NOTES DE COURS SUR LES GROUPES

HERVÉ LANNEAU

Résumé.

Ceci sont des notes sur le cours de D04 : Groupe et action de groupe.

Niveau L3 Université de Rennes1

L'auteur a volontairement laissé dans l'ombre certaines démonstrations, notamment en ce qui concerne les premiers chapitres. Il laisse au lecteur le soin de les retrouver, certaines indications sont cependant données en ce qui concerne les propositions plus difficiles. Bien entendu les démonstrations difficiles sont exposées et au fur et à mesure des chapitres.

Je pense que le lecteur doit pouvoir faire les démonstrations non données et en dernier recours il peut se référer à son cours manuscrit.

Les chapitres 9 et 12 sont hors programme en D04 pour l'année 2008

Table des matières

Date: 21 janvier 2009.

1. Relations d'équivalence et construction d'ensembles quotients

Introduction :
Soit E un ensemble et $(E_i)_{i\in I}$ une partition de E donc $E = \bigcup_{i\in I} E_i$ et $E_i \cap E_j = \emptyset$ si $i \neq j$.

A une telle partition on peut associer une relation binaire $\Re$ définie par :

$$x\Re y \Rightarrow x\text{et } y \text{ sont dans le même sous-ensemble } E_i.$$

Une telle relation satisfait aux propriétés suivantes :

(1) réflexive : $\forall x \in X\ x\Re x$
(2) symétrique : $\forall x, y \in X\ x\Re y \Rightarrow y\Re x$
(3) transitive $\forall x, y, z \in X\ (x\Re y \text{ et } y\Re z) \Rightarrow x\Re z$

Nous dirons qu'il s'agit d'une relation d'équivalence sur E. Pour tout x de E il existe un unique i tel que $x \in E_i$. Ce sous-ensemble sera appellé classe d'équivalence de x. Donc tout y se trouvant dans le même sous-ensemble que x aura la même classe d'équivalence. Cet ensemble est noté par $\bar{x}$ et donc formellement nous avons la propriété que $y \in \bar{x} \Leftrightarrow \bar{y} = \bar{x}$.

Réciproquement

Définition 1.0.1. Une relation d'équivalence $\Re$ sur un ensemble X est une relation binaire telle que $\Re$satisfasse aux trois propriétés ci-dessus.

Définition 1.0.2 (Classes d'équivalence)**.** Soit X un ensemble et $\Re$ une relation d'équivalence sur X. Pour $x \in X$ on appelle classe d'équivalence de x l'ensemble $\bar{x} = \{y \in X / y\Re x\}$.

On peut montrer que $y \in \bar{x} \iff \bar{x} = \bar{y}$.

L'ensemble de toutes ces classes forme une partition de X ; Il est noté $\dfrac{X}{\Re}$, et est appelé ensemble quotient de X par $\Re$.

L'application $p : X \to \dfrac{X}{\Re}$ définie par $p(x) = \bar{x}$ est dite projection canonique. Cette application est surjective. Au fait quand est-elle injective ?

Remarquons que $\dfrac{X}{\Re}$ est contenu dans $\mathcal{P}(X)$ et non pas dans X comme affirmé parfois sur certaines copies.

Exemples :
1) Soit $E = \mathbb{Z}$ partitionné par les n sous-ensembles $E_i (0 \leq i < n)$ avec E_i l'ensemble de tous les entiers ayant i comme reste dans la division par n. Cette partition donne naissance à la relation d'équivalence $x\Re y \Leftrightarrow x - y$ est multiple de n. Relation connu sous le nom de congruence.

L'ensemble quotient sera noté par $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. C'est un ensemble de n éléments constitué des classes des entiers 0,1,...,n-1. On pourra remarquer que $\bar{k} = \overline{n-k}$ et en particulier que $\bar{0} = \bar{n}$. (Il sera étudié en détail au chapitre 3 en tant de groupe)

2) La construction des Rationnels :
Sur $\mathbb{Z} \times \mathbb{Z}^*$ on considére la relation d'équivalence $\Re$ définie par
$(a, b)\Re(c, d)$ si et seulement si $ad = bc$. L'ensemble quotient est ce que l'on connait depuis longtemps à savoir $\mathbb{Q}$.
Ceci est en fait la définition des rationnels que l'on demande au CAPES.

Proposition 1.0.1 (théorème de factorisation)**.**

Soit $\Re$ une relation d'équivalence sur X et $p : X \to \dfrac{X}{\Re}$ la projection canonique. Pour toute application $f : X \to Y$ telle que $x\Re y \Rightarrow f(x)=f(y)$ il existe une application unique $\overline{f} : X/\Re \to Y$ telle que $f = \overline{f} \circ p$.

Indication : Il suffit de poser $\bar{f}(\bar{x}) = f(x)$. Il reste à montrer que $\bar{f}$ est une application donc que la définition de $\bar{f}$ ne dépend pas du représentant choisi.

2. Notion de groupe, sous-groupe, morphisme

2.1. **Groupe.**

Définition 2.1.1. Un groupe est un couple $(G, *)$ où G est un ensemble non vide et $*$ une loi de composition interne sur G qui vérifie les trois propriétés suivantes :

(P1) La loi $*$ est associative.

$$\forall g, g^{'}, g^{''} \in G \ (g * g^{'}) * g^{''} = g * (g^{'} * g^{''})$$

(P2) La loi $*$ posséde un élément neutre notée e

$$\exists e \in G \text{ tel que } \forall g \in G \ g * e = e * g = g$$

(P3) Tout élément de G posséde un symétrique .

$$\forall g \in G \ \exists g^{'} \text{ tel que } g * g^{'} = e = g^{'} * g$$

On dira que G est commutatif ou encore abélien si pour tout g et $g^{'}$ de G $g * g^{'} = g^{'} * g$.

Dans le cas où G est fini de cardinalité n on dira que G est d'ordre n. Donc l'ordre d'un groupe, à ne pas confondre avec l'ordre d'un élément, notion que nous verrons plus tard, n'est rien d'autre que son nombre déléments.

Proposition 2.1.1. *Un groupe G a un unique* élément neutre.
Tout élément de G posséde un *unique* symétrique .

Notation 2.1.1. La loi de composition interne d'un groupe G sera couramment notée

$$\text{« multiplicativement» } g * g^{'} = gg^{'}$$

soit

$$\text{« additivement» } g * g^{'} = g + g^{'}$$

Dans le premier cas l'inverse de g sera notée par g^{-1} et dans le second cas par $-g$.

Sauf mention du contraire , dans la suite on choisira la notation multiplicative.

Si n est un entier positif, on note par g^n le composé de g avec lui même n fois. On remarquera que $g^{n+m} = g^n g^m$.

En particulier si G est commutatif, pour tout g_1 et g_2 de G $(g_1 g_2)^n = g_1^n g_2^n$. Remarquons que cette relation est fausse si G n'est pas commutatif.

L'inverse de g^n sera noté par g^{-n}.

Proposition 2.1.2 (Régles de calcul dans un groupe et Règle de simplification)**.**

Pour tout x,y,z de G on a $xy = xz \Longleftrightarrow y = z$ et $xz = yz \Longleftrightarrow x = y$.
Inverse d'un composé :
Pour tout x, y de G on a $(xy)^{-1} = y^{-1}x^{-1}$.

Exemple 2.1.1. Quelques exemple de groupes :

$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{C}+)$ sont des groupes abéliens.

Si n est un entier positif alors $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$ est un groupe abélien. Bien entendu ceci devient faux si on remplace la loi $+$ par la loi de multiplication. Ce groupe sera étudié en détail au chapitre suivant.

Si E est un ensemble, l'ensemble des bijections de E sur lui-même, noté S_E est un groupe pour la loi de composition des applications. Lorsque E est un ensemble fini de cardinalité n, ce groupe est appelé groupe symétrique de E et noté S_n. Son ordre est $n!$ et sera étudié en détail au chapitre 5.

Si n est un entier positif $GL(n,\mathbb{K})$,ensemble des matrices inversibles $n \times n$ si $\mathbb{K}$ est un corps, est un groupe pour la multiplication des matrices.

Si E est un ensemble muni d'une loi de composition interne, associative et possédant un élément neutre alors l'ensemble des éléments inversibles est un groupe. Cet ensemble sera noté $E^{\times}$. Par exemple si k est un corps $k - \{0\}$ est un groupe abélien.

Par exemple $(\frac{\mathbb{Z}}{n\mathbb{Z}})^{\times}$ est un groupe dont les éléments sont les $\bar{m}$ telle que m et n soient premiers entre eux. (En effet il suffit d'appliquer Bezout).

Un autre exemple de groupes est donné par le produit direct de groupes :

Soit G et H deux groupes notés multiplicativement. Le produit cartésien $G \times H$ est muni d'une structure de groupe par $(g,h)(g^{'},h^{'}) = (gg^{'},hh^{'})$.

2.2. **Sous-groupes.**

Définition 2.2.1. Soit G un groupe. Un sous-groupe de G est un sous-ensemble H non vide de G vérifiant :

H est stable pour la multiplication

La loi induite par celle de G sur H fait de H un groupe.

Proposition 2.2.1. *Soit H un sous-ensemble du groupe G. Pour vérifier que H est un sous-groupe de G il suffit de montrer que*

Si $x, y \in H$ alors $xy \in H$ et $x^{-1} \in H$. Ces deux conditions pouvant être condensées en la condition : Si $x, y \in H$ alors $xy^{-1} \in H$.

Remarquons que si H est un sous-groupe de G alors e (e élément neutre de G) appartient à H.

Exemple 2.2.1. Quelques exemples de sous-groupes

1) Si G est un groupe $Z(G) = \{g \in G / gg^{'} = g^{'}g \ \forall g^{'} \in G\}$ est un sous-groupe de G. On l'appelle le centre de G. Ce groupe jouera une importance primordiale par la suite.

2) $\mathbf{U}_n$ l'ensemble des racines n^{ieme} de l'unité de $\mathbb{C}^*$ est un sous-groupe de $(C^*, \times)$.

3) Un exemple géométrique :

Soit P le plan afffine Euclidien. On appele isométrie du plan toute application $f : P \longrightarrow P$ qui conserve les distances c'est à dire telle que $\forall x, y \in P, d(f(x), f(y)) = d(x, y)$.

Il est facile de montrer que toute isométrie est bijective. L'ensemble des isométries $Is(P)$ du plan est un sous-groupe de S_P. On étudiera entre autre les sous-groupes de $Is(P)$ formé des isométries conservant certaines figures planes (rectangle,carré, triangle isocéle,équilatéral ...) cf le chapitre 4

4) Les sous-groupes de $\mathbb{Z}$: Nous allons montrer que les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ $n \in \mathbb{N}$.

Preuve :

On vérifie que $n\mathbb{Z}$ est un sous-groupe.

Soit donc H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$ sinon H contient un entier m que l'on peut supposer positif car si $m < 0$ alors $-m$ appartient à H. Considérons $E = \{h > 0/h \in H\}$. E étant non vide posséde un plus petit élément n et tout h de H s'écrit $h = nq + r$ par la division Euclidienne et $0 \leq r < n$ donc $r = h - nq$ appartient à H et donc $r = 0$.

