Université Pierre et Marie Curie
Master de Sciences et Technologies
Mention *Mathématiques et Applications*
Spécialité *Education et Formation*, Section CAPES, M1
Année 2011 - 2012

GROUPES

1. Définitions et exemples

1.1. L'étude des équations algébriques au début du 19ième siècle a amené les mathématiciens à une nouvelle notion : celle de groupe. Cette notion joue maintenant un rôle central en mathématiques et pas seulement en mathématiques.

Exemples préparant l'introduction de la notion de groupe : l'ensemble des isométries d'un polygone régulier (on munit cet ensemble de l'opération de composition), l'ensemble $\mathbb{Z}$ des nombres entiers (on munit cet ensemble de l'opération d'addition), l'ensemble $\mathbb{R}^*$ des nombres réels non nuls (on munit cet ensemble de l'opération de multiplication).

1.2. Définition d'un groupe. Pour un ensemble arbitraire G, une opération qui, à un couple de deux éléments quelconques de G, associe un élément de G s'appelle *opération interne* (ou *loi interne*) sur G. Par exemple, la composition est une opération interne sur l'ensemble des isométries d'un polygone régulier, l'addition est une opération interne sur l'ensemble $\mathbb{Z}$ des nombres entiers et la multiplication est une opération interne sur l'ensemble $\mathbb{N}$ des nombres naturels. Attention : l'ordre des éléments d'un couple est, en général, important pour le résultat de l'opération.

Un couple $(G, \cdot)$, où G est un ensemble et $\cdot$ est une opération interne sur G s'appelle *groupe* si

(1) il existe un élément e (appelé *élément neutre*) de G tel que, pour tout élément a de G on ait,
$$a \cdot e = e \cdot a = a,$$

(2) pour tout élément a de G, il existe un élément a' (appelé *inverse* de a) de G tel que
$$a \cdot a' = a' \cdot a = e,$$

(3) l'opération interne $\cdot$ est *associative*, c'est-à-dire, pour des éléments quelconques a, b et c de G, on a
$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Exemples. Le groupe des bijections d'un ensemble E, muni de la loi donnée par la composition des bijections (ce groupe est noté $(S_E, \circ)$), le groupe des translations d'un espace affine, le groupe des isométries affines d'un espace affine euclidien.

D'autres exemples :

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}^{+*}, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{U}, \times)$, où $\mathbb{U}$ est l'ensemble des nombres complexes de module 1,
$O_n(\mathbb{R})$, $SO_n(\mathbb{R})$, $GL_n(K)$, $SL_n(K)$, où n est un nombre entier strictement positif, et K est un corps.

On verra beaucoup d'autres exemples plus tard.

L'unicité d'élément neutre, l'unicité d'inverse. Écriture multiplicative. Tables de multiplication de groupes finis.

1.3. Sous-groupes. Soit $(G, \cdot)$ un groupe. Un *sous-groupe* H de G est un sous-ensemble $H \subset G$ tel que

(1) H contient e,
(2) H est stable par multiplication : si h_1 et h_2 sont des éléments de H, alors $h_1 \cdot h_2 \in H$,
(3) H est stable par inversion : si $h \in H$, alors $h^{-1} \in H$.

Un sous-groupe est un groupe à part entière.

Proposition. *Soit $\{H_i\}_{i \in I}$ une famille de sous-groupes d'un groupe G. Alors, l'intersection des sous-groupes H_i est un sous-groupe de G.*

Sous-groupe engendré par un sous-ensemble. Soit G un groupe, et soit A un sous-ensemble de G. Le sous-groupe $< A >$ de G *engendré par* A est l'intersection de tous les sous-groupes de G qui contiennent A.

Proposition. *L'ensemble $< A >$ coïncide avec l'ensemble des produits $g_1 \dots g_n$, où n est un nombre entier positif ou nul, et, pour tout $i = 1, \dots, n$, on a $a_i \in A$ ou $a_i^{-1} \in A$.* (On considère que le produit vide est égal à l'élément neutre de G.)

