de groupes, d'après la proposition 1.3.7, $\pi(K)$ est un sous-groupe de G/H. On a donc une application

$$\begin{array}{ccccc} \Phi : & \{\text{sous-groupes de } G \text{ contenant } H\} & \to & \{\text{sous-groupes de } G/H\} \\ & K & \mapsto & \pi(K) \end{array}$$

Il reste à montrer que Φ est bijective. Pour cela, on va montrer que Φ possède une application réciproque et le résultat suivra. Pour K' un sous-groupe de G/H, on considère l'ensemble $\pi^{-1}(K')$. D'après la proposition 1.3.7, c'est un sous-groupe de G. On a $e_{G/H} \in K'$ donc $\pi^{-1}(\{e_{g/H}\}) \subset \pi^{-1}(K')$. Mais $\pi^{-1}(\{e_{G/H}\}) = \mathrm{Ker}(\pi) = H$. Donc $\pi^{-1}(K')$ contient H. On a donc défini une application :

$$\begin{array}{ccccc} \Psi : & \{\text{sous-groupes de } G/H\} & \to & \{\text{sous-groupes de } G \text{ contenant } H\} \\ & K' & \mapsto & \pi^{-1}(K) \end{array}$$

Il reste à montrer que Ψ et Φ sont réciproques l'une de l'autre.

- Soit K un sous-groupe de G contenant H, alors, $\Psi(\Phi(K)) = \pi^{-1}(\pi(K))$. On a déjà $K \subset \pi^{-1}(\pi(K))$. Soit $x \in \pi^{-1}(\pi(K))$, alors $\pi(x) \in \pi(K)$ ce qui implique que $\overline{x} = \overline{y}$ pour $y \in K$. Donc on a $y^{-1}x \in H$ et donc $x \in yH$. Comme $y \in K$ et $H \subset K$, il suit que $x \in K$. On a donc $\pi^{-1}(\pi(K)) \subset K$. Donc $\Psi(\Phi(K)) = K$.
- Soit K' un sous-groupe de G/H. On a $\Phi(\Psi(K')) = \pi(\pi^{-1}(K'))$. On a déjà $\pi(\pi^{-1}(K')) \subset K'$. Réciproquement, si $x \in K'$, comme π est surjective, il existe $y \in G$ tel que $\pi(y) = x \in K'$ donc $x \in \pi(\pi^{-1}(K'))$. Il suit $\Phi(\Psi(K')) = K'$.

Donc Ψ et Φ sont réciproques l'une de l'autre et donc sont des bijections.

□

Théorème 2.3.4 (Théorème de factorisation pour les groupes) *Soient G et G' deux groupes et $f : G \to G'$ un morphisme de groupes. Soit $H \lhd G$ un sous-groupe normal de G tel que $H \subset \mathrm{Ker}(f)$. Alors il existe un unique morphisme de groupes $\overline{f} : G/H \to G'$ tel que $\overline{f} \circ \pi = f$ où $\pi : G \to G/H$ est la surjection canonique.*

Preuve.

1. On va tout d'abord définir l'application $\overline{f}$ pour qu'elle vérifie les propriétés du théorème. Soit $\overline{x} = xH$ avec $x \in G$. Alors, on doit avoir $\overline{f}(\overline{x}) = f(x)$. Il faut vérifier que ceci définit bien une application de G/H dans G' autrement dit que si $\overline{x} = \overline{y}$ pour $(x, y) \in G^2$ alors $f(x) = f(y)$. On suppose donc $\overline{x} = \overline{y}$ c'est à dire $xy^{-1} \in H$ alors $f(x)f(y)^{-1} \in f(H)$. Or, on a $H \subset \mathrm{Ker}(f)$ donc $f(xy^{-1}) = e_{G'}$. Il suit $f(x) = f(y)$. Donc notre application $\overline{f}$ est bien définie et elle est unique à vérifier la propriété $\overline{f} \circ \pi = f$.
2. Reste à montrer que $\overline{f}$ est un homomorphisme de groupes. Soit $x \in G$ et $y \in G$, on veut montrer que $\overline{f}(\overline{x}.\overline{y}) = \overline{f}(\overline{x})\overline{f}(\overline{y})$. Par définition on a $\overline{x}.\overline{y} = \overline{x.y}$ donc $\overline{f}(\overline{x}.\overline{y}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y})$. Donc f est bien un homomorphisme de groupes.

□

Supposons que l'on dispose de deux groupes G et G' et d'un sous-groupe normal H de G. Si $f : G \to G'$ est un morphisme de groupes tel que $H \subset \mathrm{Ker}(f)$. Alors, le théorème ci-dessus nous montre l'existence d'une unique application $\overline{f} : G/H \to G'$ telle que $\overline{f} \circ \pi = f$. Dans ce cas, on dira que f *passe au quotient.*

Théorème 2.3.5 (Théorème d'isomorphie pour les groupes) *Soient G et G' deux groupes et soit $f : G \to G'$ un morphisme de groupes. Alors on a un isomorphisme :*

$$G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f).$$

Preuve. On pose $H := \mathrm{Ker}(f)$, c'est un sous-groupe normal de G. On peut donc appliquer le théorème de factorisation pour les groupes : il existe une unique application $\overline{f}$ de $G/\mathrm{Ker}(f)$ dans G' tel que $\overline{f} \circ \pi = f$ où $\pi : G \to G/H$ est la surjection canonique. Soit $x \in G$ et soit $\overline{x} \in G/H$ sa classe de congruence et supposons que $\overline{f}(\overline{x}) = e_{G'}$. On a $\overline{f}(\overline{x}) = f(x)$ donc $x \in \mathrm{Ker}(f) = H$ donc $\overline{x} = e_{G/H}$. On a donc $\mathrm{Ker}(\overline{f}) = \{e_{G/H}\}$. Donc $\overline{f}$ est injective et donc l'application $\overline{f}$ de G/H dans $\mathrm{Im}(f)$ est bijective d'où l'isomorphisme.

□

Exemple. Considérons $GL_{2n}(\mathbb{C})$ et son sous-groupe normal $SL_n(\mathbb{C})$. $SL_n(\mathbb{C})$ est en fait le noyau de l'application déterminant. L'application déterminant

est bien sûr surjective dans $\mathbb{C}^*$. En effet si $\lambda \in \mathbb{C}^*$, $A := \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 1 \end{pmatrix}$ vérifie $\mathrm{Det}(A) = \lambda$. On en déduit que $GL_n(\mathbb{C})/SL_n(\mathbb{C}) \simeq \mathbb{C}^*$ car $\mathrm{Im}(\det) = \mathbb{C}^*$.

Définition 2.3.6 Un groupe G est dit *simple* si il n'a pas de sous-groupe normal non trivial.

Ce type de groupes est particulièrement important. En effet, étant donné un groupe fini G, si on dispose d'un sous-groupe normal H non trivial, on peut ramener l'étude de G à l'étude de H et du groupe quotient G/H. Alors, l'ordre de G/H est plus petit que l'ordre de G. Soit ce groupe est simple, soit on dispose d'un sous-groupe normal et on peut former un autre groupe quotient. On peut ainsi continuer jusqu'à trouver un groupe simple G' et esperer récupérer des propriétés de G à partir de G'.

Ainsi, les groupes simples finis peuvent être perçus comme les composantes de base de tous les groupes finis, de la même façon que tous les nombres entiers peuvent être décomposés en produit de nombres premiers.

La classification des groupes finis simples a été achevée en 1982 et est un des monuments des mathématiques du vingtième siècle. Le résultat est que ce sont les groupes quotients $\mathbb{Z}/p\mathbb{Z}$ avec p premier, groupes que nous étudierons dans la prochaine partie, les groupes alternés (qui sont des sous-groupes des groupes symétriques, voir le chapitre 4), les groupes dits de Chevalley (qui sont des sous-groupes de groupes de matrices associés à des considérations géométriques ...) ainsi que 26 sous-groupes tout à fait inclassables et appelées groupes sporadiques (dont le plus "gros", appelé "le Monstre", possède environ 8.10^{53} éléments !).

2.4 Exemple fondamental : les groupes quotients de $\mathbb{Z}$

Dans cette partie, nous allons chercher tous les groupes quotients du groupe $\mathbb{Z}$. Nous avons déjà vu certains sous-groupes de $\mathbb{Z}$: ces sont les sous-groupes de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$. Nous allons maintenant montrer que ce sont les seuls sous-groupes de $\mathbb{Z}$. Soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$. Supposons donc que $H \neq \{0\}$. Alors H contient necessairement des entiers strictement positifs (il suffit de prendre un élément non nul quelconque de H et de considérer son inverse : un des deux est strictement positif). Partie

non vide de $\mathbb{N}$, l'ensemble $H \cap \mathbb{N}_{>0}$ contient un plus petit élément que nous notons n. $n\mathbb{Z}$ est le sous-groupe de $\mathbb{Z}$ engendré par n, comme $n \in H$, on en déduit que $n\mathbb{Z} \subset H$.