4) $O(n, \mathbb{R}) = \{A \in M_n(\mathbb{R})/A^t A = Id\}$ est un sous-groupe de $GL(n, \mathbb{R})$. Ce groupe, dit groupe orthogonal, a une importance toute particuliére dans le cadre de la géométrie notamment pour n = 2 ou 3 pour létude des isométries.

Exercice 1. Montrer que $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ si $d = pgcd(m, n)$

Proposition 2.2.2. *Soit $\{H_i\}$ une famille de sous-groupes de G. Alors $\bigcap H_i$ est un sous-groupe de G. Ce résultat devient faux pour $\bigcup H_i$.*

Par exemple considérer les deux sous-groupes de $(\mathbb{Z}, +), 3\mathbb{Z}$ et $8\mathbb{Z}$. (3 + 8 n'appartient pas à $3\mathbb{Z} \cap 8\mathbb{Z}$).

Proposition 2.2.3. *Soit H et K deux sous-groupes du groupe G.*
On note par HK l'ensemble $\{hk \ / \ h \in H, k \in K\}$.
HK est un sous-groupe de G si et seuement si $HK = KH$

Preuve :
Si $HK = KH$ le lecteur vérifiera que HK est un sous-groupe.
Examinons la réciproque. Supposons donc que HK soit un sous-groupe .
Montrons d'abord que $KH \subset HK$. Si $h \in H$ et $k \in K$ alors $kh = (h^{-1}k^{-1})^{-1}$ et HK étant un sous-groupe $h^{-1}k^{-1} \in HK$ et son inverse aussi.
Montrons que $HK \subset KH$. Soit $x \in HK$ donc $x^{-1} \in HK$ et par suite $x^{-1} = hk$ donc $x = (hk)^{-1} = k^{-1}h^{-1}$ appartient à KH.

2.3. **Homomorphisme de groupes.**

Soit G et $G^{'}$ deux groupes.

Définition 2.3.1. Un homomorphisme de G dans $G^{'}$ est une application $f : G \to G^{'}$ telle que $f(gg^{'}) = f(g)f(g^{'})$ pour tout g et $g^{'}$ de G.

Terminologie :
Si f est un homomorphisme bijectif de G dans $G^{'}$ on dira que f est un **isomorphisme** .
Si f est un isomorphisme de G dans G on dira que f est un **automorphisme** et l'ensemble des automorphismes de G sera noté par $Aut(G)$.
Par la suite nous dirons morphisme pour homomorphisme.

Proposition 2.3.1. *$Aut(G)$ est un groupe pour la loi de composition des applications.*

Exercice 2. Montrer que $Int(G) = \{f_g : G \to G/g \in G\}$ où f_g est définie par $f_g(h) = ghg^{-1}$ est un sous-groupe de $Aut(G)$.
Cet ensemble est appelé ensemble des automorphismes intérieurs de G.

Proposition 2.3.2. *Si f est un homomorphisme de G dans $G^{'}$ alors :*

a) Pour tout n de $\mathbb{Z}$ et tout g de G $f(g)^n = f(g^n)$, donc en particulier, pour tout g de G $f(g)^{-1} = f(g^{-1})$.
b) L'image de l'élément neutre de G est l'élément neutre de $G^{'}$.
c) L'image d'un sous-groupe est un sous-groupe.
d) L'image réciproque d'un sous-groupe est un sous-groupe.

Définition 2.3.2. Si f est un homomorphisme de G dans $G^{'}$, on appelle
noyau de f et on note Ker(f) l'ensemble $\{g \in G/f(g) = e_{G'}\}$.
image de f et on note Im(f) l'ensemble $\{f(g)/g \in G\}$.

Proposition 2.3.3. *Si f est un homomorphisme de G dans G' Ker(f) est un sous-groupe de G et Im(f) est un sous-groupe de G'.*

Proposition 2.3.4. *f est injective si et seulement si Ker(f) = e_G.*
f est surjective si et seulement si Im(f) = G'.

Remarquons que si G et G' sont des groupes finis de même ordre alors si f $G \to G'$ est un homorphisme on a les équivalences suivantes :
f est un isomorphisme $\iff$ f est injective $\iff$ f est surjective.

2.4. **Table d'un groupe fini.** Soit G un groupe fini ; $G = \{g_i / 1 \leq i \leq n\}$. On peut faire la table de G en formant un tableau de n lignes et n colonnes et en marquant à la i^{me} ligne et j^{me} colonne le composé $g_i g_j$. On remarquera que dans une même ligne ou colonne on doit retrouver les n éléments du groupe. Par exemple pour un groupe à 3 éléments on ne trouvera qu'une seule table possible mais pour montrer que cette table est bien celle d'un groupe il faudrait vérifier l'associativité. En fait, il suffit de montrer que c'est la table de $(\frac{\mathbb{Z}}{3\mathbb{Z}}, +)$ (cf le chapitre suivant) et donc de conclure que à isomorphisme prés il n'existe qu'un seul groupe à 3 éléments.

Bien sur cette méthode ne suffira pas pour des groupes d'ordre plus élevés. Il nous faut donc des outils qui seront développés par la suite.

Avant d'entamer le chapitre sur les groupes quotients, on va examiner de plus près un groupe connu. C'est le premier exemple de groupe quotient que les étudiants rencontrent en L2 sans connaitre la notion théorique de groupe quotient qui fait l'objet du chapitre 4. Nous étudierons auparavant la notion d'ensemble quotient et notamment nous introduirons l'ensemble $\frac{\mathbb{Z}}{n\mathbb{Z}}$. On le munira par la suite d'une structure de groupe induite par celle du groupe $(\mathbb{Z}, +)$.

3. Les groupes $(\frac{\mathbb{Z}}{n\mathbb{Z}},+)$ et $((\frac{\mathbb{Z}}{n\mathbb{Z}})^\times,\times)$

Dans toute la suite n est un entier positif

3.1. Congruences dans $\mathbb{Z}$.

Sur $\mathbb{Z}^2$ on considère la relation $a\mathcal{R}b \Longleftrightarrow a-b$ est multiple de n.

Cette relation est une relation déquivalence sur $\mathbb{Z}$. On a donc un ensemble quotient $\frac{\mathbb{Z}}{\mathcal{R}}$, ensemble que l'on notera $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

NOTATION : La relation $a\mathcal{R}b$ est encore notée $a \equiv b \pmod n$ et on dira a congru à b modulo n.

Par exemple $10 \equiv 0 \pmod 2$, $3 \equiv 1 \pmod 2$ mais aussi $3 \equiv -1 \pmod 2$

Remarquons que $a \equiv b \pmod n$ est équivalent à dire que a et b ont mêmes restes dans la division par n.

Revenons aux classes d'équivalences : $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est l'ensemble des classes d'équivalence et la classe de a notée $\bar{a}$ sera donc formé des entiers b ayant le même reste que a dans la division par n. Donc si r est le reste de la division de a par n alors $\bar{a} = a + n\mathbb{Z} = \bar{r}$.

D'autre part, le théorème de la division Euclidienne nous dit que le reste de la division de a par n est un entier r tel que $0 \leq r < n$ donc $\frac{\mathbb{Z}}{n\mathbb{Z}}$ a exactement $n-1$ éléments et on peut décrire $\frac{\mathbb{Z}}{n\mathbb{Z}}$ par $\{\bar{0},\bar{1},...,\overline{n-1}\}$. On peut aussi décrire $\frac{\mathbb{Z}}{n\mathbb{Z}}$ par $\{\bar{0},\overline{-1},...,\overline{1-n}\}$ car $\overline{-1} = \overline{n-1}$, $\overline{-2} = \overline{n-2}$, etc

Propriété 1 :

Soit a, b, a', b' quatre éléments de $\mathbb{Z}^4$. Si $a \equiv a'$ (mod n) et $b \equiv b'$ (mod n) alors $a+b \equiv a'+b'$ (mod n).

3.2. Le groupe $(\frac{\mathbb{Z}}{n\mathbb{Z}},+)$.

la propriété 1 permet donc de définir sur $\frac{\mathbb{Z}}{n\mathbb{Z}}$ une loi interne, notée $+$, à savoir $\bar{a}+\overline{a'} = \overline{a+a'}$.

Examinons pourquoi : En fait il faut vérifier que $f : \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{n\mathbb{Z}}$ définie par $f(\bar{x},\bar{y}) = \overline{x+y}$ est une application, ce qui découle de la propriété. On dira que la relation $\equiv$ est compatible avec la loi de groupe de $\mathbb{Z}$. Remarquons que la commutativité de $\mathbb{Z}$ intervient.

Cette loi est une loi de groupe sur $\frac{\mathbb{Z}}{n\mathbb{Z}}$. L'élément neutre est $\bar{0}$ et l'inverse de $\bar{a}$ est $\overline{-a}$.

Par exemple dans $\frac{\mathbb{Z}}{6\mathbb{Z}}$ on a $\bar{2}+\bar{5} = \bar{7} = \bar{1}$ et $\overline{-2}+\overline{-5} = \overline{-7} = \overline{-1} = \bar{5}$ ce que l'on peut aussi calculer par $\overline{-2}+\overline{-5} = \bar{4}+\bar{1}$.

Comment trouver les morphismes de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ dans $\frac{\mathbb{Z}}{m\mathbb{Z}}$?

Soit $f : \frac{\mathbb{Z}}{n\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{m\mathbb{Z}}$ un morphisme. On remarque que la connaissance de $f(\bar{1}) = \bar{k}$ est suffisante car f étant un morphisme et tout $\bar{x}$ étant la somme de $\bar{1}$ x fois on posera $f(\bar{x}) = k\bar{x}$. Comme $f(\bar{0}) = \bar{0}$ on doit de plus avoir $f(\bar{n}) = n\bar{k} = \bar{0}$ soit $nk \equiv 0$(modulo m). Si ces conditions sont remplies alors les seuls morphismes possibles sont de cette forme car la condition $nk \equiv 0$(modulo m) nous assure que f est bien une application.

Prenons un exemple concret et cherchons les morphismes possibles de $\frac{\mathbb{Z}}{5\mathbb{Z}}$ dans $\frac{\mathbb{Z}}{10\mathbb{Z}}$.

On doit donc avoir $f(\bar{1}) = \bar{k}$ avec $5k$ multiple de 10, soit 5 choix possibles pour $\bar{k}$ à savoir $\bar{0}$, $\bar{2}$,$\bar{4}\bar{6}.\bar{8}$ On conclue donc que l'on a que 5 morphismes possibles.

Nous laissons au lecteur la réponse si n et m sont premiers entre eux.

Théorème 3.2.1. *Le théorème Chinois :*
Soit m et n deux entiers premiers entre eux. Alors

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}} \text{ est isomorphe à } \frac{\mathbb{Z}}{nm\mathbb{Z}}$$

.

Preuve :
Si k est un entier notons par $\bar{k}$ la classe de k dans $\frac{\mathbb{Z}}{nm\mathbb{Z}}$, par $\tilde{k}$ la classe de k dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ et par notons par $\hat{k}$ la classe de k dans $\frac{\mathbb{Z}}{m\mathbb{Z}}$.
Soit $f : \frac{\mathbb{Z}}{nm\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$ définie par $f(\bar{k}) = (\tilde{k}, \hat{k})$.

