1 Introduction à la théorie des groupes

On sait que l'ensemble $\mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$ est muni de deux opérations usuelles à savoir : L'addition et la multiplication. Un espace vectoriel est aussi muni d'une opération de telle sorte : L'addition de deux vecteurs. Cela donne un nouveau moyen de mieux comprendre ces ensembles et mieux encore : de les classifier. Ainsi, avec ces opérations, on a ce qu'on appellera des structures algébriques sur ces ensembles. Ainsi notre but est de formaliser ces idées de manière abstraite.

1.0.1 Définition

Soit E un ensemble. Une opération binaire (ou loi de composition interne) $\star$ sur E est définie par l'application :

$$\begin{array}{ccc} E \times E & \mapsto & E \\ (x, y) & \mapsto & x \star y \end{array}$$

Autrement dit, pour tout x et y éléments de E, $x \star y$ est un élément de E et il est défini de manière unique. Un ensemble E muni d'une opération $\star$ sera noté par $(E, \star)$. S'il n'y a pas de confusion, l'opération $x \star y$ sera notée tout simplement par xy. Si T est une partie de E, on dit que l'opération est fermée sur T, si la restriction de l'application sur $T \times T$ a pour image dans T. Autrement dit, pour tout x et y dans T, on a $x \star y \in T$. On dit aussi que la loi de composition sur T est interne.Un opération binaire sur un ensemble E définit de ce qu'on appellera une structure algébrique sur E. Autrement dit, on dit que $(E, \star)$ est une structure algébrique.

1.0.2 Exemples

1. L'addition, la soustraction et la multiplication sont des opérations binaires sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$;
2. La soustraction n'est une loi de composition interne sur $\mathbb{N}$;
3. L'addition et la multiplication des matrices carrées sont des opérations binaires ;
4. L'addition et la soustraction de vecteurs sont des opérations binaires sur les espaces vectoriels;
5. Le produit vectoriel de deux vecteurs sur $\mathbb{R}^3$ est une opération binaire sur $\mathbb{R}^3$;
6. La loi de composition d'applications est une opération binaire sur l'ensemble $\mathbb{R}^R$ des applications numériques ;
7. L'addition est une loi de composition interne sur l'ensemble des nombres paires ;
8. L'addition n'est pas une loi de composition interne sur l'ensemble des nombres impaires.

En primaire, on a appris les tables d'additions et de multiplications sur l'ensemble des entiers naturels. Ci dessous est une tentative de formaliser cet idée sur un ensemble fini :

1.0.3 Définition

Soit $(E, \star)$ un ensemble fini muni de l'opération binaire $\star$. Le tableau qui présente, pour tout élément x et y de E, les résultats qu'on obtient par la loi $\star$ est appelé table de Cayley de $(E, \star)$.

1.0.4 Exemples

Soit $(\{-1, 0, 1\}, \times)$ un ensemble où $\times$ est la multiplication usuelle sur $\mathbb{Z}$. Son table de Cayley est le suivant :

$\times$	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

Voici quelques caractéristiques usuelles d'une opération binaire sur un ensemble :

1.0.5 Définition

Soit $(E, \star)$ un ensemble. On dit que :

i) La loi $\star$ est associative si pour tout x, y et z dans E, on a $x \star (y \star z) = (x \star y) \star z$;

ii) La loi $\star$ est commutative si pour tout a et b dans E, on a $a \star b = b \star a$;

iii) E admet un élément neutre ou un identité e si pour tout $x \in E$, on a $e \star x = x \star e = x$;

iv) Supposons que E admet un élément neutre e. Un élément t de E admet un inverse s'il existe un élément u de E tel que $t \star u = u \star t = e$.

1.0.6 Proposition

Soit $(E, \star)$ une structure algébrique admettant un élément neutre. Alors :

i) L'élément neutre est unique ;

ii) Si de plus, l'opération est associative, l'inverse d'un élément inversible est unique.

L'inverse d'un élément inversible x de E sera noté par x^{-1}.
Démonstration:

i) Supposons qu'on a deux éléments neutres e_1 et e_2. Par définition, on a $e_1 \star e_2 = e_1 = e_2 \star e_1 = e_2$. D'où $e_1 = e_2$, i.e, l'élément neutre est unique.

ii) Soit x un élément inversible de E. Désignons par e l'élément neutre. Supposons qu'ils existent deux inverses de y_1 et y_2 de x. Par définition, on a : $x \star y_1 = e = x \star y_2$. Donc, en multipliant cet égalité par y_1 à gauche, on a, par associativité de l'opération binaire, $(y_1 \star x) \star y_1 = (y_1 \star x) \star y_2$. D'où, $y_1 = y_2$.

1.1 Introduction et Définitions

1.1.1 Définition

Une structure algébrique $(E, \star)$ est dite un monoïde si elle admet un élément neutre et la loi de composition interne $\star$ est associative. Si de plus, tout élément de E admet un inverse, alors la structure $(E, \star)$ est appelé un groupe. Une structure de groupe est dite abélienne si la loi de composition est aussi commutative. On dit dans ce cas que le groupe est abélien.

1.1.2 Remarque

Si $(E, \star)$ est un monoïde, l'ensemble E est non vide.