Exemple. Soit G un groupe, et soit g un élément de G. Pour tout nombre entier strictement positif n, le produit de g par lui-même n fois est noté g^n, et le produit de g^{-1} par lui-même n fois est noté g^{-n}. On convient que $g^0 = e$, où e est l'élément neutre de G. Alors, le sous-groupe engendré par $A = \{g\}$ coïncide avec $\{g^n, n \in \mathbb{Z}\}$.

2. Morphismes de groupes

Soient G et G' deux groupes. Un *morphisme* (de groupes) de G dans G' est une application $f : G \to G'$ telle que, pour tous éléments g_1 et g_2 dans G, on ait $f(g_1 g_2) = f(g_1) f(g_2)$.

Exemples.

- Si G est un groupe, et H est un sous-groupe de G, alors l'inclusion $i : H \to G$ est un morphisme de groupes.
- L'application *déterminant* $GL_n(K) \to K^*$ est un morphisme de groupes.
- L'exponentielle $\exp : \mathbb{R} \to \mathbb{R}^{+*}$ est un morphisme de groupes.

Proposition. *Soit $f : G \to G'$ un morphisme de groupes. Alors, f envoie l'élément neutre de G sur l'élément neutre de G'. Pour tout élément g de G, le morphisme f envoie g^{-1} sur $(f(g))^{-1}$.*

Noyau at image d'un morphisme. Soit $f : G \to G'$ un morphisme de groupes. Le *noyau* de f, noté $\ker(f)$, est l'ensemble des éléments g dans G tels que $f(g) = e'$, où e' est l'élément neutre de G'. L'*image* de f, notée $\mathrm{im}(f)$, est l'ensemble des éléments g' de G' tels qu'il existe $g \in G$ vérifiant $g' = f(g)$.

Proposition. *Pour tout morphisme de groupes $f : G \to G'$, le noyau $\ker(f)$ de f est un sous-groupe de G, et l'image $im(f)$ de f est un sous-groupe de G'.*

Proposition. *Soit $f : G \to G'$ un morphisme de groupes. Alors, f est injectif si et seulement si* $\ker(f) = \{e\}$*, où e est l'élément neutre de f.*

Si un morphisme de groupes $f : G \to G'$ est bijectif, on dit que f un *isomorphisme*. Si $f : G \to G$ est un isomorphisme de G dans G, on dit que f est un *automorphisme* de G. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G. Cet ensemble, muni de l'opération de composition, est un groupe (c'est un sous-groupe du groupe de bijections $(S_G, \circ)$).

Considérons maintenant des automorphismes très importants d'un groupe G : les *automorphismes intérieurs* ou *conjugaisons*. Pour un élément quelconque g de G, la *conjugaison* par g est l'application

$$\begin{aligned} c_g : G &\to G \\ x &\mapsto gxg^{-1}. \end{aligned}$$

Il est facile de voir que, pour tout élément g de G, l'application c_g est un morphisme de groupes : pour des éléments x et y quelconques de G, on a

$$c_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = c_g(x)c_g(y).$$

On note $\mathrm{Int}(G)$ l'ensemble des automorphismes intérieurs de G.

3. Classes à gauche et classes à droite modulo un sous-groupe

Dans toute cette section, G est un groupe et H est un sous-groupe de G.

Pour tout élément g de G, on considère deux applications :

- *translation à gauche* $t_{g,\text{gauche}} : G \to G$ définie par $t_{g,\text{gauche}}(x) = gx$,
- *translation à droite* $t_{g,\text{droite}} : G \to G$ définie par $t_{g,\text{droite}}(x) = xg$.

Attention : si g ne coïncide pas avec l'élément neutre de G, alors les applications $t_{g,\text{gauche}}$ et $t_{g,\text{droite}}$ ne sont pas des morphismes de groupes.

Proposition. *Pour tout élément g de G,*

- *les applications $t_{g,\text{gauche}}$ et $t_{g,\text{droite}}$ sont bijectives,*
- *l'application $g \mapsto t_{g,\text{gauche}}$ est un morphisme injectif de groupes de G dans S_G.*

En particulier, tout groupe G peut être vu comme un sous-groupe de S_G.

Attention : pour obtenir un morphisme de groupes $G \to S_G$ à l'aide de translations à droite, il faut considérer une application $g \mapsto t_{g^{-1},\text{droite}}$.