On vérifie que f est une application, et un morphisme. En utilisant le fait que m et n sont premiers entre eux, par le lemme de Gauss, $\mathrm{Ker}(f) = \bar{0}$ donc f est injective. Enfin comme les ensembles de départ et d'arrivée ont même nombre d'éléments f est un isomorphisme.

Les groupes d'ordre 3 à isomorphisme prés :
Soit G un groupe d'ordre 3 donc ensemblistement $G = \{e, a, b\}$, e désignant l'élément neutre. Si nous faisons la table du groupe (cf chapitre 1 p6) on a forçément $ab = e$. Donc $a^{-1} = b$. $a^2 \neq e$ sinon $a = a^{-1} = b$ et $a^2 \neq a$ donc $a^2 = b$. De même $b^2 = a$. Ceci permet de faire l'unique table possible et de s'aperçevoir que l'on a la table de $\frac{\mathbb{Z}}{3\mathbb{Z}}$. On a donc à isomorphisme prés un seul groupe à 3 éléments.

3.3. Le groupe $((\frac{\mathbb{Z}}{n\mathbb{Z}})^\times, \times)$.

Propriété 2 :

Soit a, b, a', b' quatre éléments de $\mathbb{Z}^4$. Si $a \equiv a'$ (mod n) et $b \equiv b'$ (mod n) alors $ab \equiv a'b'$ (mod n).

Cette propriété permet donc de définir sur $\frac{\mathbb{Z}}{n\mathbb{Z}}$ une loi interne, noté $\times$, à savoir $\overline{a} \times \overline{a'} = \overline{aa'}$.

Cette loi $\times$ est associative et $\frac{\mathbb{Z}}{n\mathbb{Z}} - \{\bar{0}\}$ posséde pour cette loi un élément neutre : $\bar{1}$. Par contre tout les éléments de $\frac{\mathbb{Z}}{n\mathbb{Z}} - \{\bar{0}\}$ ne sont pas forcement inversibles.

Par exemple dans $\frac{\mathbb{Z}}{6\mathbb{Z}} - \{\bar{0}\}$, $\bar{4}$ ne posséde pas d'inverse pour $\times$. En effet il n'existe pas de $\bar{x}$ tel que $\bar{4} \times \bar{x} = \bar{1}$. Par contre $\bar{5}$ est inversible pour $\times$ car $\bar{5} \times \bar{5} = \overline{25} = \bar{1}$.

On considére l'ensemble noté $(\frac{\mathbb{Z}}{n\mathbb{Z}})^\times$ qui est l'ensemble des éléments non nuls de $\frac{\mathbb{Z}}{n\mathbb{Z}}$, inversibles pour la loi $\times$. Cet ensemble est alors muni d'une structure de groupe pour $\times$.

Les éléments de $(\frac{\mathbb{Z}}{n\mathbb{Z}})^\times$ sont les $\bar{k}$ où k est premier avec n. (Ceci est une application directe de Bezout)

Un petit exemple de divination :
Le devin vous demande de multiplier votre jour de naissance par 12 et votre mois de naissance par 31puis de lui donner la somme de ces deux produits. Il vous donnera alors le jour et mois de votre naissance. Par exemple si vous êtes né le 2 avril vous lui donnerez le nombre 148. Au fait comment le devin va t'il retrouver la date du 2 avril ?

Exercice 3. Soit $f : \dfrac{\mathbb{Z}}{33\mathbb{Z}} \longrightarrow \dfrac{\mathbb{Z}}{33\mathbb{Z}}$ définie par $f(\bar{x}) = 17\bar{x} + \bar{9}$.

a) f est-il un morphisme ?

b) f est-elle bijective ? Si oui expliciter f^{-1}.

Exercice 4. Soit $f : \dfrac{\mathbb{Z}}{4\mathbb{Z}} \longrightarrow (\dfrac{\mathbb{Z}}{5\mathbb{Z}})^{\times}$ définie par $f(\bar{k}) = \bar{2}^k$.

1) montrer que f est bien définie et est un morphisme. (Attention aux lois)

2) Montrer que f est un isomorphisme.

3.4. **Une introduction aux groupes quotients.**

Nous connaisons le groupe $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. Tentons de prolonger cette notion à G, un groupe quelconque, et H un sous-groupe de G, c'est à dire remplacons $\mathbb{Z}$ par G et $n\mathbb{Z}$ par H.

Dans toute la suite la loi de G est supposé multiplicative.

Nous sommes amenés à définir une relation déquivalence sur G, en analogie à la relation $\equiv$, par $x\mathcal{R}y \Longleftrightarrow xy^{-1} \in H$. Ce qui est équivalent à $x \in Hy$.

On a donc un ensemble quotient $\dfrac{G}{H}$ que l'on va essayer de munir d'une structure de groupe. Toujours en analogie avec $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, posons $\bar{x}\bar{y} = \overline{xy}$.

On doit donc vérifier en premier lieu que l'on a une loi de composition et par suite que $f : \dfrac{G}{H} \longrightarrow \dfrac{G}{H}$ définie par $f(\bar{x}, \bar{y}) = \overline{xy}$ est une application. Donc $(\bar{x}, \bar{y}) = (\bar{x'}, \bar{y'}) \Longrightarrow \overline{xy} = \overline{x'y'}$ autrement dit que $Hx = Hx'$ et $Hy = Hy' \Longrightarrow Hx'Hy' = Hx'y'$. Cette égalité est vérifiée si G est commutatif mais par contre est fausse si G est quelconque.

Ceci améne donc une condition sur le sous-groupe H et à une nouvelle définition :

Si G est un groupe et H un sous-groupe, on dira que H est distingué si pour tout y de G $yH = Hy$.

A ce moment f est bien une application et $\dfrac{G}{H}$ devient un groupe pour cette loi.

Reste une question :

On a introduit une nouvelle notion mais se justifie t'elle c'est à dire existe t'il des groupes, non commutatifs, possédant des sous-groupes distingués non triviaux $(\neq \{e\}) et \neq G)$? La réponse est oui heureusement. Par exemple si G est un groupe et f un morphisme de G dans G' alors $\ker(f)$ est un sous-groupe distingué. Donc cette nouvelle notion se justifie. Le prochain chapitre introduit de facon théorique cette généralisation.

4. Groupe quotient

4.1. **Classes a droite et a gauche modulo un sous groupe.** Soit H un sous-groupe du groupe G. On considére les deux relations suivantes sur G

$x \sim_H y \iff xy^{-1} \in H$ et $x_H \sim y \iff y^{-1}x \in H$.

Proposition 4.1.1. *Ces deux relations sont des relations d'équivalence sur G*

La classe d'équivalence de x pour $x \sim_H y$ sera dite classe à droite modulo H et l'ensemble quotient sera noté $(G/H)_d$. La classe d'équivalence de x pour $x_H \sim y$ sera dite classe à gauche modulo H et l'ensemble quotient sera noté $(G/H)_g$.

Donc la classe à gauche de x modulo H sera l'ensemble $xH = \{xh/h \in H\}$.

Remarquons que si G est commutatif alors ces deux relations sont identiques.

Proposition 4.1.2. *Toute classe d'équivalence à droite (ou à gauche) a le même nombre d'éléments que H.*

Indication : l'application $f : H \to Hx$ définie par $f(h) = hx$ est bijective.

Théorème 4.1.3 (Théorème de Lagrange)**.** *Si G est un groupe fini et H un sous-groupe alors l'ordre de H divise l'ordre de G.*

Preuve :

Considérons l'ensemble des classes à gauche et notons par k le nombre de ces classes. Chaque classe à gauche posséde exactament $m = |H|$ éléments et comme les classes à gauche forment une partition de G on a donc $|G| = km$ d'où le résultat.

Remarquons que la démonstrattion aurait pu se faire en considérant les classes à droite ce qui justifie la partie 2) du corollaire suivant

Corollaire 4.1.4.

1) Tout groupe d'ordre premier ne posséde pas de sous-groupe propre (c'est à dire un sous-groupe $\neq G$ et $\neq \{e\}$.

2) Si G est fini le nombre de classe à droite est égale au nombre de classes à gauche.

En fait ce résultat est encore vrai si G est d'ordre infini car $f : (G/H)_d \to (G/H)_g$ définie par $f(Hx) = x^{-1}H$ est une application bijective.

Définition 4.1.1. Le nombre de classes à gauche (et donc le nombre de classes à droite) sera noté par $[G : H]$ et sera appellé indice de H dans G. Dans le cas fini on a donc $[G : H] = |G|/|H|$

4.2. **Groupe quotient.**

Soit G un groupe et $\sim$ une relation d'équivalence sur G. On se demande si on peut munir l'ensemble $G/\sim$ d'une structure de groupe telle que la projection canonique soit un morphisme, donc que la loi sur $G/\sim$ soit $\bar{x}\bar{y} = \overline{xy}$.

Ceci nous amène à la définition suivante (dans le but que la loi précédente soit bien définie).

Définition 4.2.1. Soit $\sim$ une relation d'équivalence sur un groupe G. On dit que $\sim$ est compatible avec la structure de groupe de G si pour tous x_1, x_2, y_1 et y_2 dans G tels que $x_1 \sim x_2$ et $y_1 \sim y_2$ on a $x_1y_1 \sim x_2y_2$.

Proposition 4.2.1. *Soit $\sim$ une relation d'équivalence sur un groupe G. Alors il existe sur $G/\sim$ une unique structure de groupe telle que la projection canonique soit un morphisme si et seulement si $\sim$ est compatible avec la multiplication de G.*

Proposition 4.2.2. *Soit G un groupe et H un sous-groupe. Si $x \sim_H y = x_H \sim y = \sim$ alors $\sim$ est compatible avec la loi de G.*

On notera par G/H le groupe quotient pour la relation $\sim$ (Remarquer que $\bar{e} = H$).

Ceci amène à la notion suivante :

4.3. **Sous-groupe distingué.**

Définition 4.3.1. Si H est un sous-groupe de G on dira que H est distingué (ou encore normal ou invariant) si pour tout x et y de G
$x \sim_H y = x_H \sim y$. On notera $H \lhd G$.

Proposition 4.3.1. *Si H est un sous-groupe de G alors $H \lhd G$ si et seulement si l'une des trois affirmations suivantes est vérifiée :*
1) $\forall g \in G\ gH = Hg$
2) $\forall g \in G\ gHg^{-1} = H$
3) $\forall g \in G\ gHg^{-1} \subset H$

Remarque : La propriété c) se traduit par " pour tout h de H il existe h' de H tel que $ghg^{-1} = h'$". h' n'est pas forcément h.

Exemple 4.3.1. Ker(f) si f est un morphisme de groupes est un sous-groupe distingué.
$Z(G)$ est un sous-groupe distingué de G.
$Int(G)$ est un sous-groupe distingué de $Aut(G)$.

Si donc $H \lhd G$ on pourra parler du groupe quotient $\dfrac{G}{H}$ qui est donc muni de la loi, si G est un groupe multiplicatif, $\bar{x}\bar{y} = \overline{xy}$. On a évidemment $(\bar{x})^{-1} = \overline{x^{-1}}$ et aussi $\bar{e} = H$.

Théorème 4.3.2. *Premier théorème d'isomorphisme*
Si $f : G \to G'$ est un morphisme de groupes alors $G/Ker(f)$ est isomorphe à $Im(f)$.