1.1.3 Proposition

Soient $(M_1, \star_1)$ et $(M_2, \star_2)$ deux monoïdes d'éléments neutres respectifs e_1 et e_2. Considérons l'opération binaire $\star$ sur l'ensemble produit $G := M_1 \times M_2$ définie par :

$$\begin{array}{ccc} G \times G & \to & G \\ ((a,x),(b,y)) & \mapsto & (a,x) \star (b,y) := (a \star_1 b, x \star_2 y). \end{array}$$

La structure $(G, \star)$ est un monoïde d'élément neutre (e_1, e_2). C'est ainsi qu'on définit une structure algébrique sur un produit cartésien de deux ensembles.

1.1.4 Exemples

1. $(R, \star)$ est un monoïde ;
2. $(\mathbb{N}, +)$ n'est pas un groupe mais c'est un monoïde ;
3. $(\mathbb{Z}\backslash\{0\}, \times)$ est un monoïde, mais pas un groupe ;
4. Soit $n \geq 3$. Les structures $(\mathbb{Z}/n\mathbb{Z}\backslash\{0\}, \times)$ et $(M_n(\mathbb{R})\backslash\{0\}, \times)$ ne sont pas de groupes en général mais des monoïdes ;
5. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens ;
6. $(\mathbb{R}^2, +)$ est un groupe abélien ;
7. Soit n un entier naturel non nul. Les structures $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(M_n(\mathbb{R}), +)$ sont des groupes abéliens ;
8. Soient n et m deux entiers naturels non nuls. La structure $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$ est un groupe abélien ;
9. Si V est un espace vectoriel, la structure $(V, +)$ est un groupe abélien ;
10. L'ensemble des rotations de centre $(0, 0)$ sur $\mathbb{R}^2$ définit un groupe abélien avec la loi composition des transformations ;
11. L'ensemble des applications numériques bijectives définit un groupe non abélien avec la loi de composition des applications ;
12. L'ensemble $GL_n(\mathbb{R})$ des matrices carrées inversibles d'ordre $n \geq 2$ à coefficients dans $\mathbb{R}$ définit un groupe non abélien avec la loi multiplication des matrices ;
13. Soit E un ensemble fini. L'ensemble $P(E)$ des applications bijectives de E dans E définit un groupe avec la loi de composition des applications. On appelera cet groupe, le groupe de permutation de l'ensemble E. Si E est de cardinal n, on notera cet groupe par S_n.

Dans toute la suite, on ne s'intéressera qu'à des structures de groupes. C'est l'objectif principal de notre cours d'algèbre 1 même si l'étude des monoïdes est une branche très riche de l'algèbre abstraite.

1.1.5 Définition

Soient $(G, \star)$ un groupe et H une partie de G. On dit que H est un sous-groupe de G si $(H, \star)$ est un groupe. Si H est un sous-groupe de G, on le notera par $H < G$.

1.1.6 Proposition

Soit $(G, \star)$ un groupe. Une partie H de G est un sous-groupe de G si et seulement si les propositions suivantes sont vérifiées :

i) Pour tout x et y dans H, on a $x \star y \in H$;

ii) L'élément neutre de G est dans H;

iii) Si x est un élément de H, l'inverse x^{-1} de x dans G appartient à H. Autrement dit, une partie non-vide H de $(G, \star)$ est un sous-groupe de G si et seulement si pour tout x et y dans H, on a $x \star y^{-1}$ appartient à H.

1.1.7 Exemples

Soit n un entier naturel non nul.

1. Si $(G, \star)$ est un groupe d'identité e, les parties G et $\{e\}$ sont des sous-groupes de G. On les appelle les sous-groupes triviaux de G. Un sous groupe non trivial de G sera appelé un sous-groupe propre de G;

2. $\mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$ sont des sous-groupes de $(\mathbb{C}, +)$;

3. Le sous-ensemble $n\mathbb{Z}$ des multiples de n dans $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$;

4. Le sous-ensemble des matrices d'ordre n à coefficient dans $\mathbb{R}$ dont le déterminant est égal à 1 est un sous-groupe de $GL_n(\mathbb{R})$. Ce sous-groupe sera noté par $SL_n(\mathbb{R})$ et sera appelé le groupe linéaire spécial.

5. Soit $E = \{1, 2, \cdots, n\}$. Le groupe S_n est un sous groupe de S_{n+1}. Si $k \in \{1, 2, \cdots, n\}$, le sous ensemble des éléments qui fixe k dans $P(E)$ est un sous-groupe de S_n;

6. Si $n \leq 3$, les sous groupes triviaux sont les seuls sous groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$;

7. Le sous ensemble $\{0, 2\}$ est le seul sou groupe propre de $(\mathbb{Z}/4\mathbb{Z}, +)$;

8. Les sous ensembles $\{(0, 0), (0, 1)\}$ et $\{(0, 0), (1, 0)\}$ sont les seuls sous groupes propres de $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$.

1.1.8 Proposition

Soient H et K deux sous groupes d'un groupe G. Alors, le sous-ensemble $H \cap K$ est un sous groupe de G. Mais, en général, le sous ensemble $H \cup K$ de G n'est pas un sous groupe de G. Soient $(G, \star)$ un groupe et g un élément de G. Considérons le sous-ensemble $< g >$ de G défini par :

$$< g >:= \{g^k : k \in \mathbb{Z}\}$$

où $g^k := g \star g \star \cdots \star g$, k fois si $k \geq 1$, $g^0 := e$, l'identité de G et on a $g^k := (g^{-1})^{-k}$ si k est strictement négatif.