Proposition. *Soient x et y deux éléments de G. Alors, soit les ensembles $xH = t_{x,\text{gauche}}(H)$ et $yH = t_{y,\text{gauche}}(H)$ coïncident, soit ils sont disjoints.*

Démonstration. Supposons que $xH \cap yH \neq \emptyset$, et soit $z \in xH \cap yH$. Donc, il existe un élément h_1 de H tel que $xh_1 = z$, et il existe un élément h_2 de H tel que $yh_2 = z$. Donc, $x = z(h_1)^{-1} = yh_2(h_1)^{-1}$.

Soit s un élément quelconque de xH. Il existe un élément h de H tel que $xh = s$. Alors, $s = xh = yh_2(h_1)^{-1}h \in yH$, ce qui termine la démonstration. □

On définit une relation d'équivalence sur les éléments de G : deux éléments x et y de G sont équivalents si $xH = yH$. Ces classes d'équivalence s'appellent *classes à gauche modulo H*. L'ensemble des classes à gauche modulo H est noté G/H et

la surjection $\pi : G \to G/H$ qui à x associe sa classe xH est appelée *projection canonique*. Un *système de représentants* des classes à gauche est une partie de G contenant exactement un élément de chaque classe.

De façon similaire, on définit les classes à droite modulo H et l'ensemble $H\backslash G$.

4. Sous-groupes distingués et quotients

Tout sous-groupe H d'un groupe G peut être représenté comme image d'un morphisme de groupes. Par contre, il n'est pas vrai en général que tout sous-groupe H de G peut être représenté comme noyau d'un morphisme de groupes : les noyaux de morphismes sont des sous-groupes très particuliers.

Soit G un groupe. Un sous-groupe H de G est dit *distingué*, ou *normal*, si pour tout élément h de H et pour tout élément g de G, on a $ghg^{-1} \in H$. Lorsqu'un sous-groupe H de G est distingué, on écrit $H \triangleleft G$.

Un sous-groupe H est distingué si et seulement si il est invariant par tout automorphisme intérieur : pour tout élément g de G, on a $c_g(H) \subset H$.

Proposition. *Soit G un groupe, et soit $H \triangleleft G$ un sous-groupe distingué. Alors, les classes à gauche et à droite modulo H coïncident : on a $xH = Hx$ pour tout élément x de G (c'est-à-dire, $G/H = H\backslash G$). Réciproquement, si les classes à gauche et classes à droite modulo un sous-groupe H coïncident, alors H est un sous-groupe distingué.*

Démonstration. Supposons que le sous-groupe H est distingué. Soit x un élément de G. Alors, pour tout élément h de H, on a $xhx^{-1} \in H$, donc, $xh = xhx^{-1}x \in Hx$. Ceci montre que $xH \subset Hx$. On montre de la même manière que $Hx \subset xH$.

Supposons maintenant que $xH = Hx$ pour tout élément x de G. Alors, pour tout élément x de G, on a $xHx^{-1} = H$. □

Proposition. Soit $f : G \to G'$ un morphisme de groupes. Alors, le noyau $\ker(f)$ de f est un sous-groupe distingué de G.

Réciproquement, tout sous-groupe distingué d'un groupe G est le noyau d'un certain morphisme $f : G \to G'$.

Théorème. *Soit G un groupe, et soit H un sous-groupe distingué de G. Alors,*

(a) *il existe une unique structure de groupe sur l'ensemble quotient $G/H = H\backslash G$ telle que la projection canonique $\pi : G \to G/H$ soit un morphisme de groupes ;*

(b) *pour tout morphisme $f : G \to G'$ tel que $H \subset \ker(f)$, il existe un unique morphisme $\tilde{f} : G/H \to G'$ tel que $f = \tilde{f} \circ \pi$; le noyau de $\tilde{f}$ est l'image de $\ker(f)$ dans G/H ; en particulier, $\tilde{f}$ est injectif si et seulement si $H = \ker(f)$.*