Indication : L'application h de $G/Ker(f)$ dans $Im(f)$ définie par $h(\bar{g}) = f(g)$ est un isomorphisme. (Ne pas oublier de vérifier que h est bien définie)

Proposition 4.3.3. *Propriété universelle du quotient*
Soit G un groupe et H un sous-groupe distingué de G. Alors pour tout G' et tout morphisme $f : G \to G'$ tel que $H \subset ker(f)$ il existe un unique morphisme $\bar{f} : G/H \to G'$ tel que $\bar{f} \circ p = f$ si p est la projection canonique de G sur G/H.

Proposition 4.3.4. *Sous les hypothéses précédentes on a*
a) f surjective $\Rightarrow \bar{f}$ surjective.
b) $H = Ker(f) \Rightarrow \bar{f}$ injective

5. Sous-groupe engendré

5.1. **systéme de générateur.** Sauf mention du contraire G est un groupe noté multiplicativement.

Définition 5.1.1. Soit S un sous-ensemble du groupe G. Le sous-groupe de G engendré par S est l'intersection de tous les sous-groupes de G contenant S. On le notera par $< S >$.

Proposition 5.1.1. *a) <S> est le plus petit sous-groupe de G contenant S.*

b) <S> est l'ensemble des produits finis d'éléments de S ou de leurs inverses.Un tel produit sera dit mot sur S.

Donc un mot sur S est du type $\prod_{i=1}^{i=n} s_i^{\epsilon_i}$ *où* $\epsilon_i \in \{-1, 0, 1\}$ *et* $s_i \in S$.

Indication pour b) L'ensemble des mots sur S forme un sous- groupe de G et conclure .

Exercice 5. Quel est le sous-groupe de $\mathbb{Z}$ engendré par $\mathbb{N}$ puis par $S = \{2, 3\}$ et le sous-groupe de $\mathbb{R}$ engendré par 1 ?

Exemple 5.1.1.

Le groupe D_4 : Soit S le sous-ensemble de $GL(2, \mathbb{R})$ formé des deux matrices

$$r = \begin{pmatrix} \cos(\Pi/2) & -\sin(\Pi/2) \\ \sin(\Pi/2) & \cos(\Pi/2) \end{pmatrix} \text{ et } s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

.

Géométriquement, dans le plan vectoriel muni d'une base orthonormale e_1, e_2, ces deux matrices représentent une rotation de centre l'origine et d'angle $\Pi/2$ et une symétrie par rapport à vect e_1.

On vérifie que $r^i \neq Id$ si $0 < i < 4$ et que $r^4 = Id$ ainsi que $s^2 = Id$ et enfin que $rs = sr^3$. On trouve donc pour $< S >$ un groupe à 8 éléments. Ce groupe est appelé groupe diédral et on verra plus tard qu'il s'agit du groupe des isométries du carré.

Exercice 6. Soit S le sous-ensemble de $GL(2, \mathbb{C})$ formé des deux matrices

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \text{ et } J = \begin{pmatrix} 0 & 1 \\ -1 & -0 \end{pmatrix}$$

écrites dans la base canonique. On verifie aisément que $I^4 = Id, I^2 = J^2, JI = I^3J$. Combien le sous-groupe de $GL(2, \mathbb{C})$ engendré par S a t-il déléments ? Ce groupe est appelé groupe des quaternions.

5.2. **Remarques utiles.**

Soit G un groupe engendré par $\{g_1, \ldots, g_k\}$.

On désire montrer que H sous-groupe de G est distingué dans G. Il suffit de montrer que pour tout h de H et tout i $(1 \leq i \leq k)$ $g_i h (g_i)^{-1}$ est élément de H.

De même si $G^{'}$ est un autre groupe engendré par $\{g_1^{'}, \ldots, g_l^{'}\}$ pour montrer que $G \subset G^{'}$ il suffit de montrer que pour tout i $(1 \leq i \leq k)$ g_i appartient à $G^{'}$ donc est un produit fini de $g_i^{'} (1 \leq i \leq l)$ ou de leurs inverses.

5.3. **Groupe monogène et groupe cyclique.**

Définition 5.3.1. Un groupe G est monogène si il existe g de G tel que tout élément de G soit de la forme g^k où k appartient à $\mathbb{Z}$. (On suppose ici que G est noté multiplicativement). Si G était noté additivement alors tout élément de G serait de la forme kg où k appartient à $\mathbb{Z}$.

On notera $G = <g>$ et on dit que g est un générateur de G.

Un groupe cyclique est un groupe monogène fini.

Exemple 5.3.1. $(\mathbb{Z},+)$ et $(\dfrac{\mathbb{Z}}{n\mathbb{Z}},+)$ sont des groupes monogènes.

Remarque : Si G est monogène alors le générateur n'est pas unique. Par exemple $\dfrac{\mathbb{Z}}{4\mathbb{Z}} = <\bar{1}>=<\bar{3}>$.

Proposition 5.3.1. *:*
Si $f : G \to G'$ est un morphisme de groupes et si G est monogène alors $f(G)$ est monogène.

Théorème 5.3.2 (Théorème de caractérisation des groupes monogène)**.** *Si G est un groupe monogène alors soit G est isomorphe à $\mathbb{Z}$ soit il existe un entier $n> 0$ tel que G soit isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.*

Preuve :
Si $G =< g >$ considérons le morphisme surjectif : $\mathbb{Z} \to G$ défini par $f(k) = g^k$.
Deux cas sont possibles : soit f est injectif auquel cas G est isomorphe à $\mathbb{Z}$ soit f n'est pas injectif et donc son noyau est un sous-groupe de $\mathbb{Z}$ donc de la forme $n\mathbb{Z}$ $(n > 0)$ et on applique le premier théorème d'isomorphisme.
On en déduit que si G est cyclique d'ordre n et g est un générateur alors on peut décrire G par $G = \{e, g, .., g^{n-1}\}$ en notation multiplicative ou en notation additive $G = \{e, g, .., (n-1)g\}$.

Corollaire 5.3.3. *Deux groupes cycliques de mme ordre sont isomorphes. Donc en particulier tout groupe cyclique d'ordre n est isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.*

5.4. **Ordre d'un élément.** Soit G un groupe et g un élément de G. On appelle ordre de g l'ordre du sous-groupe $< g >$ et on le notera $o(g)$.
Cet ordre peut étre infini par exemple pout tout élément de $\mathbb{Z}$. Le seul élément d'ordre 1 dans un groupe est l'élément neutre.

Proposition 5.4.1. *Soit g un élément du groupe G fini et n un entier positif.*

a) g est d'ordre n si et seulement si n est le plus petit entier positif tel que $g^n = e$.

b) g est d'ordre n si et seulement si $g^n = e$ et si $g^k = e$ alors k est multiple de n.
En particulier dans un groupe fini d'ordre n pour tout g de G on a $g^n = e$ car l'ordre de g divise n par le théorème de Lagrange.

Preuve :
Pour b) Soit n l'ordre de g et $g^k = e$. Divisons k par n donc $k = nq + r$ avec $0 \leq r < n$. $g^r = e$ et comme n est le plus petit entier tel que $g^n = e$ on a $r = 0$.
Cette proriété sera trés souvent utilisée.
Un exemple d'utilisation : Trouver à isomorphisme prés tous les groupes d'ordre 4.
Soit G un groupe d'ordre 4. Soit G posséde un élément d'ordre 4 donc G est cyclique et isomorphe à $\dfrac{\mathbb{Z}}{4\mathbb{Z}}$ soit G ne posséde aucun élément d'ordre 4 donc tous les éléments, hormis e sont d'ordre 2. Par suite ensemblistement $G = \{e, a, b, c\}$ avec $a^2 = b^2 = c^2 = e$. Essayons de construire la table du groupe.De ce fait $ab = ba$ car $b^{-1}aba^{-1} = e$. On est forçé de poser $ab = c$, $ac = b$,$bc = a$. Une fois la table construite on 'aperçoit que c'est la table de $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$. Donc à isomorphisme prés on n'a que deux groupes d'ordre 4.

Exercice 7. a) Montrer que dans le groupe $\dfrac{\mathbb{Q}}{\mathbb{Z}}$ tout élément est d'ordre fini.

b) Le groupe $\dfrac{\mathbb{Q}}{\mathbb{Z}}$ est-il fini ?

c) Soit G un groupe , x, y, z des éléments de G et N un sous-groupe distingué. On suppose que $x^5 \in N$, $y^7 \in N$ et que $y^{-1}zxz^{-1} \in N$. Montrer que $x \in N$ et $y \in N$. Indication : On pourra se placer dans $\frac{G}{N}$ et calculer les ordres de $\bar{x}$ et $\bar{y}$.

Proposition 5.4.2. *Si p est premier à isomorphisme prés il n'existe qu'un seul groupe d'ordre p à savoir $\frac{\mathbb{Z}}{p\mathbb{Z}}$ et de plus tous les éléments de G , $\neq e$ sont générateurs.*

Proposition 5.4.3. *Un isomorphisme de groupes conserve l'ordre des éléments.*

Exemple d'application : $\frac{\mathbb{Z}}{4\mathbb{Z}}$ et $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$.ne sont pas isomorphes.

5.5. **Sous-groupes des groupes monogènes.**

Compte tenu du théoréme de classification il suffit détudier les sous-groupes de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ puisque les sous-groupes de $\mathbb{Z}$ sont connus à savoir les groupes $d\mathbb{Z}$ où d est un entier positif.

Théorème 5.5.1 (Le Théoréme fondamental est le suivant)**.** *On notera par $\pi : \mathbb{Z} \to \frac{\mathbb{Z}}{n\mathbb{Z}}$ le morphisme surjectif défini par $\pi(k) = \bar{k}$.*

Les sous-groupes de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sont les $\pi(d\mathbb{Z})$ où d est un entier positif divisant n, donc sont isomorphe à $\frac{\mathbb{Z}}{d\mathbb{Z}}$

Preuve : On montre que l'on a une correspondance bijective entre les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ et les sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}$. En effet les deux applications

$\pi^* : \{$ sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}\} \to \{$ sous-groupes de $\frac{\mathbb{Z}}{n\mathbb{Z}}\}$ définie par $\pi^*(H) = \pi(H)$

et $\pi_* : \{$ sous-groupes de $\frac{\mathbb{Z}}{n\mathbb{Z}}\} \to \{$ sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}\}$ définie par $\pi_*(H) = \pi^{-1}(H)$ sont inverses l'une de l'autre.

Il suffit alors de remarquer qu'un sous-groupe de $\mathbb{Z}$ contenant $n\mathbb{Z}$ est un $d\mathbb{Z}$ où d divise n.

Exercice 8. a) Quels sont les sous-groupes de $\frac{\mathbb{Z}}{6\mathbb{Z}}$?

b) Montrer que G est cyclique d'ordre p, p premier, si et seulement si G ne posséde pas de sous-groupes propres.

5.6. **Générateurs d'un groupe monogène.**

Théorème 5.6.1. *Soit $G =< g >$ un groupe monogène noté multiplicativement..*

a) Si Gest infini alors g et g^{-1} sont les seuls générateurs de G.

b) Si G est fini d'ordre n, l'ensemble des générateurs est $\{g^k / \ k$ et n soient premiers entre eux dans $\mathbb{Z}\}$.