1.1.9 Proposition

Le sous ensemble $< g >$ est un sous groupe de G. Plus précisément, si $H < G$ contenant l'élément g, alors $< g >$ est un sous groupe de H. On dit dans ce cas que $< g >$ est le sous groupe cyclique engendré par g.
Démonstration: Vérifions les critères de sous-groupes mentionnées dans la Proposition 2.12 :

i) Soient x et y deux éléments de $< g >$. Par définition, ils existent n et m deux entiers tels que $x = g^n$ et $y = g^m$. Ainsi, $xy = g^{n+m}$. D'où $xy \in < g >$.

ii) Par définition, $g^0 = e$. Donc, l'élément neutre est dans $< g >$.

iii) Soit $x \in < g >$. Par définition il existe un entier i tel que $g^i = x$. De plus, $x \star g^{-i} = g^0 = e$. Donc, g^{-i} est l'inverse de x. Par définition, $g^{-i} \in < g >$.

1.1.10 Exemples

1. Soit n un entier naturel non nul. Le sous groupe $n\mathbb{Z}$ est un sous groupe cyclique de $\mathbb{Z}$ engendré par n;

2. Le sous ensemble $\{0, 5, 10, 15\}$ est un sous groupe cyclique de $(\mathbb{Z}/20\mathbb{Z}, +)$ engendré par 5.

1.1.11 Définition

On dit qu'un groupe G est cyclique s'il est engendré par un de ces éléments.

1.1.12 Proposition

Soit n un entier non nul. Les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z}, +)$ sont cycliques.
Démonstration: Ces groupes sont engendrés respectivement par 1 et $\dot{1}$

1.1.13 Définition

Soient G un groupe et g un élément de G. Le nombre d'éléments de G qu'on notera par $|G|$ est appelé ordre du groupe G. On appellera l'ordre du groupe $< g >$, l'ordre de l'élément g qu'on notera par $|g|$. Ainsi, si le groupe G est fini, l'ordre de G n'est autre que le cardinal de G. Sinon, l'ordre de G est infini.

1.2 Homomorphismes de Groupes

1.2.1 Définition

Un tableau carré à n lignes remplies par n éléments distincts dont chaque ligne et chaque colonne ne contient qu'un seul de ces éléments est appelé carré latin.

1.2.2 Exemples

1. Un sudoku est un carré latin ;

2. Le table de Cayley du groupe $(\mathbb{Z}/6\mathbb{Z}, +)$ est un carré latin ;

3. Le table de Cayley du monoïde $(\mathbb{Z}/6\mathbb{Z}, \times)$ n'est pas un carré latin.

1.2.3 Proposition

Le table de Cayley d'un groupe fini est un carré latin.
Maintenant examinons les tables de Cayley des groupes : $(\mathbb{Z}/2\mathbb{Z}, +)$ et $(\{1, -1\}, \times)$. Le table deCayley de $(\mathbb{Z}/2\mathbb{Z}, +)$ est :

$+$	0	1
0	0	1
1	1	2

tandis que celui de $(\{-1, 1\}, \times)$ est la suivant :

$\times$	-1	1
-1	1	-1
1	-1	1

A première vue, ces groupes sont différents. Les ensembles ne sont pas les mêmes, ni les structures. Mais les tables de Cayley correspondants sont similaires à celui du groupe $(\{a, b\}, \star)$ dont le table de Cayley est le suivant :

$\star$	a	b
a	a	b
b	b	a

Dans ce cas, on dit que les groupes $(\mathbb{Z}/2\mathbb{Z}, +)$ et $(\{1, -1\}, \times)$ sont isomorphes. Ainsi, l'idée est de comparer deux structures. Mais, pour cela, l'existence d'une application entre les deux ensembles qui définissent les groupes ne suffira pas. Il nous faut aussi un minimum de "compatibilité" entre les deux structures.La généralisation de manière formelle de ces idées est l'objet de cette section.

1.2.4 Introduction et Définitions

1.2.5 Définition

Soient $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes. Une application f de G_1 dans G_2 qui est compatible aux structures de deux groupes est appelée homomorphisme de groupes. Plus précisément, l'application f de G_1 dans G_2 est un homomorphisme si pour tout x et y éléments de G_1, on a :

$$f(x \star_1 y) = f(x) \star_2 f(y).$$

Si de plus, l'application f est bijective, on dit que f est un isomorphisme et on note par $G_1 \simeq G_2$.

1.2.6 Exemples

1. Soit $(G, \star)$ un groupe. L'identité Id_G est un isomorphisme ;
2. L'injection canonique $(\mathbb{Z}, +) \mapsto (\mathbb{R}, +)$ est un homomorphisme ;
3. L'application $(\mathbb{Z}/2\mathbb{Z}, +) \mapsto (1, -1, \times),\ x \mapsto (-1)^x$ est un isomorphisme ;
4. La surjection canonique $(\mathbb{Z}, +) \mapsto (\mathbb{Z}/n\mathbb{Z}, +)$ est un homomorphisme ;
5. L'application $(GL_n(\mathbb{R}), \times) \mapsto (\mathbb{R}\backslash\{0\}, \times),\ A \mapsto det(A)$ est un homomorphisme;
6. Une application linéaire entre deux espaces vectoriels est un homomorphisme ;
7. L'application exponentielle induit un isomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+\backslash\{0\}, \times)$.