Démonstration.
(a) Définissons une multiplication sur G/H. La projection canonique $\pi : G \to G/H$ est surjective. Donc, pour deux éléments quelconques x_1 et x_2 de G/H, on peut trouver des éléments g_1 et g_2 de G tels que $x_1 = \pi(g_1)$ et $x_2 = \pi(g_2)$. Si l'on veut

que π soit un morphisme de groupes, on doit avoir

$$x_1x_2 = \pi(g_1)\pi(g_2) = \pi(g_1g_2),$$

ce qui montre que l'on n'a pas le choix pour définir le produit de x_1 et x_2. Montrons que ce produit est indépendant des choix de g_1 et g_2 comme antécédents de x_1 et x_2. Si on choisit d'autres d'antécédents $\widehat{g}_1$ et $\widehat{g}_2$ de x_1 et x_2, respectivement, il existe des éléments h_1 et h_2 de H tels que $\widehat{g}_1 = g_1h_1$ et $\widehat{g}_2 = g_2h_2$. Comme $g_2^{-1}h_1g_2 \in H$, on a $g_2^{-1}h_1g_2h_2 \in H$, d'où

$$\pi(\widehat{g}_1\widehat{g}_2) = \pi(g_1h_1g_2h_2) = \pi(g_1g_2g_2^{-1}h_1g_2h_2) = \pi(g_1g_2).$$

Ceci montre que le produit x_1x_2 défini à l'aide d'antécédents de x_1 et x_2 est indépendant du choix de ces antécédents.

L'ensemble G/H, muni de la multiplication que l'on vient de définir, est un groupe. En effet, le role d'élément neutre est joué par la classe formée par les éléments de H. Si $x \in G/H$ et g est un élément de G tel que $\pi(g) = x$, alors l'inverse de x est $\pi(g^{-1})$. Finalement, l'associativité de la multiplication dans G/H est un corollaire immédiat de l'associativité de la multiplication dans G.

De plus, par construction, la projection canonique $\pi : G \to G/H$ est un morphisme de groupes.

(b) Soit $f : G \to G'$ un morphisme tel que $H \subset \ker(f)$. Pour tout élément x de G/H, on peut choisir un élément g de G tel que $x = \pi(g)$. En utilisant l'hypothèse $H \subset \ker(f)$, on obtient que l'élément de G' égal à $f(g)$ ne dépend pas du choix d'un antécédent g de x. On peut donc poser $\tilde{f}(x) = f(g)$. Ceci définit une application $\tilde{f} : G/H \to G'$. Pour voir que c'est un morphisme de groupes, soient x_1 et x_2 deux éléments de G/H, et soient g_1 et g_2 deux éléments de G tels que $x_1 = \pi(g_1)$ et $x_2 = \pi(g_2)$. Alors, g_1g_2 est un antécédent dans G de x_1x_2, d'où

$$\tilde{f}(x_1x_2) = f(g_1g_2) = f(g_1)f(g_2) = \tilde{f}(x_1)\tilde{f}(x_2).$$

Ceci montre que $\tilde{f}$ est un morphisme de groupes. Déterminons le noyau de $\tilde{f}$. Soit x un élément de $\ker(\tilde{f})$. Choisissons un élément g de G tel que $x = \pi(g)$. On a $f(g) = \tilde{f}(x) = e'$, où e' est l'élément neutre de G'. Donc, $g \in \ker(f)$ et x appartient à l'image de $\ker(f)$ dans G/H. Réciproquement, si y appartient à l'image de $\ker(f)$ dans G/H, alors $\tilde{f}(y) = e'$, c'est-à-dire, $y \in \ker \tilde{f}$. □

Corollaire. *Soit $f : G \to G'$ un morphisme surjectif de groupes, et soit $\tilde{f} : G/\ker(f) \to G'$ le morphisme tel que $\tilde{f} \circ \pi = f$, où $\pi : G \to G/\ker(f)$ est la projection canonique. Alors, $\tilde{f}$ est un isomorphisme.*

Exemple. Soit n un nombre entier strictement positif. Alors, le quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$ des multiples de n est le groupe bien connu $\mathbb{Z}/n\mathbb{Z}$.