Preuve : a) est laissé au lecteur.

b) $< g >=< g^k > \Leftrightarrow$ il existe m tel que $g^{km} = g$. Donc $km - 1$ est multiple de n et on conclue par Bezout.

Corollaire 5.6.2. *Les générateurs du groupe $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$ sont les éléments inversibles pour la loi $\times$ de l'anneau $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times)$ donc les $\bar{k}$ tels que k et n soient premiers entre eux.*

5.7. **Produit de groupes cycliques.**

Proposition 5.7.1. *:*

Soit $G = < g >$ un groupe cyclique d"ordre n et $H = < h >$ un groupe cyclique d"ordre m. Alors (g, h) est d'ordre ppcm(m,n) dans le groupe $G \times H$.

Nous retrouvons ainsi comme Corollaire le :

Corollaire 5.7.2 (Théorème Chinois)**.** $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \times \dfrac{\mathbb{Z}}{m\mathbb{Z}}$ *est isomorphe à* $\dfrac{\mathbb{Z}}{nm\mathbb{Z}} \iff$ *n et m sont premiers entre eux.*

6. Le groupe symétrique S_n

Rapppelons qu'il s'agit du groupe des bijections de l'ensemble $\{1, 2, ..., n\}$ pour la loi de composition. Son ordre est $n!$.

6.1. **Généralités.** Soit $\sigma \in S_n$, on notera en général σ par

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

. Dans cette notation, le produit de $\sigma, \tau \in S_n$ se calcule par, puisqu'il s'agit de la composition d'applications,

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

Par exemple on a $\left(\begin{smallmatrix} 1&2&3 \\ 2&3&1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1&2&3 \\ 2&1&3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1&2&3 \\ 3&2&1 \end{smallmatrix}\right)$ (et non $\left(\begin{smallmatrix} 1&2&3 \\ 1&3&2 \end{smallmatrix}\right)$).

Terminologie : On dira que i $\in \{1, 2, ..., n\}$ est un point fixe de σ si $\sigma(i) = i$ et on appelle support de σ l'ensemble $\{i/\sigma(i) \neq i\}$. On notera le support de σ par Supp(σ)

Proposition 6.1.1. *Soit σ et τ deux permutations à supports disjoints alors $\sigma\tau = \tau\sigma$.*

Preuve :

On remarquera que si $i \in$ Supp(τ) alors $\tau(i) \in$ Supp(τ) car si $\tau(i) = j, j \neq i$ alors $\tau(j) = j$ impliquerait que $\tau(i) = \tau(j)$ et τ est bijective.

On distinguera les 3 cas $i \in$ Supp(τ), $i \in$ Supp(σ), i $\notin$ Supp(σ) $\cup$ Supp(τ) et on conclue.

Définition 6.1.1. Notion de σ-orbite

Soit σ un élément de S_n.

Sur $\{1, 2, ..., n\}$ on considère la relation $\sim$ définie par

$$i \sim j \iff \text{il existe } k \in \mathbb{Z} \text{ tel que } i = \sigma^k(j)$$

.

Cette relation est une relation d'équivalence et la classe d'équivalence de i sera appellée σ-orbite de i. et notée O_σ(i). Donc O_σ(i) = $\{\sigma^k(i)/k \in \mathbb{Z}\}$.

Remarquons que toute σ- orbite a k éléments si k est l'ordre de σ. Cette terminologie de σ-orbite s'expliquera lors du chapitre suivant.

6.2. **Cycles dans S_n et Signature.**

Soit $\sigma \in S_n$ et $i_1, ..., i_k$ des éléments de $\{1, 2, ..., n\}$ deux à deux di stincts. La permutation σ de support $\{i_1, ..., i_k\}$ définie par $\sigma(i_j) = i_{j+1}$ si $1 \leq j < k$ et $\sigma(i_k) = i_1$ est appellée cycle de longueur k et notée $(i_1, ..., i_k)$.

Remarquons que les cycles $(i_1, ..., i_k)$ et par exemple $(i_2, ..., i_k, i_1)$ sont les mêmes.

Une transposition est un cycle de longueur 2 donc une permutation qui échange 2 éléments et laisse tous les autres fixes.

Dans S_n le cycle (1, ...,n) est appellé permutation circulaire.

Théorème 6.2.1 (Théorème de décomposition)**.** *Tout élément de S_n peut s'écrire*

$$\sigma = \gamma_1 ... \gamma_k$$

où les γ_i sont des cycles à support deux à deux disjoints. Cette décomposition est unique à l'ordre prés.

Indication : Les σ-orbites forment une partition de $\{1, 2, ..., n\}$ et chaque σ-orbite donne naissance à un cycle.

Ordre d'une permutation
Si σ est un cycle de longueur l son ordre est l.

Proposition 6.2.2. *Soit σ un élément de S_n tel que $\sigma = \gamma_1...\gamma_l$ soit sa décomposition en cycles disjoints. L'ordre de σ est le ppcm(longueurs (γ_i)) $(1 \leq i \leq l)$).*

Indication :$\sigma^k|_{Supp(\gamma_i)} = \gamma_i^k$. Donc si k est l'ordre de σ alors k est un multiple de la longueur des γ_i pour $1 \leq i \leq l$.

Pratique de la décomposition en cycle
Il suffit de trouver toutes les σ-orbite.
Sur un exemple si σ est la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$ alors $\sigma =$ (1,5,3)(4,6).
Les cycles étant disjoints ceci permet de calculer les puissances de σ. Par exemple σ est d'ordre 6 donc $\sigma^{2006} = \sigma^{6\times 334+2} = \sigma^2$.

Cycle conjugé
Soit γ un cycle de S_n et σ une permutation de S_n .Le conjugué de γ par σ est le cycle $\sigma\gamma\sigma^{-1}$ et si $\gamma = (i_1, ..., i_k)$ alors $\sigma\gamma\sigma^{-1} = (\sigma(i_1), ..., \sigma(i_k))$.
La vérification est immédiate. Cette formule sera souvent utilisée dans les exercices.

Proposition 6.2.3. Un systéme de générateurs de S_n
Pour n $\geq$ 2 toute permutation est un produit de transpositions non permutables en général.

Indication : En effet le cycle (1,...,k) = (1,2)(2,3)...(k-1,k) et on conclue par le théorème de décomposition.
On remarquera que la décomposition n'est pas unique, par exemple la transposition (i,j) est aussi le produit des 3 transpositions, (1,i)(1,j)(1,i), et que dans le produit on n'a pas forçément des transpositions disjointes.
Cependant on verra, par la suite, que le nombre de transpositions dans la décomposition de σ a toujours même parité.
Bien sur on a d'autres systémes de générateurs de S_n. On en verra certains au cours des exercices.

Définition 6.2.1 (Signature d'une permutation)**.** Soit σ une permutation de S_n. On appelle signature de σ l'entier $(-1)^{n-k}$ si k est le nombre de σ-orbites. On le note $\epsilon(\sigma)$.

Si nous utilisons la décomposition en cycles disjoints, k est le nombre de cycles intervenant dans la décomposition **en comptant pour 1 tout cycle correspondant à un point fixe** . Par exemple :
si γ est un cycle de longueur l dans S_n, on a $\epsilon(\gamma) = (-1)^{n-(n-l+1)} = (-1)^{(l-1)}$. (car on a $n-l$ points fixes).

Théorème 6.2.4. *Soit $\sigma \in S_n (2 \leq n)$ alors quelque soit la transposition $\tau \in S_n$ on a $\epsilon(\sigma\tau) = -\epsilon(\tau)$.*

Preuve :
Supposons que $\tau = (i, j)$.
Si k $\notin O_\sigma(i)$ et k $\notin O_\sigma(j)$ alors $O_{\sigma\tau}(k) = O_\sigma(k)$.
Considérons les σ- orbites contenant i ou j.
Deux cas sont possibles :

$1^{er} cas$: i et j sont dans deux σ- orbite distinctes, calculons la $\sigma\tau$-orbite de i.

$O_\sigma(i) = \{i, \sigma(i), \ldots, \sigma^{p-1}(i)\}$ et $O_\sigma(j) = \{j, \sigma(j), \ldots, \sigma^{q-1}(j)\}$.

$\sigma\tau(i) = \sigma(j)$ donc si $1 \leq k \leq q-1$ alors $(\sigma\tau)^k(i) = \sigma^k(j)$ et $(\sigma\tau)^q(i) = j$. Donc $(\sigma\tau)^{q+1}(i) = \sigma(i)$.

Par suite pour $1 \leq k \leq p-1$ on a $(\sigma\tau)^{q+k}(i) = \sigma^k(i)$ et $(\sigma\tau)^{q+p}(i) = i$

Les éléments des σ-orbites de i et j se trouvent regroupés dans une même $\sigma\tau$- orbite

$2^{eme} cas$ i et j sont dans la même σ- orbite.

Soit $O_\sigma(i) = \{i, \sigma(i), \ldots, \sigma^{p-1}(i)\}$ et il existe un entier $r(1 \leq r \leq (p-1))$ tel que $j = \sigma^r(i)$.

Calculons la $\sigma\tau$-orbite de i.

$\sigma\tau(i) = \sigma(j) = \sigma^{r+1}(i)$ donc pour $(1 \leq l < p-r)$ $(\sigma\tau)^l(i) = \sigma^{r+l}(i)$ et $(\sigma\tau)^{p-r}(i) = i$.

Donc $O_{\sigma\tau}(i) = \{i, \sigma^{r+1}(i), \ldots, \sigma^{p-1}(i)\}$.

De même $O_{\sigma\tau}(j) = \{j, \sigma(i), \ldots, \sigma^{r-1}(i)\}$

Les éléments de $O_{\sigma\tau}(i)$ se trouvent dans deux σ- orbites différentes contenant respectivement i et j.

Si donc t est le nombre de σ-orbites distinctes, le nombre de $\sigma\tau$-orbites distinctes est $t-1$ dans le premier cas et $t+1$ dans le second d'où le résultat.

Théorème 6.2.5. *Si la permutation σ de S_n est le produit de k transpositions alors $\epsilon(\sigma) = (-1)^k$. On en déduit que dans toute décomposition de σ en produit de transpositions la parité du nombre de transpositions est la même .*

Preuve :

Soit $\sigma = \tau_1 ... \tau_k$ une décomposition de σ en produit de transpositions . Vu le théorème précédent on a $\epsilon(\tau_1 ... \tau_k) = -\epsilon(\tau_2 ... \tau_k) = (-1)^k$.

Donc si $\sigma = \tau_1 ... \tau_k = \tau_1^{'} ... \tau_l^{'}$ sont deux décompositions de σ en produit de transpositions $\epsilon(\sigma) = (-1)^k = (-1)^l$ et donc l et k ont même parités.

Théorème 6.2.6. $\epsilon : S_n \to \{-1, 1\}$ *est un morphisme surjectif de groupes.*

Preuve :

On applique le théorème précédent et $(-1)^{k+l} = (-1)^k(-1)^l$.

Définition 6.2.2 (Le groupe alterné)**.** Le noyau de ϵ est appellé groupe alterné et sera noté A_n .

Son ordre est (premier théorème d'isomorphisme) $\frac{n!}{2}$. Ses éléments sont dits permutation paire car produit paire de transpositions.