1.2.7 Proposition

Soient $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes. Si f est un homomorphisme de G_1 dans G_2, alors :

i) $f(e_1) = e_2$, où e_1 et e_2 sont respectivement les identités de G_1 et G_2;

ii) Si $\bar{x}$ est l'inverse d'un élément x de G_1, alors $f(\bar{x})$ est l'inverse de $f(x)$ dans G_2.

Démonstration:

i) Par définition, on a $f(e_1) = f(e_1 \star_1 e_1) = f(e_1) \star_2 f(e_1)$. L'élément $f(e_1)$ deG_2 est inversible. Donc, en multipliant cet inverse à gauche, on a : $e_2 = f(e_1)$;

ii) On a $e_1 = x \star_1 \bar{x}$. Donc, $e_2 = f(e_1) = f(x \star_1 \bar{x}) = f(x) \star_2 f(\bar{x})$. D'où le résultat.

1.2.8 Proposition

Soient $(G_1, \star_1), (G_2, \star_2)$ et $(G_3, \star_3)$ des groupes. Soient $f : G_1 \to G_2$ et $g : G_2 \to G_3$ deux homomorphismes. Alors :

i) $g \circ f : G_1 \to G_3$ est un homomorphisme ;

ii) Si de plus f est bijective, l'inverse de f est aussi un isomorphisme.

1.2.9 Corollaire

La relation d'isomorphisme entre groupes est une relation d'équivalence.

1.2.10 Définition

Soit $f : (G_1, \star_1) \to (G_2, \star_2)$ un homomorphisme de groupes. Le sous ensemble $Im(f)$ de G_2 défini par :

$$Im(f) := \{f(x) : x \in G_1\}$$

est appelé l'image de f tandis que le sous ensemble $Ker(f)$ de G_1 défini par :

$$Ker(f) := \{x \in G_1 : f(x) = e_2\}$$

est appelé le noyau de f où e_2 est l'identité de G_2.

1.2.11 Proposition

Soient $f : (G_1, \star_1) \to (G_2, \star_2)$ un homomorphisme de groupes, H_1 un sous groupe de G_1 et H_2 un sous groupe de G_2. Alors :

i) $Im(f)$ est un sous groupe de G_2 ;

ii) $Ker(f)$ est un sous groupe de G_1 ;

iii) L'image réciproque $f^{-1}(H_2)$ est un sous groupe de G_1 ;

iv) Mais, l'image directe $f(H_1)$ n'est pas un sous groupe en général ;

v) Si de plus f est injective, on a $Ker(f) = \{e_1\}$ où e_1 est l'identité de G_1. L'application f définit ainsi un isomorphisme de G_1 dans $Im(f)$.

1.2.12 Groupes Quotients

Soient $(G, \star)$ un groupe et H un sous groupe de G. Pour tout élément x de G, on définit les ensembles $x \star H$ et $H \star x$ comme suit :

$$x \star H := \{x \star h : h \in H\};\ H \in x := \{h \star x : h \in H\}.$$

S'il n'y a pas de confusions, on écrit gH et Hg. La relation binaire $\mathcal{R}_g$ (resp. $\mathcal{R}_d$) définit pour tout a et b par :

$$a\mathcal{R}_g b\ (resp.\ a\mathcal{R}_d b) \Leftrightarrow aH = bH\ (resp.\ Ha = Hb)$$

est une relation d'équivalence sur G. Autrement dit,

$$a\mathcal{R}_g b\ (resp.\ a\mathcal{R}_d b) \Leftrightarrow b^{-1}a \in H\ (resp.\ ab^{-1} \in H).$$

Ainsi, on a :

1.2.13 Lemme

Soient $(G, \star)$ et H un sous groupe de G. Alors :

i) Pour tout x et y dans G, on a : Soit $xH = yH\ (resp.\ Hx = Hy)$, soit $xH \cap yH = \emptyset\ (resp.\ Hx \cap Hy = \emptyset)$;

ii) Pour tout $x \in G$, l'application $H \mapsto xH,\ x \mapsto xh (resp. H \mapsto Hx,\ x \mapsto hx)$ est bijective.

Démonstration:

i) Il suffit de montrer que les relations $\mathcal{R}_g$ et $\mathcal{R}_d$ sont des relations d'équivalences ;

ii) Considérons la relation $\mathcal{R}_g$. On applique le même raisonnement pour la relation $\mathcal{R}_d$. **Injectivité** : Soient h_1 et h_2 deux éléments de H tels que $xh_1 = xh_2$. Comme G est un groupe, l'élément x est inversible. En multipliant cet égalité à gauche par x^{-1}, on a $h_1 = h_2$. Donc,l'application est injective ;
Surjective : Soit $y \in xH$. Par définition, il existe $h \in H$ tel que $y = xh$. Donc, l'application est surjective.