5. Groupes ayant des propriétés particulières

5.1. Groupes abéliens.

On dit qu'un groupe G est *abélien* (ou *commutatif*), si, pour deux éléments quelconques g_1 et g_2 de G, on a $g_1g_2 = g_2g_1$.

Le groupe $\mathbb{Z}$ est abélien. Tout sous-groupe engendré par un élément est abélien. Le groupe des isométries d'un triangle équilatéral n'est pas abélien.

On dit que deux éléments g_1 et g_2 d'un groupe G *commutent* si $g_1 g_2 = g_2 g_1$. Le *centre* d'un groupe G est l'ensemble

$$\{g \in G \mid gg_0 = g_0 g \text{ pour tout } g_0 \in G\}.$$

Le centre de G est noté $Z(G)$. Remarquons que, pour tout groupe G, le centre $Z(G)$ de G est un sous-groupe distingué de G. En effet, $Z(G)$ est le noyau du morphisme de conjugaison $c : G \to \mathrm{Aut}(G)$ défini par $g \mapsto c_g$, où $c_g(x) = gxg^{-1}$ pour tout élément x de G.

Pour les groupes abéliens, l'opération interne est d'habitude notée additivement, c'est-à-dire avec le signe $+$. L'inverse est alors appelé l'*opposé* et l'élément neutre est noté 0.

5.2. Groupes monogènes.

Un groupe est dit *monogène* (ou *cyclique*) s'il peut être engendré par un élément (parfois, on réserve le qualificatif *cyclique* aux groupes monogènes finis).

Proposition. *Soit H un sous-groupe de $\mathbb{Z}$. Alors, il existe un nombre entier positif ou nul n tel que H coïncide avec $n\mathbb{Z}$, où*

$$n\mathbb{Z} = \{k \in \mathbb{Z} \mid \textit{il existe un nombre entier } d \textit{ tel que } k = nd\}.$$

Corollaire. *Tout groupe monogène est isomorphe soit à $\mathbb{Z}$, soit à $\mathbb{Z}/n\mathbb{Z}$ pour un certain nombre entier strictement positif n.*

Démonstration. Par hypothèse, il existe un élément x de G qui engendre G. Considérons l'application $f : \mathbb{Z} \to G$ définie par $k \mapsto x^k$. C'est un morphisme surjectif de groupes. Si f est injectif, c'est un isomorphisme entre $\mathbb{Z}$ et G. Si f n'est pas injectif, il existe un nombre entier strictement positif n tel que $\ker(f) = n\mathbb{Z}$. Alors, f induit un isomorphisme $\tilde{f} : \mathbb{Z}/n\mathbb{Z} \to G$. □

5.3. Groupes finis.

Un groupe G est dit *fini* si son ensemble sous-jacent est fini. L'*ordre* (ou *cardinal*) d'un groupe G est le nombre de ses éléments si le groupe est fini, et est égal à l'infini sinon. On le note $|G|$, $\mathrm{card}(G)$ ou $\mathrm{ord}(G)$. L'ordre d'un élément g d'un groupe G est l'ordre du sous-groupe engendré par g dans G. L'ordre d'un élément g est noté $\mathrm{ord}(g)$.

Pour tout nombre entier strictement positif n, le groupe des bijections de l'ensemble $\{1, \dots, n\}$ est noté S_n (plutôt que $S_{\{1,\dots,n\}}$). Il est appelé *groupe symétrique*. L'ordre de ce groupe est égal à $n!$.

Théorème. *Soit n un nombre entier strictement positif. Tout groupe fini d'ordre n se plonge dans le groupe symétrique S_n.*

La démonstration est basée sur les deux observations suivantes :

- l'application de G dans S_G définie par $g \mapsto t_{g,\text{gauche}}$ est un morphisme injectif de groupes,
- toute bijection entre G et $\{1, 2, \dots, n\}$ produit un isomorphisme entre S_G et S_n.

Soit G un groupe, et soit H un sous-groupe de G. L'*indice* de H dans G est le cardinal (éventuellement infini) de l'ensemble quotient G/H. L'indice de H dans G est noté $(G : H)$ ou $[G : H]$.