Proposition 6.2.7. *Pour $n \geq 3$ A_n est engendré par les cycles de longueur 3.*

Preuve :

Tout élément de A_n est un produit pair de transpositions. Or $(a, b)(c, d) = (a, b, c)(b, c, d)$ et $(a, b)(b, c) = (a, b, c)$

Ce groupe est donc un sous-groupe distingué de S_n (noyau d'un morphisme ou encore d'indice 2)et sera étudié ultérieurement plus en détail.

Petit exemple d'application sur un jeu On considère le jeu bien connu suivant. Il y a un tableau à 16 cases, dont une case est vide et dont les autres sont numérotées de 1 à 15 :

(a)

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Dans ce tableau, on peut faire glisser les cases, ou autrement dit : la case vide peut être échangée avec une de ses voisines. Par exemple, en faisant glisser la case 12 dans le tableau ci-dessus, on

arrive à la position

(b)

1	2	3	4
5	6	7	8
9	10	11	
13	14	15	12

Ce qu'on se demande alors est si en partant de la position (a) en haut on peut arriver à la position

(c)

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Nous allons montrer que cela est impossible. On dira que la case vide est la case 16. En faisant glisser les cases, on fait des permutations de $\{1, 2, \ldots, 16\}$. On appellera un coup un échangement de la case 16 avec une de ses voisines. Chaque fois qu'on fait un coup, la permutation qu'on a est multipliée par un cycle de longueur deux. Donc chaque coup, la permutation qu'on a change de signe. Comme la permutation correspondant à la position (c) est le cycle $(14, 15)$, donc une permutation impaire, on ne pourra pas y arriver en un nombre pair de coups. Maintenant suivons le trajet que fait la case 16 quand on fait des coups. En prétendant que la case 16 fait son trajet sur un échiquier où les cases sont noir et blanc

n	b	n	b
b	n	b	n
n	b	n	b
b	n	b	n

on constate qu'à chaque coup, la case où se trouve le 16 change de couleur. On voit donc qu'après un nombre impair de coups, la case 16 ne peut pas se trouver à sa position initiale. Nous avons vu maintenant que la transition de la position (a) en la position (c) ne peut se faire ni en un nombre pair de coups, ni en un nombre impair de coups.

6.3. **Etude des groupes d'ordre ≤ 7.**

Théorème 6.3.1. *A isomorphisme prés il n'existe que deux groupes à 6 éléments à savoir* $\dfrac{\mathbb{Z}}{6\mathbb{Z}}$ *et* S_3.

La démonstration nécessite les deux lemmes préliminaires suivants

Lemme 6.3.2. $S_3 =< \sigma, \tau >$ *où* $\sigma = (1, 2, 3)$ *et* $\tau = (1, 2)$. *De plus* σ *est d'ordre 3,* τ *est d'ordre 2 et* $\sigma\tau = \tau\sigma^2$

Lemme 6.3.3. *Si* G *est un groupe dont tous les éléments* $\neq e$ *sont d'ordre 2 alors* G *est commutatif et si* G *est fini alors son ordre est une puissance de 2.*

Preuve du théorème :

En utilisant ces deux lemmes et en raisonnant sur l'ordre des éléments on obtient le résultat. car soit G a un élément d'ordre 6 et donc est isomorphe à $\dfrac{\mathbb{Z}}{6\mathbb{Z}}$ soit on n'en a pas auquel cas il existe un élément d'ordre 3 vu le lemme précédent. Soit σ cet élément Donc ensemblistement $G = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ où $\tau \notin \{e, \sigma, \sigma^2\}$.

τ est d'ordre 2 car $\dfrac{G}{< \sigma >}$ est d'ordre 2 donc $\bar{\tau^2} = \bar{e}$ et donc $\tau \in \{e, \sigma, \sigma^2\}$. Si $\tau^2 = \sigma$ alors $\tau^3 = \sigma\tau$ donc τ serait d'ordre 6 et si $\tau^2 = \sigma^2$ alors $\tau^3 = \sigma^2\tau$ donc τ serait d'ordre 6.De même $\sigma\tau$ et $\sigma^2\tau$ sont d'ordre 2.

Examinons $\tau\sigma$: $\tau\sigma \notin \{e, \sigma, \sigma^2, \tau\}$ et $\tau\sigma \neq \sigma\tau$ sinon $(\tau\sigma)^2 = \sigma^2$ et $(\tau\sigma)^3 = \tau$ et donc on aurait un élément d'ordre 6. Donc $\tau\sigma = \sigma^2\tau$.

On obtient un isomorphisme de G avec S_3 donné par $\sigma \to (1,2,3)$ et $\tau \to (1,2)$.

On connait donc tous les groupes à isomorphisme prés d'ordre ≤ 7. Reste à traiter les groupes d'ordre 8. Pour l'instant on en connait 5 à savoir $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$, $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}}$, $\frac{\mathbb{Z}}{8\mathbb{Z}}$ et le diédral D_4 et le groupe des quaternions . On verra par la suite que ce sont les seuls groupes à 8 éléments.

Exercice 9. 1) Donner le(s) morphisme(s) possible(s) de S_3 dans $\frac{\mathbb{Z}}{12\mathbb{Z}}$.

2) Soit σ la permutation, élément de S_{12}.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 11 & 7 & 3 & 2 & 6 & 12 & 5 & 4 & 1 \end{pmatrix}$$

La permutation σ est-elle élément de A_{12} ?

6.4. **Le groupe A_4 n'est pas simple.** Le but est de montrer que le groupe A_4 posséde un sous-groupe propre distingué.

Description des éléments de A_4

Comme $|A_4| = 12$ ses éléments sont d'ordre 1,2,3,4,6 ou 12.
Elément d'ordre 1 : l'élément neutre
Elément d'ordre 2 : produit de 2 transpositions disjointes donc (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)
Elément d'ordre 3 : produit de 2 transpositions non disjointes donc les 3-cycles :
(1,2,3), (1,2,4), (1,3,4), (2,3,4) et leurs carrés
On a donc les 12 éléments de A_4.

Etude des sous-groupes de A_4

Proposition 6.4.1. *A_4 ne contient pas de sous-groupes d'ordre 6*

Preuve : Soit H un sous-groupe d'ordre 6. H contient un 3-cycle σ_1 et donc son carré. Si H contient un autre 3-cycle $\sigma_2 \notin \{e, \sigma_1, \sigma_1^2\}$ alors $H \supset \{e, \sigma_1, \sigma_1^2, \sigma_2, \sigma_2^2, , \sigma_1\sigma_2, \sigma_1\sigma_2^2\}$ soit déja 7 éléments tous différents. (En fait on retrouve le groupe A_4 dans ce cas). Donc si H est d'ordre 6, H contient un seul 3-cycle (a,b,c), et les 3 doubles transpositions disjointes. Or (a,c)(b,d) = (a,b,c) (a,b,d) et donc le 3-cycle (a,b,d) appartientà H qui contient donc deux 3-cycles. absurde.

Remarquons que bien que 6 divise $|A_4|$ on n'a pas de sous-groupe d'ordre 6 et à fortiori d'élément d'ordre 6.

Proposition 6.4.2. *A_4 contient un sous-groupes d'ordre 4 qui est distingué.*

Preuve :
Comme A_4 n'a pas d'élément d'ordre 4, le seul sous-groupe d'ordre 4 est
$\{Id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$.
Ce sous-groupe H est distingué car il suffit de vérifier que si σ est un 3-cycle alors $\sigma\tau\sigma^{-1} \in H$ pour tout τ produit de deux transpositions disjointes.
On laisse le soin au lecteur d'énumérer les sous-groupes de A_4. On en trouvera 3 d'ordre 2 et 4 d'ordre 3 et 1 d'ordre 4.

7. Groupe opérant sur un ensemble

7.1. **Généralités.**

Définition 7.1.1. Soit G un groupe noté multiplicativement (d'élément neutre e) et X un ensemble. On dit que G opére (ou agit) à gauche sur X si il existe une application $G \times X \to X$ notée $(g, x) \to g.x$ telle que

$$e.x = x \text{ pour tout } x \text{ de } X$$
$$(gh).x = g.(h.x) \text{ pour tout } g \text{ et } h \text{ de } G \text{ et tout } x \text{ de } X.$$

.

On définit de façon similaire une action à droite. Dans toute la suite on dira que G agit sur X pour G opére sur X à gauche.

Proposition 7.1.1. *Soit G opérant sur X.*
a) Si g est un elémént de G l'application $\gamma_g : X \to X$ définie par $\gamma_g(x) = g.x$ est bijective.
b) l'application $\gamma : G \to S_X$ définie par $\gamma(g) = \gamma_g$ est un morphisme.

Preuve :
Pour a) On vérifiera que $(\gamma_g)^{-1} = \gamma_{g^{-1}}$.
Pour b) On obtient que $\gamma(gg^{'}) = \gamma_{gg'}$

Donc à toute action de G sur X correspond un morphisme de G dans S_X et réciproquement à tout morphisme α de G dans S_X correspond une action de G sur X donnée par $(g, x) \to \alpha(g)(x)$.

Exemple 7.1.1 (Exemples classiques)**.**

1) G opére sur lui-même par translation : $g.h = gh$ ou par conjuguaison : $g.h = ghg^{-1}$.
Remarquons que si H est un sous-groupe distingué de G, on a aussi une action de G sur H par conjuguaison.

2) G opére sur les parties de G par translation : $g.\{g_1...g_k\} = \{gg_1, \ldots, gg_k\}$.

3) Si H est un sous-groupe de G, G opére sur les classes à gauche de $(\frac{G}{H})_g$ par $g.xH = gxH$. Attention ne pas oublier de vérifier que l'on a bien une application.

Si G agit sur lui même par conjuguaison ceci induit donc une bijection de G dans G définie par, si g est un élément de G, $\gamma_g(h) = ghg^{-1}$.
On vérifie que γ_g est un morphisme appellé automorphisme interieur.

Proposition 7.1.2. *Soit G un groupe fini d'ordre n. Alors G est isomorphe à un sous-groupe de S_n.*

Preuve :
Faisons opérer G sur G par translation. Ceci induit donc un morphisme γ de G dans S_n. $ker(\gamma) = \{g \in G / \forall h \in G \ gh = h\}$. Par suite si $g \in G$ $ge = g = e$ donc $ker(\gamma) = \{e\}$ et on conclue par le premier théorème d'isomorphisme.

Proposition 7.1.3. $\frac{G}{Z(G)}$ *est isomorphe à Int(G).*

Preuve :
Soit $f : G \to Int(G)$ définie par $f(g) = f_g$ où $f_g(h) = ghg^{-1}$. On vérifie que $f_g \in Int(G)$, et que f est un morphisme surjectif dont le noyau est $Z(G)$.

7.2. **Orbites et Stabilisateurs.**

Définition 7.2.1. Soit G un groupe opérant sur l'ensemble X.

On appelle stabilisateur de $x \in X$ et on note G_x le sous-groupe de G

$$G_x = \{g \in G / g.x = x\}$$

Ne pas oublier de vérifier que G_x est un sous-groupe. .

En conséquence si G est fini le cardinal de G_x divise le cardinal de G.

On dit que $x \in X$ est un point fixe si $G_x = G$.

Sur X on considére la relation $x\mathcal{R}y \iff \exists g \in G / y = g.x$.