1.2.14 Théorème (Théorème de Lagrange)

Soient G un groupe fini et H un sous groupe de G. On a :

$$|G| = [G : H]|H|$$

où $[G : H] := |G/\mathcal{R}_g| = |G/\mathcal{R}_d|$. L'entier $[G : H]$ est appelé l'indice de H dans G. En particulier, $|H|$ divise $|G|$.
Démonstration:
Comme G est un ensemble fini, donc les ensembles $G/\mathcal{R}_g$ et $G/\mathcal{R}_d$ sont finis. Or, les relations $\mathcal{R}_g$ et $\mathcal{R}_d$ sont des relations d'équivalences. Donc, les ensembles $G/\mathcal{R}_g$ et $G/\mathcal{R}_d$ forment respectivement une partition de l'ensemble G. De plus, d'après le lemme précédent, pour tout x et y dans G, on a :

$$|H| = |xH| = |yH|\ (resp.\ |H| = |Hx| = |Hy|).$$

D'où : $|G| = [G : H]|H|$ où $[G : H] := |G/\mathcal{R}_g| = |G/\mathcal{R}_d|$. L'exemple suivant est fondamental :
Considérons le groupe S_3 et l'application bijective f élément de S_3 définie par : $\sigma(1) = 2, \sigma(2) = 1$ et $\sigma(3) = 3$. Le sous ensemble $H = \{Id_{\{1,2,3\}}, \sigma\}$ est un sous groupe de S_3 . Considérons l'élément$\tau \in S_3$ défini par : $\tau(1) = 3, \tau(2) = 2$ et $\tau(3) = 1$. Ainsi, on peut vérifier qu'on a :

$\tau H \neq H\tau$. Supposons de plus qu'il existerait un homomorphisme de groupes $f : S_3 \to G$ telle que $H = Ker(f)$. Par définition, on a $f(\sigma) = e_G$, l'identité de G. De plus, on a :

$$\begin{aligned} f(\tau\sigma\tau^{-1}) &= f(\tau)f(\sigma)f(\tau^{-1}) \\ &= f(\tau)e_G(f(\tau))^{-1} \\ &= f(\tau)(f(\tau))^{-1} = e_G \end{aligned}$$

, i.e, $\tau\sigma\tau^{-1} \in H$. Autrement dit, on a $\tau H\tau^{-1} = H$. Ce qui contredit le fait que $\tau H \neq H\tau$. D'où : H ne peut pas être le noyau d'un homomorphisme de S_3 vers n'importe quel groupe. En effet,

1.2.15 Proposition

Soit $f : G_1 \to G_2$ un homomorphisme de groupes. Pour tout $x \in G_1$, on a :

$$xKer(f) = Ker(f)x.$$

Autrement dit, pour tout $x \in G$ et $h \in Ker(f)$, on a : $xhx^{-1} \in Ker(f)$ ou bien pour tout $x \in G$, on a $xKer(f)x^{-1} = Ker(f)$.

De manière générale ;

1.2.16 Proposition

Soient G un groupe et H un sous groupe de G. Les deux propositions suivantes sont équivalentes :

i) $G/\mathcal{R}_g = G/\mathcal{R}_d$;

ii) Pour tout $x \in G$, on a $xH = Hx$ (ou bien $xHx^{-1} = H$).

Si l'une de deux propositions est vérifiée, les deux ensembles quotients induits par les deux relations d'équivalences coïncident et on le notera par G/H.

Démonstration:

Supposons qu'on a $G/\mathcal{R}_g = G/\mathcal{R}_d$. Soit $x \in G$. Par hypothèse, il existe $y \in G$ tel que $xH = Hy$. Comme H est un sous groupe, l'identité e de G est dans H. Donc, $x = xe \in Hy$, i.e, il existe $h \in H$ tel que $x = hy$. En multipliant ce dernier égalité à droite par y^{-1}, on a $xy^{-1} = h \in H$. Par définition de la relation $\mathcal{R}_d$, cela veut dire que : $Hx = Hy$. D'où, $xH = Hx$ ou bien $xHx^{-1} = H$. La réciproque est relativement facile. Ainsi, on définit :

1.2.17 Définition

Soit G un groupe. Un sous groupe H de G est appelé un sous groupe normal de G si l'une des propositions précédentes est vérifiée.

1.2.18 Théorème

Soient G un groupe et$H$ un sous groupe normal de G. Alors, l'opération binaire sur G induit une relation binaire $\star$ sur l'ensemble quotient G/H définie pour tout x et y dans G par : $(xH)\star(yH) := xyH$. De plus, $(G/H, \star)$ définit une structure de groupe. En particulier, la surjection $G \to G/H$ est un homomorphisme surjective de groupes dont le noyau est H.

1.2.19 Remarque

Il est important de noter que tout sous groupe d'un groupe abélien est normal.

1.2.20 Théorème (Premier théorème d'isomorphisme)

Soit $f : (G_1, \star_1) \to (G_2, \star_2)$ un homomorphisme de groupes. On a :

$$G_1/Ker(f) \simeq Im(f)$$

. *Démonstration:* On montre que l'application f définie par :

$$\begin{array}{rcl} f : G_1/Ker(f) & \to & Im(f) \\ xKer(f) & \mapsto & f(x) \end{array}$$

définit un isomorphisme de groupes.

1.2.21 Exemples

1. Par l'homomorphisme surjective $GL_n(\mathbb{R}) \to \mathbb{R}\backslash\{0\}, A \mapsto det(A)$, on en déduit $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}\backslash\{0\}$;

2. Considérons l'homomorphisme de groupes $f : (R, +) \to (\mathbb{C}\backslash\{0\}, \times), \theta \mapsto e^{2i\pi\theta}$. On montre qu'on a : $Im(f) = S_1 := \{z \in \mathbb{C} : |z| = 1\}$ et $Ker(f) = \mathbb{Z}$. Ainsi, on a :

   $$(\mathbb{R}/\mathbb{Z}, +) \simeq (S_1, \times)$$

   où S_1 est le cercle de rayon 1 dans $\mathbb{R}^2$.