Soit maintenant $x \in H$. On peut supposer $x > 0$ et On fait la division euclidienne de x par n : il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tel que $0 \leq r \leq n-1$ vérifiant $x = nq + r$. Comme $n \in H$ et $x \in H$, on en déduit $r \in H$. Mais n étant le plus petit élément strictement positif de H, il suit $r = 0$ donc $x = nq \in n\mathbb{Z}$. On a donc $H = n\mathbb{Z}$. Notons de plus que comme $\mathbb{Z}$ est commutatif, tous les sous-groupes de $\mathbb{Z}$ sont normaux. On a donc démontré le théorème suivant :

Théorème 2.4.1 *Les seuls sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N} \cup \{0\}$.*

Soit $n \in \mathbb{N} \cup \{0\}$, on peut former maintenant le groupe quotient $\mathbb{Z}/n\mathbb{Z}$. Pour $(k, m) \in \mathbb{Z}$, la relation de congruence est la suivante : on a $k \equiv m(\text{mod } n\mathbb{Z})$ (que l'on notera pour simplifier $k \equiv n(\text{mod } n)$) c'est à dire $\overline{k} = \overline{m}$ si et seulement si $k - m \in n\mathbb{Z}$ soit encore :

$$m \equiv k(\text{mod } n) \iff \begin{array}{c}\text{le reste de la division euclidienne de } m \text{ et } k \\ \text{par } n \text{ est le même}\end{array}$$

Ainsi, $\mathbb{Z}/n\mathbb{Z}$ est composé de n éléments $\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ et, pour $\overline{k}$ et $\overline{m}$ dans $\mathbb{Z}/n\mathbb{Z}$ la loi interne est donnée par $\overline{k}.\overline{m} = \overline{k.m}$ qui est égale à $\overline{r}$ où r est le reste de la division euclidienne de $k.m$ par n.

Exemple. On a :

$$\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}.$$

Le tableau suivant nous donne la loi interne dans ce groupe quotient de $\mathbb{Z}$

$+$	$\overline{\mathbf{0}}$	$\overline{\mathbf{1}}$	$\overline{\mathbf{2}}$
$\overline{\mathbf{0}}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{\mathbf{1}}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{\mathbf{2}}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

En fait, nous avons déjà rencontré ces groupes :

Proposition 2.4.2 *Soit $n \in \mathbb{N}$ alors le groupe $\mathbb{Z}/n\mathbb{Z}$ est isomorphe au groupe C_n des racines nième de l'unité dans $\mathbb{C}$.*

Preuve. Soit le morphisme de groupes

$$\begin{array}{rccc} f: & \mathbb{Z} & \to & C_n \\ & k & \mapsto & \exp(\frac{2ik\pi}{n}) \end{array}$$

Il est clair que l'application f est surjective. Son noyau est l'ensemble des $k \in \mathbb{Z}$ nul ou tel que n divise k c'est à dire $n\mathbb{Z}$. On utilise alors le théorème 2.4.2 qui nous dit que $\mathbb{Z}/n\mathbb{Z} \simeq C_n$

□

An particulier, le théorème 1.4.8 se reformule de la façon suivante :

Théorème 2.4.3 (Classification des groupes monogènes) *Soit G un groupe monogène.*

1. *Si G est infini, G est isomorphe à $\mathbb{Z}$*
2. *Si G est fini d'ordre n, G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Chapitre 3

Théorèmes de Sylow

3.1 Actions de groupes

Définition 3.1.1 Soit S un ensemble et soit G un groupe. Une action de G sur S est une application :

$$\alpha : G \times S \to S$$

telle que :

1. $\forall (g_1, g_2) \in G^2,\ \forall x \in S, \alpha(g_1, \alpha(g_2, x)) = \alpha(g_1 g_2, x)$,
2. $\forall x \in S,\ \alpha(e_G, x) = x$.

On dit alors que G *agit sur* S ou que G *opère sur* S. Pour simplifier on notera $\alpha(x, s) = x.s$ (il ne faut cependant pas confondre l'action de G avec la loi interne de G !). Quand il y aura risque de confusion (en particulier lorsque $X = G$), nous essaierons d'adopter une autre notation pour l'action de G sur X, par exemple, $\alpha(x, s) = x * s$.

En particulier, étant donné un groupe G, G agit toujours sur lui même de deux façons différentes :

– via l'action

$$\begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & x.y \end{array}$$

On parle *d'action par translation.*

– via l'action

$$\begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & x.y.x^{-1} \end{array}$$

On parle *d'action par conjugaison.*

Ces deux actions seront particulièrement importantes dans la suite du chapitre.

Définition 3.1.2 Soit G un groupe agissant sur un ensemble X et $x \in X$. *Le stabilisateur de* x est par définition l'ensemble $G_x = \{\sigma \in G, \mid \sigma.x = x\}$. *L'orbite de* x sous l'action de G est l'ensemble $G.x := \{g.x \mid g \in G\}$.

Le stabilisateur d'un élément $x \in X$ sous l'action de G est aussi parfois noté $\mathrm{Stab}_G(x)$. Il est immédiat de vérifier que c'est un sous-groupe de G.

Exemple.

1. Soit $GL_n(\mathbb{C})$ l'ensemble des matrices inversibles à n lignes et n colonnes et à coefficients dans $\mathbb{C}$. Alors, $GL_n(\mathbb{C})$ agit sur $\mathbb{C}^n$ via l'action :

$$\begin{array}{ccc} GL_n(\mathbb{C}) \times \mathbb{C}^n & \to & \mathbb{C}^n \\ (A, x) & \mapsto & Ax. \end{array}$$

   Soit x un élément non nul de $\mathbb{C}^n$. Alors $A \in G_x$ si et seulement si $Ax = x$ c'est à dire si $(A - I)x = 0$. Donc le stabilisateur de x est l'ensemble des matrices inversibles avec valeur propre 1 et ayant x comme vecteur propre associé à cette valeur propre.

2. Plus généralement, le groupe linéaire $GL_k(V)$, ensemble des applications k-linéaires d'un k-espace vectoriel V (où k est un corps) agit sur V de la même manière.

3. L'ensemble $\mathfrak{S}_n$ des bijections de $\{1, \cdots, n\}$ vers $\{1, \cdots, n\}$ agit sur $\{1, \cdots, n\}$ de la façon suivante :

$$\begin{array}{ccc} \mathfrak{S}_n \times \{1, \cdots, n\} & \to & \{1, \cdots, n\} \\ (\sigma, j) & \mapsto & \sigma(j). \end{array}$$

   L'orbite d'un élément $j \in \{1, \cdots, n\}$ est l'ensemble des $\sigma(j)$ pour $\sigma \in \mathfrak{S}_n$. C'est évidemment l'ensemble $\{1, \cdots, n\}$ en entier.

Proposition 3.1.3 *Soit G un groupe agissant sur un ensemble X. Soit x un élément de X. Alors, il existe une bijection entre l'orbite $G.x$ de x et l'ensemble des classes à gauche de G modulo G_x.*

Preuve. On construit une application Φ de G/G_x, l'ensemble des classes de congruences à gauche de G modulo G_x vers l'orbite $G.x$ de x. Pour $g \in G$, on pose $\Phi(gG_x) = g.x \in G.x$. Il faut vérifier que cette application est bien définie. Soit donc $g' \in G$ tel que $gG_x = g'G_x$ alors ${g'}^{-1}g \in G_x$. On en déduit donc $({g'}^{-1}g).x = x$ d'où $g.x = g'.x$. L'application Φ est donc bien définie. Elle est de plus clairement surjective et si $g.x = g'.x$ alors $({g'}^{-1}g).x = x$ et donc $gG_x = g'G_x$ c'est à dire ${g'}^{-1}g \in G_x$ donc elle est injective. Φ est donc une bijection entre G/G_x et $G.x$ ce qui prouve la proposition.

□

Attention, le stablisateur d'un élément n'est pas forcément un sous-groupe normal de G donc on n'a pas nécessairement une structure de groupe sur l'ensemble G/G_x.

Supposons qu'un groupe G agisse sur X. Alors il existe un ensemble S tel que $X = \coprod_{x\in S} G.x$ c'est à dire que $X = \cup_{x\in S} G.x$ et $G.x \cap G.y = \emptyset$ si $x \neq y$ sont dans S . Pour S, il suffit de prendre un représentant de chaque orbite : on obtient alors évidemment $X = \cup_{x\in S} G.x$ et si $G.x \cap G.y \neq \emptyset$ alors il existe $(g, g') \in G^2$ tel que $g.x = g'.y$ d'où $(g'^{-1}g).x = y$ ce qui signifie que x et y sont dans la même orbite.

Théorème 3.1.4 (Equation des classes) *Soit G un groupe agissant sur un ensemble fini X. Soit S un système de représentants des orbites (comme ci-dessus) c'est à dire $X = \coprod_{x\in S} G.x$ (réunion disjointe). Alors, on a :*

$$o(X) = \sum_{x\in S} [G : G_x],$$

où $o(X)$ désigne le cardinal de X.

Preuve. Soit $x \in S$. On utilise la proposition précédente, on a une bijection entre $G.x$ et l'ensemble des classes de congruence à gauche modulo G_x. Ceci signifie que $o(G.x) = [G : G_x]$. Or on a $o(X) = \sum_{x\in S} o(G.x)$ d'où le résultat.
□

Signalons la conséquence suivante concernant les p-groupes. Soit p un nombre premier. Un *p-groupe* est un groupe d'ordre une puissance de p. Par exemple $\mathbb{Z}/8\mathbb{Z}$ est un 2-groupe (il est d'ordre 2^3 avec 2 premier).

Proposition 3.1.5 *Soit G un p-groupe agissant sur un ensemble X et soit X^G l'ensemble des points fixes sous l'action de G c'est à dire $X^G = \{x \in X \mid g.x = x \ \forall g \in G\}$. On a alors :*

$$o(X^G) \equiv o(X) \ (mod\ p)$$

Preuve. D'après le théorème de Lagrange, l'ordre de chaque sous-groupe de G divise l'ordre de G. L'ordre d'un sous-groupe est donc une puissance de p car G est un p-groupe. Ainsi $[G : G_x]$ est soit divisible par p soit égale à 1. De plus, $[G : G_x] = 1$ si et seulement si $o(G_x) = o(G)$ c'est à dire si pour tout $g \in G$, on a $g.x = x$ c'est à dire si $x \in X^G$. On utilise maintenant l'équation des classes : tous les $[G : G_x]$ sont nuls modulo p excepté si $x \in X^G$ ce qui démontre la proposition.