Théorème (Lagrange). *Soit G un groupe fini, et soit H un sous-groupe de G. Alors, on a $|G| = (G : H)|H|$. En particulier, le cardinal d'un sous-groupe divise le cardinal du groupe. De plus, si K est un sous-groupe de G tel que $K \subset H$, alors $(G : K) = (G : H)(H : K)$.*

Corollaire. *Soit G un groupe fini. On pose $n = \mathrm{ord}(G)$. Alors, pour tout élément x de G, on a $x^n = e$, où e est l'élément neutre de G.*

6. Actions de groupes

Soit G un groupe, et soit X un ensemble. Une *action* de G sur X est un morphisme de groupes $\rho : G \to S_X$ du groupe G vers le groupe S_X des bijections de X. Si $\rho : G \to S_X$ est une action de G sur X, alors

(1) $\rho(e) = \mathrm{id}_X$, où e est l'élément neutre de G et $\mathrm{id} : X \to X$ est l'application identité de X ;
(2) $\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2)$ pour deux éléments quelconques g_1 et g_2 de G.

En général, on écrit ρ_g ou simplement g au lieu de $\rho(g)$, et gx ou $g.x$ au lieu de $\rho_g(x)$. Souvent, les éléments de X sont appelés *points*.

Exemples.

- Soit G un groupe. Les translations à gauche dans G donnent lieu à un morphisme injectif $G \to S_G$ qui est une action de G sur lui-même (c'est-à-dire, ici $X = G$).
- Soit K un corps, et soit V un espace vectoriel sur K. Le groupe $G = GL(V)$ des automorphismes linéaires de V agit sur V, sur l'ensemble des droites de V (par $\rho_g(d) = g(d)$ pour tout élément g de G et toute droite d de V), sur l'ensemble des endomorphismes linéaires de V (par $\rho_g(f) = g \circ f$ pour tout élément g de G et tout endomorphisme linéaire $f : V \to V$).
- Le groupe des isométries affines d'un espace affine euclidien agit sur l'espace lui-même, sur l'ensemble de ses triangles, sur l'ensemble de ses droites, sur l'ensemble de ses cercles ...

Soit G un groupe agissant sur un ensemble X. Un sous-ensemble Y de X est dit *stable*, ou *invariant*, sous G, si, pour tout élément g de G, on a $g(Y) \subset Y$.

Remarque. Une action d'un groupe G sur un ensemble X permet souvent de fabriquer d'autres actions en considérant des groupes reliés à G ou des ensembles reliés à X. Par exemple,

(1) pour tout sous-groupe H de G, il y a une action restreinte de H sur X obtenue par la composition $H \hookrightarrow G \to S_X$;
(2) si un sous-ensemble Y de X est stable sous G, il y a une action induite de G sur Y. (Attention : pour un sous-ensemble quelconque Y de X, l'ensemble des éléments g de G tels que $g(Y) \subset Y$ n'est pas forcement un sous-groupe de G.)

Soit G un groupe agissant sur un ensemble X. L'*orbite* d'un point x de X sous le groupe G (ou le G-*orbite* de x), est le sous-ensemble $\mathcal{O}_G(x) = \{gx \mid g \in G\}$ de X.

Si Y est un sous-ensemble de X, alors le *stabilisateur* de Y dans G est le sous-groupe de G composé des éléments g tels que $g(Y) = Y$. (La vérification du fait qu'il s'agit d'un sous-groupe est un exercice facile.) En particulier, le stabilisateur d'un point x de X est le sous-groupe G_x de G défini par $G_x = \{g \in G \mid gx = x\}$.

Si Y est un sous-ensemble de X, alors le *fixateur* de Y dans G est le sous-groupe de G composé des éléments g de G tels que, pour tout point y de Y, on ait $g(y) = y$. Le fixateur de Y est donc l'intersection des stabilisateurs G_y des points $y \in Y$. Lorsque Y est un point, le stabilisateur de Y coïncide avec le fixateur de Y.