On vérifie que $\mathcal{R}$ est une relation d'équivalence sur X et on appelle orbite de x notée Gx la classe d'equivalence de x donc

$$Gx = \{g.x / g \in G\}$$

.

Exemple : Soit $\sigma \in S_n$. Faisons agir $< \sigma >$ sur $\{1, ..., n\}$ par $(\sigma^k, i) \to \sigma^k(i)$. L'orbite de i pour cette action n'est rien d'autre que la σ-orbite de i.

Du fait que $\mathcal{R}$ soit une relation d'équivalence les orbites forment une partition de X et donc si X est fini son cardinal est la somme des cardinaux des orbites.

Si G agit sur G par conjuguaison deux éléments d'une même orbite sont dits conjugués.

On dira aussi que deux sous-groupes H_1 et H_2 de G sont conjugués si il existe $g \in G$ tel que $H_1 = gH_2g^{-1}$.

Exercice 10.

a) Si G opére sur lui-même par translation quel est l'orbite et le stabilisateur de $h \in G$?

b) Si G opére sur lui-même par conjuguaison quel est le stabilisateur de $h \in G$?

Proposition 7.2.1. *Si G opére sur X. Si x et y sont dans la même orbite alors les stabilisateurs de x et y sont conjugués.*

Preuve :

Par hypothése, $\exists g \in G$ tel que $y = g.x$.

On va montrer que $G_y \subset gG_xg^{-1}$ donc que si $g^{'} \in G_y$ alors $g^{-1}g^{'}g \in G_x$ soit $(g^{-1}g^{'}g).x = x$.

$(g^{-1}g^{'}g).x = (g^{-1}g^{'}).y = g^{-1}.(g^{'}.y) = g^{-1}.y = x$.

Inversement si $g^{'} \in gG_xg^{-1}$ alors $g^{'} = ghg^{-1}$ et $h.x = x$ donc $g^{'}.y = ghg^{-1}.y = g.h.x = g.x = y$

Théorème 7.2.2. *Si G opére sur X alors pour tout x de X le cardinal de Gx est $[G : G_x]$ donc le nombre de classes à gauche (ou à droite) de $(\frac{G}{G_x})_g$.*

Indication : On montre que l'application $\lambda : Gx \to (\frac{G}{G_x})_g$ définie par $\lambda(g.x) = gG_x$ est une bijection. (Ici encore commençer par vérifier que l'on a bien une application).

Corollaire 7.2.3 (formule des classes)**.** *Soit G opèrant sur X ensemble fini. Si r est le nombre d'orbites et x_i un repréntant de la i^{eme} orbite alors $|Gx_i| = [G : G_{x_i}]$.*

En particulier $|X| = \sum_{1 \leq i \leq r} |Gx_i|$.

Remarquons que si G est fini $|Gx| = \frac{|G|}{|G_x|}$ et donc que le cardinal d'une orbite divise le cardinal du groupe.

7.3. **Cas d'opération par conjuguaison.** Soit G opérant sur G par conjuguaison donc $g.h = ghg^{-1}$

Les orbites sont appellées classes de conjuguaison.

Remarquons que $h \in Z(G) \iff G_h = G \iff Gh = \{h\}$

Exercice 11. Déterminer les groupes finis G qui ont une seule classe de conjuguaison puis deux classes de conjuguaison. On verra en TD le cas des groupes qui possédent 3 classes de conjuguaison.

Proposition 7.3.1. *Formule des classes.*

Soit G un groupe fini opérant sur G par conjuguaison alors

$$|G| = |Z(G)| + \sum_{1 \leq i \leq k} |Gx_i|$$

où k est le nombre d'orbites et les x_i sont les représentants des orbites de cardinal > 1.

7.4. **Application aux p-groupes.**

Un groupe G est dit un p-groupe (p premier) si son ordre est $p^\alpha (\alpha > 0)$.

Lemme 7.4.1. *Si G est un p-groupe son centre est non trivial.c'est à dire $\neq \{e\}$.*

Preuve :

Si G est non abélien faire opérer G sur G par conjuguaison et appliquer la formule des classes.

Lemme 7.4.2. *Tout groupe d'ordre p^2 (p premier) est abélien.*

Preuve :

Le lemme précédent nous dit que $|Z(G)| = p$ ou p^2. Si $|Z(G)| =$ p, on a $\dfrac{G}{Z(G)}$ cyclique et donc G est abélien sinon $Z(G) = G$.

Ce dernier résultat nous permettra (cf chapitre 8) de classifier tous les groupes d'ordre p^2 et de montrer que l'on n'a que $\dfrac{\mathbb{Z}}{p^2\mathbb{Z}}$ ou $\dfrac{\mathbb{Z}}{p\mathbb{Z}} \times \dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

7.5. **Etude des points fixes et une application le Théoréme de Cauchy.** Soit G un groupe opérant sur X.

On dit que $x \in X$ est un point fixe si $G_x = G$ donc si pour tout g de G $g.x = x$. Si donc G est fini ceci revient à dire que $Gx = \{x\}$.

On notera par $Fix(G)$ l'ensemble des points fixes.

Lemme 7.5.1. *Soit G un groupe d'ordre p^n opèrant sur X ensemble fini.*

on a $|Fix(G)| \equiv |X|$ (mod p).

Nous savons qu'une conséquence du théoréme de Lagrange est que l'ordre d'un élément de G , groupe fini, divise l'ordre du groupe. Nous avons déja vu que la réciproque est fausse (A_4 n'a pas d'élément d'ordre 4 ou 6). Par contre pour certains types de groupes, les groupes cycliques, la réciproque est vraie (confére le chapitre 5). Le théoréme suivant précise que pour certains types de diviseurs la réciproque est encore vraie.

Proposition 7.5.2 (Théoréme de Cauchy)**.**

Soit p un entier premier divisant l'ordre de G groupe fini. Alors G posséde un élément d'ordre p.

Preuve :

Soit $X = \{(g_1, ..., g_p) \in G^p / g_1...g_p = e\}$.

Pour choisir un élément de X on doit choisir $p-1$ éléments de G donc $|X| = |G|^{p-1}$. En effet une fois $g_1, ..., g_{p-1}$ choisis, on a $g_p = (g_1...g_{p-1})^{-1}$.

Soit $\sigma : X \to X$ définie par $\sigma(g_1, ..., g_p) = (g_2, ..., g_p, g_1)$. On vérifie que $\sigma \in S_X$. On en déduit une action de $< \sigma >$, qui est isomorphe à $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, sur X. Pour cette action le cardinal des orbites divisant celui de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ est 1 ou p. Si donc x est le nombre d'orbites à 1 élément et y celui des orbites à p éléments on a $|X| = x+py$. Comme $|X|$ est un multiple de p, x est mutiple de p et donc $x > 1$. Il existe donc un p-tuple $(g_1, ..., g_p)$de X tel que $(g_1, ..., g_p) = (g_2, ..., g_p, g_1) = ... = (g_p, g_1, ..., g_{p-1})$ soit $g_1 = ... = g_p$. Donc $g^p = g_1...g_1 = e$ et g est d'ordre p.

Une autre démonstration utlisant les théorémes de Sylow, sera vue au chapitre 9.

Exercice 12. Soit G un groupe à 15 éléments agissant sur un ensemble de 17 éléments en ne laissant aucun point fixe. Quel est le nombre d'orbites ? Donner le nombre d'éléments de chaque orbite.

8. Classification à isomorphisme prés des groupes d'ordre ≤ 8

Le but est étant donné un entier $n \geq 8$ et un groupe d'ordre n de donner à isomorphisme prés le(s) groupe(s) G.

Nous utiliserons les résultats suivants :

R1) Si p est un entier premier alors tout groupe G d'ordre p est isomorphe à $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ et donc tout élément de $G \neq e$ est générateur.

R2) Si dans G tout élément $\neq e$ est d'ordre 2 alors G est commutatif et de plus $|G|$ est une puissance de 2.

R3) Tout groupe abélien fini est un produit de groupes cycliques dont l'ordre est une puissance d'un nombre premier. (Ce résultat fait l'objet du chapitre ? ?) mais ne sera pas exposé en L-3.

Par exemple si G est d'ordre 8 et abélien à isomorphisme près on trouvera 3 groupes $\dfrac{\mathbb{Z}}{8\mathbb{Z}}, \dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{4\mathbb{Z}}, \dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$.

R4) Si $Z(G)$ est le centre de G et si $\dfrac{G}{Z(G)}$ est cyclique alors G est commutatif.

R5) Tout p-groupe (c'est à dire tout groupe dont l'ordre est une puissance d'un nombre premier) a un centre non trivial (donc non rèduit à $\{e\}$

Rappelons que l'on connait des groupes non commutatifs

-> d'ordre 6 à savoir S_3, qui est le groupe engendré par σ et τ si $\sigma = (1,2,3)$ et $\tau = (1,2)$ avec la relation $\sigma\tau = \tau\sigma^2$.

-> d'ordre 8 à savoir D_4, groupe des isométries du carré, engendré par r, rotation de centre le centre du carré et d'angle $\dfrac{\pi}{2}$ et s, symétrie par rapport à une diagonale avec la relation $sr = r^3 s$.

Soit donc G tel que $|G| = n, n \leq 8$.

Si $\underline{n = 2, 3, 5, 7}$:

par R1 G est cyclique isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

SI $\underline{n = 4}$:

Soit on a un élément d'ordre 4 et donc G est cyclique, isomorphe à $\dfrac{\mathbb{Z}}{4\mathbb{Z}}$.

Soit tous les éléments $\neq e$ sont d'ordre 2 et par R2 et R3 G est isomorphe à $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$.

On peut aussi, sans utiliser R2 et R3, faire la table du groupe et s'apercevoir que c'est celle de $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$.

Si $\underline{n = 6}$:

Soit on a un élément d'ordre 6 et donc G est cyclique, isomorphe à $\dfrac{\mathbb{Z}}{6\mathbb{Z}}$

Soit on a pas d'éléments d'ordre 6 donc tous les éléments $\neq e$ sont d'ordre 2 ou 3. Par R2 il existe un élément d'ordre 3 (6 n'est pas une puissance de 2).

Soit σ cet élément. Donc ensemblistement $G = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ où $\tau \notin \{e, \sigma, \sigma^2\}$. On vérifiera que ces 6 éléments sont tous distincts.

τ est d'ordre 2 car $\dfrac{G}{< \sigma >}$ est un groupe d'ordre 2 ($< \sigma >$ est distingué dans G car d'indice 2) donc $\bar{\tau}^2 = \bar{e}$ et donc $\tau \in \{e, \sigma, \sigma^2\}$. Si $\tau^2 = \sigma$ alors $\tau^3 = \sigma\tau$ donc τ serait d'ordre 6 et si $\tau^2 = \sigma^2$ alors $\tau^3 = \sigma^2\tau$ donc τ serait d'ordre 6. De même $\sigma\tau$ et $\sigma^2\tau$ sont d'ordre 2.

Examinons $\tau\sigma$: $\tau\sigma \notin \{e, \sigma, \sigma^2, \tau\}$ et $\tau\sigma \neq \sigma\tau$ sinon $(\tau\sigma)^2 = \sigma^2$ et $(\tau\sigma)^3 = \tau$ et donc on aurait un élément d'ordre 6. Donc $\tau\sigma = \sigma^2\tau$.