1.2.22 Théorème (Troisième théorème d'isomorphisme)

Soient $(G, \star)$ un groupe, H et N deux sous groupes normaux de G tels que $H \subset N$. Alors, H est un sous groupe normal de N. De plus, le groupe N/H est un sous groupe normal de G/H et on a :

$$(G/H)/(N/H) \simeq G/N.$$

Démonstration:
On montre que l'application f définie par :

$$\begin{array}{rcl} f : G/H & \to & G/N \\ xH & \mapsto & xN \end{array}$$

est un homomorphisme surjective de groupes. N'oubliez pas de démontrer que l'application est bien définie d'abord. Ainsi, on a : $Im(f) = G/N$ et $Ker(f) = \{xH : xN = N\} = \{xH : x \in N\} = N/H$. D'après le premier théorème d'isomorphisme, on a le résultat.

1.2.23 Exemples

Soit n un entier naturel non nul. Considérons le groupe $G = (Z, +)$. Soit d un diviseur positif de n. Ainsi, $n\mathbb{Z}$ et $d\mathbb{Z}$ sont de sous groupes normaux de G tels que $n\mathbb{Z} \subset d\mathbb{Z}$. D'où, d'après le troisième théorème d'isomorphisme, on en déduit :

$$(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/d\mathbb{Z}.$$

Le théorème suivant classifie les groupes cycliques à isomorphismes près :

1.2.24 Théorème

Soit G un groupe cyclique. On a $G \simeq \mathbb{Z}$ ou $G \simeq \mathbb{Z}/n\mathbb{Z}$ où n est un entier naturel.
Démonstration: Soit g un élément de G tel que $G =< g >$. Considérons l'homomorphisme de groupe f définie par :

$$\begin{array}{rcl} f : Z & \to & G \\ k & \mapsto & g^k \end{array}.$$

L'homomorphisme f est par définition surjective. Donc, d'après le premier théorème d'isomorphisme, on a $\mathbb{Z}/Ker\, f \simeq G$. Or, on sait que les sous groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ où n est entier naturel. D'où le résultat.

1.3 Exemples de Groupes

1.3.1 Le groupe de permutations S_n

Dans toute la suite, considérons le groupe de permutations Sn comme étant le groupe des applications bijectives de l'ensemble $\{1, 2, 3, \cdots, n\}$ dans lui même. Il est clair que l'ordre du groupe S_n est $n!$. Et bien évidemment, la loi binaire sur Sn est la loi de composition d'applications. S'il n'y a pas de confusion, on notera les deux compositions possibles de deux éléments σ et τ de S_n par $\sigma\tau$ et $\tau\sigma$. Dans la littérature, ils existent deux notations pour les éléments de S_n : La notation en matrices et la notation en cycles.
La notation en matrices : Soit $\sigma \in S_n$ défini pour tout $i \in \{1, 2, 3, \cdots, n\}$ par $\sigma(i) = a_i \in \{1, 2, 3, \cdots, n\}$. Ainsi, l'élément σ sera noté par : $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$.
La notation en cycles : Un élément σ de S_n est appelé un k-cycle s'il existe k éléments $a_1, a_2, \cdots, a_k$ de $\{1, 2, 3, \cdots, n\}$ tels que :

- $\sigma(i) = isi \notin \{a_1, a_2, \cdots, a_k\}$;
- $\sigma(a_i) = a_{i+1} si 1 \leq i \leq k-1$;
- $\sigma(a_k) = a_1$.

Dans ce cas, on notera σ par :

$$(a_1\ a_2\ \cdots\ a_k)$$

. Deux cycles $(a_1\ a_2\ \cdots\ a_k)$ et $(b_1\ b_2\ \cdots\ b_l)$ sont dits disjoints si $\{a_1, a_2, \cdots, a_k\} \cap \{b_1, b_2, \cdots, a_l\} = \emptyset$.

1.3.2 Proposition

Soient σ et τ deux cycles disjoints. On a : $\sigma\tau = \tau\sigma$.

1.3.3 Définition

Un 2-cycle est appelé une transposition.

1.3.4 Proposition

Soit $\sigma = (a_1\ a_2\ \cdots\ a_k)$ un cycle de Sn où $k \geq 2$. Alors, σ peut être une composition des transpositions. Plus précisément, on a :

$$(a_1\ a_2\ \cdots\ a_k) = (a_1 a_2)(a_2 a_3) \cdots (a_{k-1} a_k)$$

. *Démonstration:*
On montre qu'on a : $(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_2)(a_2\ a_3\ \cdots\ a_k)$. Puis, on raisonne par récurrence.

1.3.5 Remarque

Noter bien que la décomposition d'un cycle en produit de transpositions n'est pas unique. Par exemple, dans S_3 , on a :

$$(1\ 2)(2\ 3)(3\ 1) = (2\ 3)$$

.

1.3.6 Proposition

Toute permutation de S_n est un produit (ou une composition) de cycles deux à deux disjoints. Par conséquent, elle est aussi un produit de transpositions.