□

3.2 Théorèmes de Sylow

Nous allons maintenant étudier précisemment la structure des groupes finis. Etant donné un groupe G, le but est ici de savoir combien G a de sous-groupes, quels sont les ordres de ces sous-groupes, lesquels sont normaux etc .... Les outils fondamentaux pour cette étude vont être donnés par les théorèmes de Sylow. La démonstration de ces théorèmes demande une compréhension en profondeur des actions de groupes et de l'équation des classes.

Définition 3.2.1 Soit G un groupe fini d'ordre n, p un nombre premier qui divise n et p^α la plus grande puissance de p qui divise n. On appelle *p-sous-groupe de Sylow* de G tout sous-groupe de G d'ordre p^α.

Un p-sous-groupe de Sylow est donc en particulier un p-groupe. L'inverse n'est pas vrai car si $\alpha \geq 2$, un sous-groupe d'ordre p est un p-groupe mais pas un p-sous-groupe de Sylow.

Rappellons qu' un entier n se factorise de façon unique sous la forme :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

où les p_i sont les nombres premiers divisant n et les $p_i^{\alpha_i}$ les plus grandes puissances de p qui divise n.

On dira que deux sous-groupes H et H' de G sont *conjugués* si il existe $g \in G$ tel que $H = gHg^{-1}$.

Théorème 3.2.2 (Théorèmes de Sylow) *Soit G un groupe fini d'ordre n et p un nombre premier divisant n.*

1. *Le nombre de p-sous-groupes de Sylow est congru à 1 modulo p.*
2. *Deux p-sous-groupes de Sylow quelconques sont conjugués.*
3. *Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow.*
4. *Le nombre de p-sous-groupes de Sylow divise m où $n = p^\alpha m$ et où $\text{pgcd}(p, m) = 1$.*

Preuve. Nous allons démontrer ce théorème en quatre temps.
1. Préliminaire. Nous commençons par démontrer le résultat suivant. Soit G un groupe commutatif fini et p un nombre premier tel que p divise $o(G)$. Alors, G contient un élément d'ordre p et donc un sous-groupe d'ordre p.

On raisonne par récurrence sur l'ordre de G. Supposons tout d'abord que $o(G) = p$ alors le résultat est évident (tout élément différent de e_G dans

G est d'ordre p). On suppose maintenant la propriété satisfaite pour tout groupe H avec p divisant $o(H)$ et $o(H) < o(G)$. Notons tout d'abord que si G contient un élément x d'ordre pq pour un $q \in \mathbb{N}_{>0}$ alors $o(x^q) = p$. Supposons maintenant que G contienne x avec $o(x) = q$, $x \neq e_G$ et tel que p ne divise pas q. Soit H le sous-groupe engendré par x. H est normal car G est commutatif donc on peut former le groupe quotient G/H. On sait que p divise $o(G)$ et $o(H)$ est premier avec p donc p divise $o(G/H) = o(G)/o(H)$. Par récurrence, il existe donc $\overline{y} \in G/H$ tel que $o(\overline{y}) = p$ avec $y \in G$. Si $y^k = e_G$ alors $\overline{y}^k = e_{G/H}$ donc p divise m et donc p divise l'ordre de y. Il existe donc $r \in \mathbb{N}_{>0}$ tel que $o(y) = rp$ et alors y^r est d'ordre p.

2. Il existe un p-sous-groupe de Sylow dans G. On va montrer le résultat suivant : si G est un groupe d'ordre $p^\alpha m$ avec m premier avec p et $\alpha \geq 0$ alors G contient un sous-groupe d'ordre p^α (la différence avec l'énoncé est qu'ici, on n'exclut pas le cas $\alpha = 0$).

On montre cette propriété par récurrence sur α et m. Si $\alpha = 0$ ou $m = 1$, c'est évident. On suppose maintenant le théorème satisfait pour tout groupe G tel que $o(G') < o(G)$.

Supposons qu'il existe un sous-groupe H de G tel que $[G : H]$ soit premier avec p. Alors l'ordre de H est nécessairement de la forme $n'p^\alpha$ avec n' premier avec p et $n' < m$. On peut alors utiliser l'hypothèse de récurrence : il existe un p-sous-groupe de Sylow de H, il est donc d'ordre p^α, c'est donc un p-sous-groupe de Sylow de G. On peut donc supposer que tout sous-groupe H de G est tel que p divise $[G : H]$. Le groupe G agit par conjugaison sur lui-même :

$$\begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & x * y := xyx^{-1} \end{array}$$

Sous cette action, on note que les éléments des orbites réduites à un élément correspondent exactement aux éléments du centre de G. En effet, si $G * x$ est une telle orbite alors pour tout $g \in G$ on a $g * x = gxg^{-1} = x$ (attention, l'action de G sur x est ici définie par $g * x = gxg^{-1}$, il ne faut pas confondre l'action avec la loi interne). On utilise maintenant l'équation des classes : G est la réunion disjointe des orbites réduites à un élément et d'autres orbites $G * x_i$ pour $i = 1, \cdots, r$. On obtient :

$$o(G) = o(Z(G)) + \sum_{i=1}^{r} [G : G_{x_i}].$$

Comme p divise $o(G)$ et tous les $[G : G_{x_i}]$, p divise nécessairement $o(Z(G))$.

Le centre $Z(G)$ est un sous-groupe commutatif de G, le résultat précédent nous montre l'existence d'un sous-groupe H de $Z(G)$ d'ordre p. Comme c'est

un sous-groupe de $Z(G)$, il est bien sûr normal (tout élément de G commute avec les éléments de H). On forme le groupe quotient G/H. Il est d'ordre $p^{\alpha-1}m$. Par récurrence, G/H contient un sous-groupe H_1 d'ordre $p^{\alpha-1}$. Soit $\pi : G \to G/H$ la surjection canonique et soit π' sa restriction à $\pi^{-1}(H_1)$. Cette restriction reste surjective dans H_1 et son noyau est $H \subset \pi^{-1}(H_1)$. On a donc $o(\pi^{-1}(H_1)) = o(H_1)o(H) = p^\alpha$. Ainsi $\pi^{-1}(H_1)$ est un sous-groupe d'ordre p^α.

3. Soient H un p-sous-groupe de G, P un p-sous-groupe de Sylow de G. Alors, il existe $g \in G$ tel que $H \subset gPg^{-1}$.

Soit $\mathcal{S}$ l'ensemble des p-sous-groupes de Sylow. $\mathcal{S} \neq \emptyset$ d'après 2.. G agit sur $\mathcal{S}$ par conjugaison :

$$\begin{array}{ccc} G \times \mathcal{S} & \to & \mathcal{S} \\ (g, K) & \mapsto & gKg^{-1} \end{array}$$

Le stabilisateur du p-sous-groupe de Sylow P est :

$$G_P = \{g \in G \mid gPg^{-1} = P\}.$$

P est un sous-groupe de G_P donc p^α divise $o(G_P)$ donc p ne divise pas $[G : G_P]$ donc ne divise pas le cardinal de $G.P := \{gPg^{-1} \mid g \in G\}$.

Maintenant H agit aussi par conjugaison sur $G.P$. Comme H est un p groupe, les orbites sous cette action, qui sont des sous-ensembles de $G.P$, ont soit un élément soit un cardinal divisible par p. Or, on vient de voir que p ne divise pas le cardinal de $G.P$, il suit qu'il existe au moins une orbite à un élément, disons celle de P'. On a donc $hP'h^{-1} = P'$ pour tout $h \in H$ avec P' conjugué à P. Considérons l'ensemble $HP' := \{h.x \mid h \in H,\ x \in P'\}$. C'est un sous-groupe de G car $HP' = P'H$. De plus, P' est un sous-groupe de HP' et il est normal dans HP' (car $hP'h^{-1} = P'$ pour tout $h \in H$ donc pour tout $h \in HP'$). On peut donc former le groupe quotient HP'/P' et on a une surjection canonique $HP' \to HP'/P'$. La restriction de cette application à H est surjective et donc $o(HP'/P') = p^r$ pour un certain r. On a $o(HP') = p^r o(P')$ donc $o(HP') = p^{r+\alpha}$. Or, HP' est un sous-groupe de G qui est d'ordre $p^\alpha m$ donc $r = 0$ et il suit $H \subset P'$. H est donc bien contenu dans un groupe de la forme gPg^{-1} pour un $g \in G$.

Ceci prouve la deuxième et la troisième assertion du théorème.

4. Le nombre de p-sous-groupes de Sylow est congrue à 1 modulo p.

On garde les mêmes notations que dans les parties précédentes. On sait que l'ensemble des p-sous-groupes de Sylow est égal à l'orbite de P sous

l'action de G par conjugaison (P étant un p-sous-groupe de Sylow fixé). Donc le cardinal de $\mathcal{S}$ est égale $[G : G_P]$. Comme $o(P)$ divise $o(G_P)$, ce cardinal divise $[G : P]$ donc m. Montrons que la seule orbite de $\mathcal{S}$ à un élément sous l'action de P est P. Supposons que $hP'h^{-1} = P'$ pour tout $h \in P$ et pour un p-sous-groupe de Sylow P'. Alors PP' est un sous-groupe de G. Exactement comme dans la partie précédente, on montre alors que $P = PP'$ donc $P \subset P'$ c'est à dire $P = P'$ car les deux groupes ont même ordre. L'équation des classes nous donne alors :

$$|\mathcal{S}| = 1 + \sum_{P' \in S, P' \neq P} [P : P_{P'}],$$

où S est tel que $\mathcal{S} = \coprod_{P' \in S} P.P'$. Pour $P' \in S$ et $P \neq P'$, $[P : P_{P'}]$ est divisible par p d'où le résultat. Ceci prouve la première assertion et la quatrième assertion.