Exemple. Soit $G = \mathbb{Z}/2\mathbb{Z}$, et soit $X = \mathbb{R}^2$. Considérons l'application $\rho : G \to S_{\mathbb{R}^2}$ définie par

$$0 \mapsto \mathrm{id}_{\mathbb{R}^2}, \quad 1 \mapsto f,$$

où $\mathrm{id}_{\mathbb{R}^2}$ est l'application identité de $\mathbb{R}^2$ et $f(x, y) = (x, -y)$ pour tout point (x, y) de $\mathbb{R}^2$. Cette application est un morphisme de groupes, il s'agit donc d'une action de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{R}^2$. Le fixateur (et le stabilisateur) de l'axe $y = 0$ est le groupe $\mathbb{Z}/2\mathbb{Z}$ tout entier. L'axe $x = 0$ est un sous-ensemble stable de $\mathbb{R}^2$ (sous l'action considérée de $\mathbb{Z}/2\mathbb{Z}$), mais le fixateur de cet axe est le sous-groupe trivial $\{0\} \subset \mathbb{Z}/2\mathbb{Z}$.

Soit G un groupe agissant sur un ensemble X. Pour tout point x de X, considérons l'application $\mathrm{ev}_x : G \to X$ définie par $g \mapsto g(x)$. Nous l'appellerons l'*application d'évaluation en x*.

Théorème. *Soit G un groupe agissant sur un ensemble X. Alors, pour tout point x de X, l'application d'évaluation en x induit une bijection entre G/G_x et $\mathcal{O}_G(x)$.*

Démonstration. Soit x un point de X. Par définition de l'orbite, l'image de ev_x est l'orbite $\mathcal{O}_G(x)$. Donc, ev_x est une application surjective de G dans $\mathcal{O}_G(x)$. Pour cette application, deux éléments g et h ont la même image si et seulement si $g^{-1}h \in G_x$. Par conséquent, d'après la définition de l'ensemble quotient G/G_x, l'application ev_x induit une application bijective entre G/G_x et $\mathcal{O}_G(x)$. $\square$

Corollaire. Si un groupe fini G agit sur un ensemble X, alors, pour tout point x de X, l'orbite de x sous G est finie et son cardinal est égal à l'indice de G_x dans G.

Soit G un groupe agissant sur un ensemble X. Considérons la relation binaire sur X définie de la façon suivante : $x \sim y$ si et seulement si il existe un élément g de G tel que $y = gx$. C'est une relation d'équivalence. Deux points x et y de X appartiennent à la même classe d'équivalence si et seulement si $\mathcal{O}_G(x) = \mathcal{O}_G(y)$, c'est-à-dire, les classes d'équivalence pour cette relation sont les orbites de l'action de G sur X. La partition en classes pour la relation d'équivalence considérée est appelée la *partition en orbites* de X.

Exemple. Soit G un groupe, et soit H un sous-groupe de G. Les classes à gauche de G modulo H peuvent être vues comme les orbites d'une action de H sur G. En effet, considérons l'action de H sur G donnée par les translations à droite : $\rho : H \to S_G$ et $\rho_h(g) = gh^{-1}$. Alors, pour tout élément g de G, l'orbite de g est la classe gH. (Attention : pour une action générale, les classes de la partition en orbites n'ont pas toujours le même nombre d'éléments.)

On dit que l'action d'un groupe G sur un ensemble X est *transitive* s'il n'y a qu'une seule orbite de l'action de G sur X. Ceci signifie que pour deux points quelconques x et y de X, il existe un élément g de G tel que $y = gx$, ou encore, que, pour tout point x de X, l'application d'évaluation $\mathrm{ev}_x : G \to X$ est surjective.

Par exemple, en partant d'une action quelconque d'un groupe G sur un ensemble X, et d'un point quelconque x de X, on obtient une action de G sur l'orbite $\mathcal{O}_G(x)$ de x, et cette action est transitive.

Soit G un groupe agissant sur un ensemble X, et soit x un point de X. Si $\mathcal{O}_G(x) = \{x\}$, on dit que l'orbite de x est *ponctuelle*, ou *réduite à un point*, ou *triviale*. Dans ce cas, on dit que x est un *point fixe* sous G.

7. Groupes symétriques et groupes alternés

7.1. Groupes symétriques.

Soit E un ensemble. On appelle *groupe symétrique* de E le groupe S_E des bijections de E. Si n est un nombre entier strictement positif et $E = \{1, ..., n\}$, le groupe symétrique de E est noté simplement S_n. Les éléments du groupe symétrique S_n sont traditionnellement appelés *permutations*.