1.3.7 Remarque

Bien qu'une permutation soit un produit de transpositions, noter bien que ces transpositions qui la décomposent ne sont pas deux à deux disjoints. Sinon, toute permutation serait d'ordre 1 ou 2 qui n'est pas vrai si $n \geq 3$. Mais, en général, ce qui est sur est le suivant :

1.3.8 Théorème

Le nombre de transpositions qui décomposent une permutation donnée : soit il est pair, soit il est impair.

1.3.9 Définition

Une permutation de S_n est dite pair si elle est décomposée par un nombre pair de transpositions. Dans le cas contraire, on dit qu'elle est impaire. On peut déterminer facilement la parité d'une permutation comme l'indique la remarque suivante :

1.3.10 Remarque

D'après la Proposition 1.3.4, un k-cycle est une composition de $k-1$ transposition. Donc, si une permutation donnée est une composition de t cycles de longueur $k_1, k_2, \cdots, k_t$ respectivement, sa parité est la même que celle du nombre $k_1 + k_2 + \cdots + k_t + t$. L'application

$$\begin{array}{rcl} \varepsilon : S_n & \mapsto & (\{-1,1\}, \times) \\ \sigma & \mapsto & \begin{cases} 1 & si\ \sigma \text{ est paire} \\ -1 & sinon \end{cases} \end{array}$$

est un homomorphisme surjective de groupes. Ainsi, d'après le premier théorème d'isomorphisme, on a $S_n/Ker\varepsilon = \{1, -1\}$. Par conséquent, l'ensemble de permutations paires forment un sous groupe normal d'indice 2 dans S_n. On notera cet sous-groupe par A_n et sera appelé le groupe alterné de degré n. De plus, d'après la Proposition 1.3.4., un k-cycle est dans A_n si et seulement si k est impair. On termine cet exemple avec un théorème important qui justifie l'importance de S_n dans la théorie des groupes :

1.3.11 Théorème (Théorème de Cayley)

Soit $(G, \star)$ un groupe fini d'ordre n. Alors, G est isomorphe à un sous-groupe de S_n.
Démonstration:
Soit $g \in G$. Considérons l'application $f_g : G \to G, x \mapsto g \star x$. Pour tout $g \in G$, l'application

f_g est clairement bijective. Autrement dit, f_g est un élément de $P(G)$, le groupe des applications bijectives de G dans G. Maintenant considérons le sous-ensemble H de $P(E)$ défini par :

$$H := \{\sigma \in P(E) : \exists g \in G \text{ tel que } \sigma = f_g\}.$$

Le sous-ensemble H est un sous groupe de $P(E)$. En effet :

- Si on désigne par e l'identité de G, l'application f e est clairement l'identité de $P(E)$. Donc, $Id_G \in H$;
- Soient f_{g_1} et f_{g_2} deux éléments de H. Pour tout $x \in G$, on a :

$$(f_{g_1} \circ f_{g_2})(x) = f_{g_1}(f_{g_2}(x)) = f_{g_1}(g_2 \star x) = (g_1 \star g_2) \star x = f_{g_1 g_2}(x).$$

  Donc, la composition des applications est stable dans H.
- Soit $g \in G$. On a $f_g^{-1} = f_g^{-1}$. Ce qui veut dire que $f_g^{-1} \in H$.

Finalement, considérons l'application $f : G \to H,\ g \mapsto f_g$. Clairement, cette application est bijective. De plus, on a : $f(g_1 \star g_2) = f_{g1g_2} = f_{g_1} \circ f_{g2}$. Donc, f est un isomorphisme de groupes. Autrement dit, $G \simeq H$. Or, H est un sous-groupe de $P(E)$ qui est isomorphe à S_n . D'où le résultat.

1.3.12 Le groupe diédral D_n

Dans cette sous-section, dans le plan euclidien, on désignera par R_n un polygone régulier de n côtés. Notons son centre par C. On sait qu'ils existent exactement 2n symétries qui laissent le polygone R_n invariant, à savoir :

- Les n rotations de centre C respectivement d'angle $2k\pi$ n où $k = 1, 2, 3, \cdots, n$;
- Les n réflexions axiales déterminées respectivement par les n axes de symétries de R_n.

1.3.13 Proposition

Les 2n symétries de R_n définies ci-dessus forment un groupe d'ordre 2n avec la loi de composition de transformations sur le plan euclidien. On notera cet groupe par D_n et sera appelé le groupe diédral d'ordre 2n. De plus, si r et τ sont respectivement la rotation d'angle $\frac{2\pi}{n}$ et une symétrie axiale, on a :

$$D_n = \{r^k : k = 1, 2, \cdots, n\} \cup \{r^k\tau : k = 1, 2, \cdots, n\}$$

et $(r^k\tau) \circ (r^l\tau) = r^{k-l}$.

1.3.14 Remarque

Le théorème de Cayley nous garantit que D_n est isomorphe à un sous-groupe de S_{2n}. Par contre, naturellement, un élément de Dn permute les n sommets du polygone R_n . Ainsi, tout élément de Dn peut être considérer comme une permutation de l'ensemble de n sommets de R_n. Ainsi, Dn est un sous-groupe de S_n.