□

On verra beaucoup d'applications de ces théorèmes en TD. Signalons toutefois les résultats suivants.

Théorème 3.2.3 (Théorème de Cauchy) *Soit G un groupe fini et p un nombre premier divisant l'ordre de G. Alors G contient un élément d'ordre p.*

Preuve. D'après les théorèmes de Sylow, G possède un p-sous-groupe de Sylow. Un élément non nul x dans ce sous-groupe est d'ordre une puissance de p, disons p^r. Alors $x^{p^{r-1}}$ est d'ordre p car $x^{p^r} = e_G$ et si $x^{p^{r-1}q} = e_G$ alors p^r divise $p^{r-1}q$ donc p divise q.

□

Proposition 3.2.4 *Soit H un p-sous-groupe de Sylow de G et n_p le nombre de p-sous-groupes de Sylow de G. Alors H est un sous-groupe normal de G si et seulement si $n_p = 1$.*

Preuve.

1. Supposons que $H \triangleleft G$ et soit H' un p sous-groupe de Sylow de G. D'après le deuxième théorème de Sylow, il existe $g \in G$ tel que $H' = gHg^{-1}$. Comme $H \triangleleft G$, nous avons $gHg^{-1} = H$ pour tout $g \in G$. Donc, on retrouve $H' = H$ et $n_p = 1$.
2. Réciproquement, on suppose que $n_p = 1$. Pour tout $g \in G$, gHg^{-1} est un sous-groupe de G d'ordre égal à $o(H)$, c'est à dire, un p-sous-groupe de Sylow. On a ainsi $gHg^{-1} = H$ car $n_p = 1$. Comme l'égalité précédente est valable pour tout $g \in G$, alors $H \triangleleft G$.

□

Exemple.

1. Soit G un groupe d'ordre $15 = 3.5$. Le nombre de 3-sous-groupes de Sylow n_3 divise 5, et $n_3 \equiv 1(\text{mod } 3)$. La seule valeur possible est 1. Donc, il y a un seul sous-groupe d'ordre 3, et il doit donc être normal. De façon analogue, le nombre de 5-sous-groupes de Sylow n_5 divise 3, et $n_5 \equiv 1(\text{mod } 5)$. Donc, il y a aussi un seul sous-groupe normal d'ordre 5.
2. Soit $\mathfrak{S}_3$ le groupe des bijections de $\{1, 2, 3\}$ sur $\{1, 2, 3\}$. Il comporte $2.3 = 6$ éléments. Le nombre de 3-sous-groupes de Sylow n_3 divise 2 et $n_3 \equiv 1(\text{mod } 3)$ donc il y en a un seul. Le nombre de 2-sous-groupes de Sylow n_2 divise 3 et $n_2 \equiv 1(\text{mod } 2)$. Il y en a donc 1 ou 3. On peut conclure par exemple en notant que l'on a au moins 2 éléments d'ordre 2 : $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ et $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ et donc on a trois 2-sous-groupes de Sylow.

Chapitre 4

Groupes symétriques

4.1 Généralités

Rappellons la définition générale des groupes symétriques :

Définition 4.1.1 Soit E un ensemble non vide. On appelle groupe symétrique sur E le groupe des bijections $E \to E$, que l'on note $\mathfrak{S}_E$. Un élément de $\mathfrak{S}_E$ est appelé *une permutation*. Lorsque $E = \{1, \cdots, n\}$, on note plus souvent $\mathfrak{S}_E = \mathfrak{S}_n$.

Il est important de noter que $\mathfrak{S}_E$ agit canoniquement sur E grâce à l'action ci-dessous :

$$\begin{array}{ccc} \mathfrak{S}_E \times E & \to & E \\ (\sigma, s) & \mapsto & \sigma(s) \end{array}$$

Proposition 4.1.2 *Soit $f : E \to F$ une bijection entre deux ensembles. Alors l'application*

$$\phi : \begin{array}{ccc} \mathfrak{S}_E & \to & \mathfrak{S}_F \\ s & \mapsto & f \circ s \circ f^{-1} \end{array}$$

est un isomorphisme de groupes.

Preuve. On a tout d'abord $\phi(s) \in \mathfrak{S}_F$ pour tout $s \in \mathfrak{S}_E$. De plus, ϕ est un homomorphisme de groupes. En effet, soient s et s' dans $\mathfrak{S}_E$, alors $\phi(s \circ s') = f \circ s \circ s' \circ f^{-1} = f \circ s \circ f^{-1} \circ f \circ s' \circ f^{-1} = \phi(s) \circ \phi(s')$. De plus, on vérifie que l'application

$$\begin{array}{ccc} \mathfrak{S}_F & \to & \mathfrak{S}_E \\ s & \mapsto & f^{-1} \circ s \circ f \end{array}$$

est l'application réciproque de ϕ. Il suit que ϕ est une bijection, c'est donc un isomorphisme.

□

Le symbole de composition (la loi interne de $\mathfrak{S}_E$) sera parfois omis par la suite. L'étude des groupes symétriques est motivée par le théorème fondamental suivant :

Théorème 4.1.3 (Théorème de Cayley) *Tout groupe G est isomorphe à un sous-groupe de $\mathfrak{S}_G$*

Preuve. Soit $g \in G$. On considère l'application suivante :

$$\begin{array}{rccc} L_g : & G & \to & G \\ & g' & \mapsto & gg' \end{array}$$

Cette application est une bijection (mais ce n'est pas un homomorphisme en général). En effet, si $h \in G$ alors $h = L_g(g^{-1}h)$ donc elle est surjective. De plus, si $gg' = gg''$ alors $g' = g''$ donc elle est injective.

On a donc une application :

$$\begin{array}{rccc} L : & G & \to & \mathfrak{S}_G \\ & g & \mapsto & L_g \end{array}$$

On montre que c'est un homomorphisme de groupes. Soit $(g, g') \in G^2$, on veut montrer que $L(gg') = L(g) \circ L(g')$. Soit $x \in G$ on a $L(gg')(x) = gg'x$ et $L(g) \circ L(g')(x) = L(g)(g'x) = gg'x$. L est de plus injective car si $L_g = L_{g'}$ alors on a pour tout $x \in G : gx = g'x$ soit en particulier pour $x = e_G$, $g = g'$. Il suit que G est isomorphe à $\mathrm{Im}(L_g)$ qui est un sous-groupe de $\mathfrak{S}_G$

□

En fait, historiquement, les groupes sont tout d'abord apparus comme sous-groupes des groupes symétriques dans les travaux de Lagrange et surtout de Galois. Ce n'est que plus tard, grâce à des mathématiciens tels que Cayley justement, Weber, Burnside et Pierpont que la définition de groupe telle qu'on l'a vu ici a été peu à peu mise en évidence. L'usage a démontré l'avantage de cette définition.

Définition 4.1.4 Soit E un ensemble et $\sigma \in \mathfrak{S}(E)$. On appelle *support* de σ l'ensemble :

$$\mathrm{Supp}(\sigma) = \{j \in E |\ \sigma(j) \neq j\}$$

Proposition 4.1.5 *Soit σ_1 et σ_2 dans $\mathfrak{S}_E$ alors :*

1. $\mathrm{Supp}(\sigma_1\sigma_2\sigma_1^{-1}) = \sigma_1(\mathrm{Supp}(\sigma_2))$
2. *Si σ_1 et σ_2 ont des supports disjoints, ils commutent.*

Preuve.

1. Soit $j \in \text{Supp}(\sigma_1\sigma_2\sigma_1^{-1})$ alors on a $\sigma_1(\sigma_2(\sigma_1^{-1}(j))) \neq j$ alors $\sigma_2(\sigma_1^{-1}(j)) \neq \sigma_1^{-1}(j)$ donc $\sigma_1^{-1}(j) \in \text{Supp}(\sigma_2)$ c'est à dire $j \in \sigma_1(\text{Supp}(\sigma_2))$.
   Réciproquement, si $j \in \sigma_1(\text{Supp}(\sigma_2))$ alors $\sigma_1^{-1}(j) \in \text{Supp}(\sigma_2)$ d'où $j \in \text{Supp}(\sigma_1\sigma_2\sigma_1^{-1})$.
2. Si σ_1 et σ_2 ont des supports disjoints. Soit $j \in E$ alors :
   - Soit $j \notin \text{Supp}(\sigma_1)$ et $j \notin \text{Supp}(\sigma_2)$. On obtient alors $\sigma_1(\sigma_2(j)) = j = \sigma_2(\sigma_1(j))$.
   - Soit $j \in \text{Supp}(\sigma_1)$ et alors $j \notin \text{Supp}(\sigma_2)$. On a alors $\sigma_1(\sigma_2(j)) = \sigma_1(j)$ car $\sigma_2(j) = j$. D'autre part on a d'après 1), $\text{Supp}(\sigma_1\sigma_1\sigma_1^{-1}) = \sigma_1(\text{Supp}(\sigma_1))$. Ainsi, $\text{Supp}(\sigma_1) = \sigma_1(\text{Supp}(\sigma_1))$. Il suit que $\sigma_1(j) \in \text{Supp}(\sigma_1)$. Mais les supports de σ_1 et σ_2 sont disjoints donc $\sigma_1(j) \notin \text{Supp}(\sigma_2)$. On obtient donc $\sigma_2(\sigma_1(j)) = \sigma_1(j)$.
   - Soit $j \notin \text{Supp}(\sigma_1)$ et alors $j \in \text{Supp}(\sigma_2)$ et on conclut de même $\sigma_2(\sigma_1(j)) = \sigma_2(j) = \sigma_1(\sigma_2(j))$.