Une façon de représenter une permutation σ appartenant à S_n est d'indiquer sur une ligne tous les entiers de 1 à n, et sur une ligne située en-dessous, les images de ces entiers par σ.

Pour tout nombre entier strictement positif n, le groupe symétrique S_n agit naturellement sur l'ensemble $\{1, \dots, n\}$. Lorsqu'on étudie le groupe S_n, on utilise souvent le vocabulaire des actions de groupes. Chaque permutation $\sigma \in S_n$ a des orbites (les σ-orbites), qui sont les orbites dans $\{1, \dots, n\}$ de l'action du groupe $G =< \sigma >\subset S_n$.

Une permutation $\sigma \in S_n$ qui possède une et une seule orbite non ponctuelle dans son action sur $\{1, \dots, n\}$ est appelée un *cycle*. Si r est le cardinal de l'orbite non ponctuelle d'un cycle σ, on dit que σ est un *r-cycle*. Un 2-cycle est aussi appelé *transposition*.

Soit n un nombre entier strictement positif, et soit $\sigma \in S_n$ une permutation. On dit que $i \in \{1, \dots, n\}$ est un *point fixe* de σ si $\sigma(i) = i$. On note $\mathrm{Fix}(\sigma)$ l'ensemble des points fixes de σ dans $\{1, \dots, n\}$. On appelle *support* de σ (et on note $\mathrm{Supp}(\sigma)$) le complémentaire dans $\{1, \dots, n\}$ de l'ensemble des points fixes de σ.

Un cycle est donc une permutation dont le support est non vide et est une orbite. Notons que, d'après la définition, l'identité n'est pas un cycle.

Soit n un nombre entier supérieur ou égal à 2. Pour tout nombre entier i entre 1 et n, l'ensemble des permutations qui fixent le point i est le stabilisateur de i pour l'action de S_n sur $\{1, \dots, n\}$. C'est un sous-groupe ; il est facile de voir qu'il s'identifie au sous-groupe des permutations de $\{1, \dots, i-1, i+1, \dots, n\}$; ce dernier sous-groupe est isomorphe à S_{n-1}.

Proposition. *Soit n un nombre entier strictement positif, et soient σ et τ deux permutations appartenant à S_n et dont les supports sont disjoints. Alors, σ et τ commutent : $\sigma\tau = \tau\sigma$.*

Théorème (Décomposition en cycles à supports disjoints). *Soit n un nombre entier strictement positif. Alors, toute permutation dans S_n s'écrit de manière unique, à l'ordre des facteurs près, comme produit de cycles à supports disjoints.*

Ceci mène à une autre manière d'écrire les permutations. Un cycle est noté en indiquant entre des parenthèses les images successives d'un point de son orbite non ponctuelle ; par exemple la notation (138) désigne le 3-cycle tel que $\sigma(1) = 3$,

$\sigma(3) = 8$ et $\sigma(8) = 1$. Dans cette notation, les points fixes du cycle n'apparaissent pas. Une permutation est notée en juxtaposant les écritures des différents cycles de sa décomposition en cycles à supports disjoints, par exemple la notation (138)(25) désigne le produit du 3-cycle (138) et la transposition (25).

Théorème. *Pour tout nombre entier supérieur ou égal à* 2*, le groupe symétrique* S_n *est engendré par les transpositions. Plus précisément, toute permutation dans* S_n *peut s'écrire comme produit d'au plus* $n-1$ *transpositions.*

7.2. Groupes alternés.

Soit n un nombre entier supérieur ou égal à 2.

Théorème. *Il existe un unique morphisme de groupes surjectif* $\varepsilon : S_n \to \{1, -1\}$.

Le morphisme de ce théorème est appelé la *signature*. Son noyau est appelé le *groupe alterné* et noté A_n. Une permutation de signature 1 est dite *paire*, et une permutation de signature -1 est dite *impaire*. Une permutation dans S_n est pair si et seulement si elle s'écrit comme produit d'un nombre pair de transpositions.