1.3.15 Le groupe linéaire $GL_n(\mathbb{R})$

Rappelons que $GL_n(\mathbb{R})$ désigne le groupe des matrices inversibles d'ordre n à coefficients dans $\mathbb{R}$. Le groupe est un groupe non abélien infini. L'application

$$\begin{array}{rccc} det : GL_n(\mathbb{R}) & \rightarrow & \mathbb{R}^\star \\ A & \mapsto & detA \end{array}$$

est un homomorphisme surjective. Son noyau est l'ensemble des matrices inversibles noté par $SL_n(\mathbb{R})$ dont le déterminant est 1. En utilisant cet homomorphisme, on montre qu'on a

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^\star.$$

Ainsi, comprendre le groupe $GL_n(\mathbb{R})$ revient à comprendre son sous-groupe normal $SL_n(\mathbb{R})$.

1.3.16 Proposition

Le groupe de permutations S_n est isomorphe à un sous-groupe de $SL_n(\mathbb{R})$.
Démonstration:
On montre que S_n est isomorphe au groupe de matrices de permutations P_n. Puisque pour tout $P \in P_n,\ detP = 1$, le groupe de matrices de permutations est un sous-groupe de $SL_n(\mathbb{R})$. Notons par $GL_n(\mathbb{Z})$ l'ensemble des matrices inversibles d'ordre n à coefficient dans $\mathbb{Z}$. Alors :

1.3.17 Proposition

$GL_n(\mathbb{Z})$ est un groupe des matrices dont le déterminant est $+1$ ou -1. Le noyau de la restriction de l'homomorphisme det sera noté par $SL_n(\mathbb{Z})$.

Démonstration: On montre que le sous-ensemble $GL_n(\mathbb{Z})$ est un sous-groupe de $Gl_n(\mathbb{R})$. Le plus dur est de montrer que si une matrice carrée à coefficients dans $\mathbb{Z}$ est inversible, son inverse est aussi à coefficients dans $\mathbb{Z}$. Mais, c'est faisable. Soit $A \in GL_n(\mathbb{Z})$. Donc, par définition, la matrice inverse A^{-1} est à coefficients dans $\mathbb{Z}$. Ainsi, $detA$ et $detA^{-1}$ sont des entiers. Or, $AA^{-1} = I_n$. Donc, $detA^{-1} = detA$ Comme $detA$ et $detA^{-1}$ sont des entiers, ceci n'est possible que si $detA = 1$ ou $detA = -1$.

Soit E un espace vectoriel sur $\mathbb{R}$. Rappelons qu'une application f de E vers un $\mathbb{R}$- espace vectoriel F est une application linéaire si pour tout (x, y) dans E^2 et (λ, μ) dans $\mathbb{R}^2$, on a :

$$f(\lambda x + \mu y) = \lambda f(x) + \mu f(y).$$

En particulier, f est un homomorphisme de groupes puisque $(E, +)$ et $(F, +)$ sont des groupes abéliens. Dans le cas où $F = E$, on dit que f est un endomorphisme. Si de plus, E est de dimension n, en utilisant l'identification des éléments de E via l'isomorphisme $E \simeq \mathbb{R}^n$, il existe une matrice A d'ordre n telle que pour tout $x \in E$, on a :

$$f(x) = Ax.$$

Si $(b_1, b_2, \cdots, b_n)$ désigne une base de E, la matrice de f est complètement déterminé de manière unique dans cette base, et l'on a :

$$A = (f(b_1)\ f(b_2)\ \cdots\ f(b_n))$$

où $f(b_i)$ est le vecteur de la i-ième colonne de A. Désignons respectivement par $Kerf$ et Imf le noyau et l'image de l'endomorphisme f . On a les propriétés suivants :

- $Kerf$ et Imf sont des sous-espaces vectoriels de E;

- $Kerf = N(A)$ et $Imf = C(A)$.

Ainsi, si on désigne par $L(E)$ l'ensemble des endomorphismes de E, on a l'isomorphisme suivante :

$$(L(E), +) \simeq (Mn(R), +).$$

De plus, si on note par $GL(E)$ l'ensemble des endomorphismes bijectives de E, on a :

$$(GL(E), \circ) \simeq (GL_n(R), \times).$$

Maintenant considérons le cas où l'on a n $= 2$. Désignons par $O_2(\mathbb{R})$ le sous-ensemble de $GL_2(\mathbb{R})$ défini par :

$$O_2(\mathbb{R}) := \{A \in GL_n(\mathbb{R}) : A^T A = AA^T = I_2\}.$$

C'est l'ensemble des matrices orthogonaux d'ordre 2. On a :

1.3.18 Proposition

$O_2(\mathbb{R})$ est un sous-groupe de $GL_2(\mathbb{R})$. De plus, pour tout $A \in O_2(\mathbb{R})$, on a $detA = 1$ ou $detA = -1$ et soit A est une matrice de rotation, soit elle est une matrice de réflexion. Plus précisément,

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ -sin\theta & \cos\theta \end{pmatrix} \text{ ou } A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

pour un certain angle θ. Le groupe des rotations sera noté par $SO_2(\mathbb{R})$.

1.3.19 Corollaire

Le groupe diédral D_n est isomorphe à un sous-groupe de $O_2(\mathbb{R})$. Pour finir, énonçons le résultat important suivant :

1.3.20 Théorème

Le groupe $SL_2(\mathbb{Z})$ est engendré par :

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}; \; T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$