□

4.2 Permutations d'un ensemble fini

Dans toute la suite, nous nous intéresserons au cas où E est fini. Or, comme tout ensemble fini de cardinal n est en bijection avec $\{1, \cdots, n\}$, d'apres la proposition 4.1.2, nous pouvons uniquement considérer les groupes $\mathfrak{S}_n$ sans perdre de généralité.

Un élément quelconque de $\mathfrak{S}_n$ pourra dans un premier temps s'écrire de la façon suivante :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

Exemple. Voir le dernier exemple du premier chapitre.

Soit $\sigma \in \mathfrak{S}_n$. Alors on vérifie facilement que la relation suivante définit une relation d'équivalence sur $\{1, \cdots, n\}$:

$$i\mathcal{R}j \iff \exists k \in \mathbb{N},\ \sigma^k(i) = j.$$

Les classes d'équivalence sont appelées les *σ-orbites*. Etant donné σ, $\{1, \cdots, n\}$ s'écrit donc comme une réunion disjointe de σ-orbites.

Exemple Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$ dans $\mathfrak{S}_5$. Alors, les σ-orbites sont $\{1, 2\}$, $\{3\}$ et $\{4, 5\}$.

Définition 4.2.1 On dit qu'une permutation σ de $\mathfrak{S}_n$ est un *cycle de longueur k* s'il existe k éléments distincts $\{a_1, \cdots, a_k\}$ de $\{1, \cdots, n\}$ tels que $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, ..., $\sigma(a_{k-1}) = a_k$, $\sigma(a_k) = a_1$ et $\sigma(x) = x$ si x n'est pas un des a_i. Si $k > 1$, $\{a_1, \cdots, a_k\}$ est donc le support de σ. Un cycle de longueur 2 appelé *une transposition*. On notera $\sigma = (a_1, \cdots, a_k)$.

Attention, pour un cycle σ, la notation ci-dessus n'est pas unique : si on reprend les données de la définition, on a aussi $\sigma = (a_2, \cdots, a_{k-1}, a_k, a_1)$ par exemple. Ceci justifie d'ailleurs l'appellation "cycle".

Si $(a_1, \cdots, a_k)$ est un cycle de longueur k alors comme $\sigma^k(a_i) = a_i$ pour tout $i \in \{1, \cdots, k\}$, l'ordre de σ est k.

Ainsi, une transposition est une permutation qui échange deux éléments. Notons qu'une permutation ne peut pas avoir un support de cardinal 1, il n'y a donc pas de cycle de longueur 1. Il y a un unique cycle de longueur 0 qui est l'identité.

Notons également qu'un cycle différent de l'identité est une permutation ayant une seule orbite non triviale, les éléments de cette orbite correspondent au support et le cardinal de cette orbite correspond à la longueur du cycle.

Exemple. Dans $\mathfrak{S}_3$, $\mathrm{Id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ est un cycle de longueur 0, $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2)$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3)$ et $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)$ sont des cycles de longueur 2 (des transpositions). $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2)$ sont des cycles de longueur 3.

Il existe des permutations qui ne sont pas des cycles, par exemple $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$ dans $\mathfrak{S}_5$ n'est pas pas un cycle mais c'est un produit de deux cycles : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ et $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$. On voit ici que les σ-orbites sont données par $\{1,2\}$, $\{3\}$ (orbite triviale) et $\{4,5\}$.

Théorème 4.2.2 *Toute permutation de $\mathfrak{S}_n$ se décompose de manière unique (à l'ordre près) en un produit de cycles dont les supports sont deux à deux disjoints.*

Preuve. Soit $\sigma \in \mathfrak{S}_n$. L'idée générale est d'utiliser l'action de $\sigma \in \mathfrak{S}_n$ sur $\{1, \cdots, n\}$ afin d'obtenir le produit de cycles égal à σ.

1. On montre tout d'abord que σ s'écrit sous forme d'un produit de cycles

à supports disjoints. Soit A_i pour $i = 1, \cdots, r$, les σ-orbites. On a :

$$\{1, \cdots, n\} = \coprod_{i=1}^{r} A_i.$$

Pour tout $i \in \{1, \cdots, r\}$, on définit $c_i \in \mathfrak{S}_n$ tel que :

$$c_i(x) := \begin{cases} \sigma(x) & \text{si } x \in A_i \\ x & \text{sinon.} \end{cases}$$

Alors c_i est soit l'identité soit un cycle de longueur plus grand (ou égal) à 2. En effet, si $x \notin A_i$ alors la c_i-orbite de x est $\{x\}$ (elle est donc triviale) et si $x \in A_i$, la c_i-orbite de x est A_i. On voit facilement que $\sigma = c_1 c_2 \cdots c_n$. En effet, soit $x \in \{1, \cdots, n\}$ et supposons que $x \in A_i$ alors pour tout $j \neq i$, on a $c_j(x) = x$ et aussi $c_j(\sigma(x)) = \sigma(x)$ car $\sigma(x) \in A_i$. Il suit que $c_1 c_2 \cdots c_n(x) = \sigma(x)$. Donc σ se décompose en produit de cycles et ils sont bien à supports disjoints (le support de chaque c_i non trivial étant A_i).

2. Il faut maintenant montrer l'unicité. Supposons que σ s'écrivent $d_1 \cdots d_s$ où les d_j sont des cycles de support B_j, disjoints 2 à 2. Soit x un élément du support B_j. Comme les supports des cycles sont disjoints, seul d_j a un effet sur x. On a donc $\sigma(x) = d_j(x)$ donc pour tout $k \in \mathbb{Z}$, $\sigma^k(x) = d_j^k(x)$. Donc B_j est une orbite A_i de σ. Quitte à réindexer les A_i, on obtient donc $A_j = B_j$ et $c_j = d_j$.

□

Ainsi, tout élément de $\mathfrak{S}_n$ pourra s'écrire comme un produit de cycles c'est à dire un produit d'éléments notés $(a_1, \cdots, a_k)$. Ceci nous fournit ainsi une deuxième notation possible pour écrire un élément de $\mathfrak{S}_n$. Notons aussi que si σ est un produit de r cycles de longueur k_i avec $i \in \{1, \cdots, r\}$ à support disjoints alors l'ordre de σ est le plus petit commun multiple des ordres des cycles, donc le plus petit commun multiple des k_i.

Exemple.

1. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} \in \mathfrak{S}_4$ s'écrit aussi $(1,2)(4,5)$ comme produit de cycles à supports disjoints. L'ordre de σ est donc $\text{ppcm}(2,2) = 2$.
2. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 8 & 6 & 5 & 4 & 3 & 7 & 1 \end{pmatrix} \in \mathfrak{S}_8$ s'écrit aussi $(1,2,8)(3,6)(4,5)$ comme produit de cycles à supports disjoints. L'ordre de σ est donc $\text{ppcm}(3,2,2) = 6$.

Théorème 4.2.3 *Toute permutation (non égale à l'identité) de $\mathfrak{S}_n$ avec $n \geq 2$ se décompose en un produit de transpositions.*

Preuve. Utilisant la proposition précédente, il suffit de montrer que tout cycle se décompose en produit de transpositions, c'est à dire en produits de cycles de longueur 2. On montre ceci par récurrence sur la longueur r du cycle. Si $r = 2$, la propriété est évidente car un cycle de longueur 2 est une transposition. Supposons la propriété vérifiée pour les cycles de longueur r et montrons-la pour les cycles de longueur $r + 1$. Soit $(\beta_1, \cdots, \beta_{r+1})$ un tel cycle, alors :

$$(\beta_1, \cdots, \beta_{r+1}) = (\beta_1, \beta_{r+1})(\beta_1, \cdots, \beta_r).$$

Comme par récurrence $(\beta_1, \cdots, \beta_r)$ s'écrit comme un produit de transpositions, on a le résultat.

□

Donc les transpositions engendrent $\mathfrak{S}_n$: tout élément de $\mathfrak{S}_n$ peut s'écrire comme produit d'élements de la forme (i, j). Notons que comme $(i, j) = (1, j)(1, i)(1, j)$, il suit que tout élément de $\mathfrak{S}_n$ peut s'écrire comme produit d'élements de la forme $(1, k)$.

La démonstration nous montre comment obtenir la décomposition de n'importe quel élément de $\mathfrak{S}_n$ en produit de transpositions. On le fait sur les exemples suivants.

Exemple.

1. On a :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 8 & 6 & 5 & 4 & 3 & 7 & 1 \end{pmatrix} = (1, 2, 8)(3, 6)(4, 5)$$

   Or $(1, 2, 8) = (1, 8)(1, 2)$ donc $\sigma = (1, 8)(1, 2)(3, 6)(4, 5)$.

2. Soit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 6 & 4 & 3 & 1 & 7 & 10 & 2 & 9 \end{pmatrix} \in \mathfrak{S}_{10}$$

   Tout d'abord, on a $\sigma = (1, 5, 3, 6)(2, 8, 10, 9)$. Ensuite, on a d'une part :

$$(1, 5, 3, 6) = (1, 6)(1, 5, 3) = (1, 6)(1, 3)(1, 5)$$

   et d'autre part

$$(2, 8, 10, 9) = (2, 9)(2, 8, 10) = (2, 9)(2, 10)(2, 8).$$

   On obtient :

$$\sigma = (1, 6)(1, 3)(1, 5)(2, 9)(2, 10)(2, 8).$$

4.3 Signature

Nous avons vu que'une permutation quelconque pouvait se décomposer en produit de transpositions. Cependant cette décomposition n'est pas unique d'après les exemples effectués. Nous allons voir que la parité du nombre de facteur dans une telle décomposition reste néanmoins invariante.

Définition 4.3.1 Soit $\sigma \in \mathfrak{S}_n$ et soit t, le nombre de σ-orbites, on appelle *signature* de σ le nombre $\varepsilon(\sigma) = (-1)^{n-t}$.

En particulier, une transposition a une signature -1 et un cycle de longueur k une signature égale à $(-1)^{k-1}$.

Proposition 4.3.2 *Pour toute permutation τ de $\mathfrak{S}_n$ et pour toute transposition σ de $\mathfrak{S}_n$, on a $\varepsilon(\tau\sigma) = -\varepsilon(\tau)$.*

Preuve. Supposons que $\sigma = (a, b)$ où a et b sont dans $\{1, \cdots, n\}$. Pour obtenir les orbites suivant $\tau\sigma$ à partir de celle de τ, seules les orbites contenant a et b seront modifié puisque sur les autres, la transposition σ agit comme l'identité. On distingue 2 cas.

1. Si a et b sont dans la même τ-orbite. Cette orbite O est alors de la forme :
$$O = \{a, \tau(a), \cdots, \tau^{r-1}(a)\},$$
avec $b = \tau^p(a)$ pour un certain $p \in \{1, \cdots, r-1\}$. Comme $\tau\sigma(a) = \tau(b) = \tau^{p+1}(a)$, l'orbite de a suivant $\tau\sigma$ est alors :
$$\{a, \tau^{p+1}(a), \cdots, \tau^{r-1}(a)\}.$$
L'orbite de b suivant $\tau\sigma$ est :
$$\{b, \tau(a), \cdots, \tau^{p-1}(a)\}.$$
Il suit que l'orbite O est remplacé par deux orbites suivant $\tau\sigma$. Dans ce cas, on a bien $\varepsilon(\tau\sigma) = -\varepsilon(\tau)$.
2. Si a et b ne sont pas dans la même τ-orbite. Soit O l'orbite de a et O' l'orbite de b. On a :
$$O = \{a, \tau(a), \cdots, \tau^{r-1}(a)\},$$
$$O' = \{b, \tau(b), \cdots, \tau^{s-1}(b)\}.$$
On vérifie que l'orbite de a sous $\tau\sigma$ est alors :
$$\{a, \tau(b), \cdots, \tau^{s-1}(b), b, \tau(a), \cdots, \tau^{r-1}(a)\}.$$
Il suit donc que O et O' se réunissent en une seule orbite suivant $\tau\sigma$. Là encore, on obtient $\varepsilon(\tau\sigma) = -\varepsilon(\tau)$.

□

Corollaire 4.3.3 *Soit $\sigma \in \mathfrak{S}_n$ et soit $\sigma = t_1 \cdots t_k$ une décomposition de σ en produit de transpositions. Alors $\varepsilon(\sigma) = (-1)^k$.*

Preuve. C'est une récurrence immédiate utilisant la proposition précédente. □

Proposition 4.3.4 *La signature est un homomorphisme de groupes surjectif de $\mathfrak{S}_n$ dans $\{\pm 1\}$ (pour $n \geq 2$).*

Preuve. Si σ est le produit de s transpositions et σ' de s' transpositions, $\sigma\sigma'$ est le produit de $s + s'$ transpositions. Donc :

$$\varepsilon(\sigma\sigma') = (-1)^{s+s'} = (-1)^s(-1)^{s'} = \varepsilon(\sigma)\varepsilon(\sigma).$$

Donc ε est bien un homomorphisme de groupes. Il est surjectif car la signature de l'identité est 1, celle de n'importe quelle transposition est -1.

□

Exemple.

1. On pose :
$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 8 & 6 & 5 & 4 & 3 & 7 & 1 \end{pmatrix} \\ &= (1,8)(1,2)(3,6)(4,5).\end{aligned}$$
Alors la signature de σ est $(-1)^4 = 1$.
2. On pose
$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 6 & 4 & 3 & 1 & 7 & 10 & 2 & 9 \end{pmatrix} \\ &= (1,6)(1,3)(1,5)(2,9)(2,10)(2,8).\end{aligned}$$
Alors la signature de σ est $(-1)^6 = 1$.

Pour ces deux exemples, on vérifie que le calcul de la signature en considérant le nombre d'orbites ou la décomposition en cycles est cohérent avec ces résultats.

Définition 4.3.5 Soit $n \geq 2$. On appelle *le groupe alterné* le noyau de la signature. On le note $\mathfrak{A}_n$.

Proposition 4.3.6 *Soit $n \geq 2$, alors $\mathfrak{A}_n$ est un sous-groupe normal de $\mathfrak{S}_n$ d'indice 2.*

Preuve. $\mathfrak{A}_n$ est un sous-groupe de $\mathfrak{S}_n$ qui est normal car c'est le noyau d'un homomorphisme. On a $\mathfrak{S}_n/\mathfrak{A}_n \simeq \{\pm 1\}$ donc on a $[\mathfrak{S}_n : \mathfrak{A}_n] = 2$.

□

Ce groupe alterné est particulièrement important en théorie des groupes. Par exemple, pour $n \geq 5$, on peut montrer que ce groupe fait partie des groupes finis simples (cela se montre en utilisant les théorèmes de Sylow).

Chapitre 5

Produits directs et Produits semi-directs

5.1 Produits directs

Soit I un ensemble non vide et soit $\{G_i\}_{i\in I}$ une famille de groupes indexée par I. Le produit direct $G := \prod_{i\in I} G_i$ est par définition l'ensemble des familles $\{x_i\}_{i\in I}$ avec $x_i \in G_i$. Pour tout $j \in J$, on dispose d'une application :

$$\begin{array}{rccc} p_j : & \prod_{i\in I} G_i & \to & G_j \\ & (x_i)_{i\in I} & \mapsto & x_j \end{array}$$

appelée *projection.* La proposition suivante ne pose pas de difficulté (à faire en exercice).

Proposition 5.1.1 *Le produit direct est naturellement muni d'une structure de groupe suivant la loi de composition :*

$$\begin{array}{ccc} \prod_{i\in I} G_i \times \prod_{i\in I} G_i & \to & \prod_{i\in I} G_i \\ ((x_i)_{i\in I}, (y_j)_{j\in I}) & \mapsto & (x_i y_i)_{i\in I} \end{array}$$

Selon cette loi, il est clair que $G := \prod_{i\in I} G_i$ est commutatif si et seulement si tous les G_i le sont. La proposition suivante est triviale.

Proposition 5.1.2 *Selon les notations ci-dessus, les projections p_j sont des homomorphisme de groupes.*

En particulier, remarquons que le noyau de la projection p_j est un sous-groupe de G et il est isomorphe à $\prod_{i\in I\setminus\{j\}} G_i$.

Exemple : $\mathbb{Z}^n$ est le produit direct de n copies de $\mathbb{Z}$.

On se pose maintenant la question suivante : quand est-ce qu'un groupe est isomorphe au produit direct de deux de ses sous-groupes ?

Il y a une réponse évidente : il est clair que tout groupe G est isomorphe à $\{e\} \times G$ ou encore à $G \times \{e\}$. On va alors reformuler la question : quand un groupe est-il isomorphe au produit direct de deux sous-groupes non triviaux ?

Soit G produit direct de G_1 et G_2. On remarque que G_1 est isomorphe au sous-groupe $H_1 = \{(x, e_{G_2}),\ x \in G_1\}$ et G_2 à $H_2 = \{(e_{G_1}, x),\ x \in G_2\}$. On a en particulier les propriétés suivantes :

1. Pour tout $h_1 \in H_1$ et $h_2 \in H_2$, on a $h_1 h_2 = h_2 h_1$.
2. $H_1 \cap H_2 = \{e_G\}$.
3. $G = H_1 H_2$.

Réciproquement, supposons que l'on dispose de deux sous-groupes H_1 et H_2 de G vérifiant les 3 propriétés ci-dessus. On va montrer que G est alors naturellement isomorphe à $H_1 \times H_2$. On a une application naturelle :

$$\begin{array}{rccc} \psi : & H_1 \times H_2 & \to & G \\ & (h_1, h_2) & \mapsto & h_1 h_2 \end{array}$$

ψ est un morphisme de groupes. En effet, pour $(h_1, h_2) \in H_1 \times H_2$ et $(h_1', h_2') \in H_1 \times H_2$, on a d'une part :

$$\psi(h_1, h_2)\psi(h_1', h_2') = h_1 h_2 h_1' h_2' = h_1 h_1' h_2 h_2,'$$

d'après (1) et d'autre part :

$$\psi((h_1, h_2)(h_1', h_2')) = \psi(h_1 h_1', h_2 h_2') = h_1 h_1' h_2 h_2.$$

Enfin, ψ est bijective. Soit $g \in G$. Alors, d'après (3), il existe $h_1 \in H_1$ et $h_2 \in H_2$ tels que $g = h_1 h_2$. Cette décomposition est en fait unique, en effet si il existe $h_1' \in H_1$ et $h_2' \in H_2$ tels que $g = h_1' h_2'$, on aurait $h_1 h_2 = h_1' h_2'$ d'où ${h_1'}^{-1} h_1 = h_2' h_2^{-1}$. Ce dernier élément est dans H_1 et H_2 donc $h_1 = h_1'$ et $h_2 = h_2'$ d'après (2).

On en déduit donc que ψ est un isomorphisme de groupes. Dans la mesure où l'isomorphisme est canonique, on peut identifier les 2 groupes et noter $G = H_1 \times H_2$. On a donc montré le théorème suivant :

Théorème 5.1.3 *Soit G un groupe et soit H_1 et H_2 deux sous-groupes de G. Alors $G = H_1 \times H_2$ si et seulement si*

1. *Pour tout $h_1 \in H_1$ et $h_2 \in H_2$, on a $h_1 h_2 = h_2 h_1$.*

2. $H_1 \cap H_2 = \{e_G\}$.
3. $G = H_1 H_2$.

On a une autre caractérisation équivalente :

Proposition 5.1.4 *Soit G un groupe et soient H_1 et H_2 deux sous-groupes de G. Alors $G = H_1 \times H_2$ si et seulement si*

1. $H_1 \lhd G$ *et* $H_2 \lhd G$.
2. $H_1 \cap H_2 = \{e_G\}$.
3. $G = H_1 H_2$.

Preuve. Il suffit de montrer que les 3 propriétés du théorème sont équivalentes aux trois propriétés du théorème 5.1.3. Supposons donc que l'on a

1'. Pour tout $h_1 \in H_1$ et $h_2 \in H_2$, on a $h_1 h_2 = h_2 h_1$.
2'. $H_1 \cap H_2 = \{e\}$.
3'. $G = H_1 H_2$.

Alors, H_1 est un sous-groupe normal de G. En effet, si $h_1 \in H_1$ et si $g \in G$ alors, d'apres (3′), il existe $h_1' \in H_1$ et $h_2' \in H_2$ tel que $g = h_1' h_2'$. D'après (3′), on obtient :

$$g h_1 g^{-1} = h_1' h_2' h_1 {h_2'}^{-1} (h_1')^{-1} = h_1' h_2' {h_2'}^{-1} h_1 (h_1')^{-1} = h_1' h_1 {h_1'}^{-1}$$

Donc on a $g \in H_1$, il suit $g H_1 g^{-1} \subset H_1$ et donc H_1 est un sous-groupe normal de G. On fait de même pour H_2 et on obtient (1). (2) est la même propriété que (2′) et (3) se déduit de (3′)

Réciproquement, supposons que H_1 et H_2 soient deux sous-groupes de G vérifiant (1), (2) et (3). Soient $h_1 \in H_1$ et $h_2 \in H_2$. Considérons l'élément $h_1^{-1} h_2^{-1} h_1 h_2$ de G. On a :

- d'une part, $h_2 \in H_2$ et $h_1^{-1} h_2^{-1} h_1 \in H_2$ car $H_2 \lhd G$ donc $h_1^{-1} h_2^{-1} h_1 h_2 \in H_2$
- d'autre part, $h_1^{-1} \in H_1$ et $h_2^{-1} h_1 h_2 \in H_1$ car $H_1 \lhd G$ donc $h_1^{-1} h_2^{-1} h_1 h_2 \in H_1$

Donc $h_1^{-1} h_2^{-1} h_1 h_2 \in H_1 \cap H_2$ et donc d'après (2), on obtient $h_1 h_2 = h_2 h_1$. (2′) et (3′) sont alors évident.

□

Un exemple classique de produit direct mais très important est donnée par la proposition suivante

Proposition 5.1.5 (Lemme Chinois) *Si p et q sont premiers entre eux, on a un isomorphisme :*

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

Preuve. On considère l'application suivante :

$$\begin{array}{rccc} \theta : & \mathbb{Z}/pq\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ & m(\text{mod } pq) & \mapsto & (m(\text{mod } p), m(\text{mod } q)) \end{array}$$

Cette application est bien définie : si $m \equiv m'(\text{mod } pq)$ alors $m = m' + pqk$ pour $k \in \mathbb{Z}$ donc $m \equiv m'(\text{mod } p)$ et $m \equiv m'(\text{mod } q)$. Φ est clairement un homomorphisme de groupes. Il est injectif car si $m \equiv 0(\text{mod } p)$ alors $m = 0$ ou p divise m et si $m \equiv 0(\text{mod } q)$ alors $m = 0$ ou q divise m. Comme p et q sont premiers entre eux, on a $m = 0$ ou pq divise m donc $m \equiv 0(\text{mod } pq)$. On conclut que θ est un isomorphisme en remarquant que les ordres des deux groupes sont les mêmes.

□

5.2 Produit semi-direct

Le produit semi-direct est une variante affaiblie du produit direct. La définition reprend la caractérisation de la proposition 5.1.4 excepté que H_2 n'est plus forcément distingué dans G.

Définition 5.2.1 Soit G un groupe et soit H_1 et H_2 deux sous-groupes de G. Alors on dit que G est *produit semi-direct* de H_1 et H_2 et on note $G = H_1 \rtimes H_2$ si et seulement si

1. $H_1 \lhd G$,
2. $H_1 \cap H_2 = \{e_G\}$,
3. $G = H_1 H_2$.

Les 2 dernières conditions nous assurent qu'un élément quelconque $g \in G$ s'écrit uniquement sous la forme $h_1.h_2$ avec $h_1 \in H_1$ et $h_2 \in H_2$. De même que pour le produit direct, on pourra alors le noter (h_1, h_2). Cependant, la loi interne sur $H_1 \rtimes H_2$ n'est plus définie de la même manière que pour le produit direct du fait que H_2 n'est pas nécessairement normal. Comment alors multiplier deux éléments $(h_1, h_2) \in H_1 \rtimes H_2$ et $(h'_1, h'_2) \in H_1 \rtimes H_2$?

Pour ceci, il s'agit d'écrire $h_1 h_2 h'_1 h'_2$ sous la forme d'un élément de H_1 multiplié par un élément de H_2. On a :

$$h_1 h_2 h'_1 h'_2 = h_1 h_2 h'_1 h_2^{-1} h_2 h'_2$$

Or, H_1 est normal donc l'élément $h_2 h'_1 h_2^{-1}$ est un élément de H_1. Donc $h_1 h_2 h'_1 h_2^{-1} \in H_1$. De plus, $h_2 h'_2 \in H_2$. Il suit donc que la loi interne dans $H_1 \rtimes H_2$ est donné par :

$$(h_1, h_2)(h'_1, h'_2) = (h_1 h_2 h'_1 h_2^{-1}, h_2 h'_2).$$

On voit en particulier que si tout élément de H_1 commute avec tout élément de H_2, le produit est en fait direct.

Exemple. On considère le groupe symétrique $\mathfrak{S}_n$ avec $n \geq 2$. Soit la transposition $\tau = (1,2) \in \mathfrak{S}_n$, l'ensemble $H_2 = \{1, \tau\}$ est un sous-groupe de $\mathfrak{S}_n$ car $\tau^2 = \mathrm{Id}$. On considère le groupe alterné $H_1 := \mathfrak{A}_n$. C'est aussi un sous-groupe de $\mathfrak{S}_n$.

1. H_1 est un sous-groupe normal de $\mathfrak{S}_n$ car c'est le noyau de la signature (et on sait que le noyau d'un homomorphisme de groupes est normal).
2. On a $H_1 \cap H_2 = \{e_G\}$. En effet τ n'est pas dans H_1 car sa signature est -1 et par définition, la signature d'un élément de H_1 est 1.
3. On a $\mathfrak{S}_n = H_1 H_2$. En effet, $H_1 H_2 = \{h_1 h_2 \mid h_1 \in H_1,\ h_2 \in H_2\}$ est un sous-esnemble de $\mathfrak{S}_n$. Il comporte $n!$ éléments distincts car H_1 est de cardinal $n!/2$, H_2 de cardinal 2 et un élément de la forme $\sigma\tau$ avec $\sigma \in H_1$ ne peut être dans H_1 car sa signature est -1. Ainsi, on a $H_1 H_2 \subset \mathfrak{S}_n$ et les deux ensembles ont même cardinal d'où l'égalité.

Donc, $\mathfrak{S}_n$ est produit semi-direct de H_1 et H_2.

5.3 Complément 1 : Produit semi-direct externe

Dans la section précédente, nous avons vu que sous certaines hypothèses, la structure d'un groupe G était entièrement déterminée par la structure et les relations entre deux de ses sous-groupes. Dans ce cas, on a dit que G était le produit semi-direct de ces deux sous-groupes.

Nous allons généraliser ici ces résultats de façon à définir le produit semi-direct de deux groupes quelconques. Cette définition est donnée grâce à la proposition suivante.

Proposition 5.3.1 *Soit N et H deux groupes et soit $Aut(N)$ le groupe des automorphismes de N. Soit $\phi : H \to Aut(N)$ un morphisme. On définit alors sur l'ensemble $N \times H$ une loi par :*

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

pour $(n,h) \in N \times H$ et $(n',h') \in N \times H$. Alors, via cette loi, $N \times H$ est naturellement muni d'une structure de groupe appelée le produit semi-direct et notée $N \rtimes_\phi H$ ou plus simplement $N \rtimes H$.

Preuve. On vérifie facilement que la loi ci-dessus est bien définie.

– Elle est de plus associative : soient $(n,h) \in N \times H$, $(n',h') \in N \times H$ et $(n",h") \in N \times H$. Alors :

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

Il suit ainsi :

$$((n,h)(n',h'))\,(n",h") = (n.\phi(h)(n').\phi(hh')(n"), hh'h"),$$

et d'autre part :

$$(n',h')(n",h") = (n'.\phi(h')(n"), h'h"),$$

et donc :

$$(n,h)\,((n',h')(n",h")) = (n.\phi(h)(n'.\phi(h')(n")), hh'h").$$

$\phi(h)$ est un automorphisme donc

$$\phi(h)(n'.\phi(h')(n")) = \phi(h)(n')\phi(h)(\phi(h')(n")).$$

De plus, comme ϕ est un morphisme de groupes, on a $\phi(h)(\phi(h')) = \phi(hh')$. Il suit

$$((n,h)(n',h'))\,(n",h") = (n,h)\,((n',h')(n",h"))\,.$$

– L'élément neutre est (e_N, e_H) (e_N étant l'élément neutre de N et e_H l'élément neutre de H). En effet, pour $(n,h) \in N \times H$, on a $(n,h)(e_N,e_H) = (n.\phi(h)(e_N), h)$. Or $\phi(h)(e_N) = e_N$ car $\phi(h)$ est un automorphisme d'où $(n,h)(e_N,e_H) = (n,h)$. D'autre part, on a $(e_N,e_H)(n,h) = (e_N.\phi(e_H)(n), h)$. Or ϕ est un morphisme donc $\phi(e_H)$ est l'élément neutre de $\mathrm{Aut}(N)$ c'est à dire l'identité. Il suit $(e_N,e_H)(n,h) = (e_N,e_H)$.
– Soit $(n,h) \in N \times H$. Alors :

$$(n,h)(\phi(h^{-1})(n^{-1}), h^{-1}) = (n\phi(h)(\phi(h^{-1})(n^{-1})), e_H) = (e_N, e_H),$$

d'où l'inverse de (n,h) est $(\phi(h^{-1})(n^{-1}), h^{-1})$.

Donc l'opération ci-dessus définit bien une structure de groupe sur $N \times H$. □

Notons que pour pouvoir définir un produit semi-direct entre deux groupes N et H, il est nécessaire de bien connaître l'ensemble $\mathrm{Aut}(N)$ ce qui est un problème délicat en général ...

Nous devons maintenant montrer que cette définition est bien cohérente avec les propriétés et les définitions de la section précédente. Soit donc N et

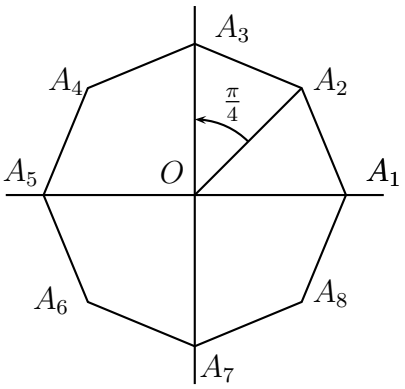
H deux groupes et $\phi : H \to \mathrm{Aut}(N)$ un morphisme. On considère le groupe $N \rtimes_\phi H$. Considérons l'ensemble $\overline{N} := \{(n, 1) \mid n \in N\} \subset N \rtimes_\phi H$. Il est immédiat de vérifier que c'est un sous-groupe de $N \rtimes_\phi H$ et que de plus ce sous-groupe est isomorphe à N. On vérifie facilement que ce sous-groupe est normal.

On peut faire (pratiquement) la même remarque pour H : l'ensemble $\overline{H} := \{(1, h) \mid h \in H\} \subset N \rtimes_\phi H$ est un sous-groupe de $N \rtimes_\phi H$ isomorphe à H. Par contre il n'est pas nécessairemet normal.

Enfin, on a évidemment $N \cap H = \{(e_N, e_H)\}$ et $\overline{N}.\overline{H} = N \rtimes_\phi H$. On a donc bien généralisé la deuxième section.

5.4 Complément 2 : Le groupe diédral

Soit $n \geq 3$ et soit $\mathcal{P}_n$ un polygône régulier dans $\mathbb{R}^2$ et de centre $(0, 0)$. Rappelons qu'une isométrie est une application linéaire bijective de $\mathbb{R}^2$ qui conserve les distances. Par définition, *le groupe diédral* $\mathcal{D}_n$ est le groupe des isométrie laissant le polygône $\mathcal{P}_n$ invariant :



Proposition 5.4.1 *Le groupe diédral est engendré par la rotation $r_{(O,\frac{2\pi}{n})}$ de centre O et d'angle $\dfrac{2\pi}{n}$ et par la symétrie $s_{(OA_1)}$ d'axe (OA_1) où A_1 est un sommet du polygône. En particulier, $\mathcal{D}_n$ est d'ordre $2n$.*

Preuve. Soit $g \in \mathcal{D}_n$. On note $\{A_1, A_2, ..., A_n\}$ les sommets du polygône numérotés de telle façon que $r_{(O,\frac{2\pi}{n})}(A_i) = A_{i+1}$ pour $i \in \{1, ..., k-1\}$ et $r_{(O,\frac{2\pi}{n})}(A_n) = A_1$. On considère deux cas :

- Supposons $g(A_1) = A_1$. Alors, comme g est linéaire et que $g(O) = O$, tous les points de la droite (OA_1) sont invariants par g. Donc g est soit l'identité soit la symétrie $s_{(OA_1)}$ d'axe (OA_1).

– Supposons que $g(A_1) = A_k$ pour $k \neq 1$. On a $r^{k-1}_{(O,\frac{2\pi}{n})}(A_1) = A_k$ d'où $r^{1-k}_{(O,\frac{2\pi}{n})} \circ g(A_1) = A_1$ et il suit que d'après le premier cas $r^{1-k}_{(O,\frac{2\pi}{n})} \circ g$ est soit l'identité soit la symétrie d'axe (OA_1). Ainsi, g s'écrit comme produit de $s_{(OA_1)}$ et $r_{(O,\frac{2\pi}{n})}$.

On en déduit ainsi que les éléments de $\mathcal{D}_n$ sont :

$$\mathrm{Id}, s_{(OA_1)}, r_{(O,\frac{2\pi}{n})}, r_{(O,\frac{2\pi}{n})} \circ s_{(OA_1)} \ ... \ r^{n-1}_{(O,\frac{2\pi}{n})}, r^{n-1}_{(O,\frac{2\pi}{n})} \circ s_{(OA_1)}$$

Donc l'ordre de $\mathcal{D}_n$ est $2n$

□

Proposition 5.4.2 *On a :*

$$D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}.$$

Preuve. Posons $N =< r_{(O,\frac{2\pi}{n})} >$ et $H =< s_{(OA_1)} >$. Alors, il est clair que H est isomorphe au groupe cyclique $\mathbb{Z}/2\mathbb{Z}$ ($s_{(OA_1)}$ est d'ordre 2) et que N est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ car $r_{(O,\frac{2\pi}{n})}$ est d'ordre n. Il reste donc à montrer les 3 propriétés de la définition 5.2.1 . Il est clair que $N \cap H = \{\mathrm{Id}\}$ et que $NH = \mathcal{D}_n$. En effet, d'après la preuve de la proposition, tous les éléments de $\mathcal{D}_n$ s'écrivent sous la forme $r^i_{(O,\frac{2\pi}{n})} \circ s^j_{(OA_1)}$ avec $i \in \{0, ..., n-1\}$ et $j \in \{0, 1\}$. Il reste donc à montrer que N est normal dans $\mathcal{D}_n$. Soit donc $g \in \mathcal{D}_n$ alors $g = r^i_{(O,\frac{2\pi}{n})} \circ s^j_{(OA_1)}$ pour $i \in \{0, ..., n-1\}$ et $j \in \{0, 1\}$. On a :

$$g \circ r_{(O,\frac{2\pi}{n})} \circ g^{-1} = r^i_{(O,\frac{2\pi}{n})} \circ s^j_{(OA_1)} \circ r_{(O,\frac{2\pi}{n})} \circ s^{-j}_{(OA_1)} \circ r^{-i}_{(O,\frac{2\pi}{n})}$$

Si $j = 0$, le résultat est évident : on a $g \circ r_{(O,\frac{2\pi}{n})} \circ g^{-1} \in N$. Remarquons que $r^i_{(O,\frac{2\pi}{n})}$ et $s_{(OA_1)}$ sont caractérisé par :

$$r^i_{(O,\frac{2\pi}{n})}(A_l) = A_{l+i} \qquad \text{et} \qquad s_{(OA_1)}(A_l) = A_{n-l+2},$$

pour tout $l \in \{1, 2, ..., n\}$ et où on a posé $A_{k+n} := A_k$.

Si $j = 1$, on vérifie facilement que pour tout $l \in \{1, 2, ..., n\}$, on a

$$g \circ r_{(O,\frac{2\pi}{n})} \circ g^{-1}(A_l) = A_{l-1} = A_{l+n-1}.$$

Donc $g \circ r_{(O,\frac{2\pi}{n})} \circ g^{-1} = r^{n-1}_{(O,\frac{2\pi}{n})}$. Comme N est engendré par $r_{(O,\frac{2\pi}{n})}$, il suit $gNg^{-1} \subset N$ donc N est normal dans $\mathcal{D}_n$. On conclut donc que $\mathcal{D}_n$ est isomorphe au produit semi-direct de N et de H d'où le résultat.

□