On peut aussi remarquer que $< \sigma >$ étant distingué dans G, $\tau\sigma\tau^{-1} \in < \sigma >$ et donc $\tau\sigma\tau^{-1}$ ayant même ordre que σ on a $\tau\sigma\tau^{-1} = \sigma$ ou σ^2. Le cas $\tau\sigma\tau^{-1} = \sigma$ est impossible car G est non commutatif donc $\tau\sigma = \sigma^2\tau$.

On obtient donc un isomorphisme de G avec S_3 donné par $\sigma \to (1,2,3)$ et $\tau \to (1,2)$.

En conclusion à isomorphisme pres il n'existe que 2 groupes à 6 éléments : S_3 et $\dfrac{\mathbb{Z}}{6\mathbb{Z}}$.

Si $\underline{n = 8}$:

Le cas où G est abélien est vu par R3). Supposons G **non commutatif** .

Lemme 1 : G posséde un élément, ρ, d'ordre 4 et $< \rho >$ est un sous-groupe distingué de G.
Preuve :

Comme G est non commutatif on a pas d'élément d'ordre 8 et par R2) les éléments $\neq e$ ne peuvent être tous d'orde 2, d'où l'existence de ρ d'ordre 4 et $< \rho >$ est un sous-groupe d'ordre 2 donc distingué.

Lemme 2 : On a $Z(G) = \{e, \rho^2\}$.
Preuve :

Montrons d'abord que $|Z(G)| = 2$. Comme $Z(G)$ est un sous-groupe de G son ordre est 1,2,4 ou 8. Par R5 ce n'est pas 1 (car $8 = 2^3$), par R4 ce n'est pas 4 (sinon $\dfrac{G}{Z(G)}$ est isomorphe à $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ donc G serait commutatif et $Z(G) \neq G$ (G est non commutatif).

Reste à montrer que $\rho^2 \in Z(G)$.

Comme $< \rho >= \{e, \rho, \rho^2, \rho^3\}$ est distingué, pour tout $g \in G$ on a $g\rho^2 g^{-1} \in < \rho >$. Or $g\rho^2 g^{-1}$ est un élement d'ordre 2 de $< \rho >$ qui n'a que ρ^2 d'ordre 2 donc pour tout $g \in G$ on a $g\rho^2 g^{-1} = \rho^2$.

Lemme 3 : On suppose qu'il existe $s \in G - < \rho >$, s d'ordre 2. Montrer que si un tel groupe existe alors $G = \{e, \rho, \rho^2, \rho^3, s, \rho s, \rho^2 s, \rho^3 s\}$ puis montrer que $s\rho s^{-1} = \rho^{-1}$. Conclure que G est isomorphe à D_4.
Preuve ;

On vérifie facilement que pour $i, j \in \{0,1,2,3\} \rho^1 s \neq \rho^j$ et que si $i \neq j$ alors $\rho^i s \neq \rho^j s$. Donc si un tel groupe existe alors ensemblistement $G = \{e, \rho, \rho^2, \rho^3, s, \rho s, \rho^2 s, \rho^3 s\}$ (G ne posséde que 8 éléments)et donc G serait le groupe engendré par ρ et s.

Montrons que $s\rho s^{-1} = \rho^{-1} = \rho^3$. Comme $< \rho >$ est distingué $s\rho s^{-1} > \in < \rho >$, donc $s\rho s^{-1} = e, \rho, \rho^2$ ou ρ^3. $s\rho s^{-1} \neq e$ sinon $\rho = e$, $s\rho s^{-1} \neq \rho$ sinon G est commutatif, $s\rho s^{-1} \neq \rho^2$ sinon $s\rho s^{-1}$ serait d'ordre 2 et il est de même ordre que ρ donc $s\rho s^{-1} = \rho^3$.

Par suite un tel groupe existe et est isomorphe à D_4.

Reste le cas où il n'existe aucun élément de $G - < \rho >$ d'ordre 2 (*).

Soit donc G un groupe tel que (*) donc tous les éléments autre que e et ρ sont d'ordre 4. Notons $\rho = i$ et $j \notin \{e, i, i^2, i^3\}$ un autre élément d'ordre 4. Esemblistement $G = \{e, i, i^2, i^3, j, ij, i^2 j, i^3 j\}$. On vérifie facilement que tous les éléments sont distincts.

De plus on a la relation $ji = i^3 j$ car $< i >$ étant un sous-groupe de G d'indice 2, il est distingué donc jij^{-1} qui est d'ordre 4 est egale à i ou i^3. Le cas $jij^{-1} = i$ est impossible car G n'est pas commutatif donc $ji = i^3 j$.

On conclue que **si** un groupe G tel que (*) existe il n'y en a qu'un à isomorphisme prés. Reste donc à trouver un tel groupe de façon concréte.

Le groupe des Quaternions $\mathbb{H}$.

Soit les deux matrices de $GL(2,\mathbb{C})$:

$$M_i = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, M_j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

.

Montrons que le sous-groupe $\mathbb{H}$ de $GL(2,\mathbb{C})$ engendré par M_i, M_j a 8 éléments.

On vérifie que M_i et M_j sont d'ordre 4 et que $M_iM_j = \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix}$.

Donc ensemblistement $G \supset \{Id, M_i, M_i^2, M_i^3, M_j, M_iM_j, M_i^2M_j, M_i^3M_j\}$. Tous ces éléments sont en effet différents. De plus on a la relation $M_jM_i = M_i^3M_j$ donc G a exactement 8 éléments.

En **conclusion** pour les groupes d'ordre 8 on en a 5 dont 3 commutatifs et 2 non commutatifs.

On peut aussi classifier les groupes d'ordre 9 : En effet au chapitre précedent on a vu que tout groupe d'ordre p^2, p premier, est abélien donc par R3 les groupes d'ordre p^2 sont, à isomorphisme pres, $\frac{\mathbb{Z}}{p^2\mathbb{Z}}$ et $\frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}$.

:

9. Théorèmes de Sylow

Soit G un groupe fini d'ordre n. On sait que si d est un diviseur de n alors G n'a pas forçément de sous-groupe d'ordre d (Par exemple A_4 n' as pas de sous-groupe d'ordre 6).

Par contre, pour certains types de diviseurs d de n, Sylow a montré (1872) que l'on avait toujours un sous-groupe d'ordre d.

Soit donc G un groupe fini d'ordre n $=p^\alpha m$ avec p premier et p premier avec m. Remarquons qu'une telle écriture est toujours possible suite à la décomposition en facteurs premiers de n.

On appelle p-sous-groupe de Sylow de G (ou encore p-Sylow de G) tout sous-groupe H de G d'ordre p^α.

9.1. **Enoncés des théorémes.**

Soient G un groupe fini, p un nombre premier, $|G| = p^\alpha m$ avec m premier à p. Alors :

Théoréme 1 : il existe des p-groupes de Sylow dans G,

Théoréme 2 : Pour tout p-sous-groupe de G et tout p-Sylow S de G, il existe un $a \in G$ tel que $H \subset aGa^{-1}$

Théoréme 3 : les p-groupes de Sylow sont conjugués entre eux : pour S et S' des p-groupes de Sylow dans G il existe $g \in G$ tel que $S' = gSg^{-1}$,

Théoréme 4 : le nombre s_p de p-groupes de Sylow dans G divise m et est congru à 1 modulo p.

9.2. **Démonstration des Théorémes.**

Démonstration du Théoréme 1

Cette démonstration a été trouvée dans les notes d'un cours sur les groupes finis simples par J-P. Serre .Elle consiste des trois lemmes suivants. Les détails dans les démonstrations de ces lemmes sont laissés au lecteur.

Lemme 1 :

Soient p premier et G le groupe $GL(n, \frac{\mathbb{Z}}{p\mathbb{Z}})$. Soit H le sous-groupe de G qui a pour éléments les matrices de la forme

$$\begin{pmatrix} 1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & 1 \end{pmatrix}$$

(c'est à dire les matrices $(a_{i,j})$ telles que $a_{i,j} = 0$ si $i > j$ et $a_{i,i} = 1$). Alors H est un p-groupe de Sylow de G.

Démonstration.

On sait que comme p est premier, $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps et donc (voir les exercices) que $|G| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = p^{1+2+\cdots+n-1}(p^n-1)(p^{n-1}-1)\dots(p-1)$ donc $|G| = p^{n(n-1)/2}m$, avec m premier à p. On vérifera que H est un sous-groupe de G, et $|H| = p^{n(n-1)/2}$ (car pour la i^{eme} colonne de la matrice on a p^{i-1} choix) donc$H$ est un p-Sylow de G.

Lemme 2 :

Soit p premier et G un groupe fini d'ordre n. Alors G est isomorphe à un sous-groupe de $GL(n, K)$ où K est un corps.

Démonstration.

Faisos agir G sur G par translation donc $(g, h) \to gh$. Ceci induit un morphisme γ de G dans S_G et ce morphisme est injectif.

En effet $ker(\gamma) = \{g/\forall h \in H, gh = h\}$ donc si $g \in ker(\gamma), ge = g = e$. Donc par le premier théoréme d'isomorphisme G est isomorphe à un sous-groupe de S_n.

Montrons maintenant que S_n est isomorphe à un sous-groupe de $GL(n, K)$ où K est un corps fini.

A toute permutation σ de S_n associons la matrice mat(σ) définie par mat$(\sigma)_{i,j} = 1$ si $\sigma(i) = j$ et 0 sinon. On vérifie que $mat(\sigma)$ est un élément de $GL(n, K)$ car mat(σ) représente une application linéaire f deK^n dans K^n dans une base $(e_1 \dots e_n)$ telle que $f(e_i) = e_j$ si $\sigma(i) = j$. Donc f transforme une base en une base et par suite est bijective et $\{mat(\sigma)/\sigma \in S_n\}$ est un sous-groupe de $GL(n, K)$.

L'application de S_n dans $GL(n, K)$ qui à σ associe $mat(\sigma)$ est un morphisme injectif d'où la conclusion.

Lemme 3 :

Soient p premier, G un groupe fini, $H \subset G$ un sous-groupe et $S \subset G$ un p-Sylow de G. Alors il existe $a \in G$ tel que $H \cap aSa^{-1}$ est un p-groupe de Sylow dans H.

Démonstration.

Une remarque générale : Soit G un groupe et H un sous-groupe de G. Si on considére un conjugué de H donc un aHa^{-1} pour $a \in G$ alors en faisant opérer G sur $(\frac{G}{H})_g$ par translation le stabilisateur de aH est aHa^{-1}.

Comme il faut considérer les conjugués de S, on fait agir G sur $(\frac{G}{S})_g$ par translation.

Il existe une orbite dont le cardinal est non divisible par p car $|(\frac{G}{S})_g|$ = m est la somme des cardinaux des orbites. Soit aS un représentant d'une telle orbite, son stabilisateur $G_{aS} = aSa^{-1}$ est donc un p-groupe.

Par restriction de l'action de G sur $(\frac{G}{S})_g$ à Hon a $H \cap aSa^{-1} = H_{aS}$ et comme $|\frac{H}{H_{aS}}| = |HaS|$, H_{aS} est un p-Sylow de H.

Démonstration du Théoréme 2

Rappelons que si G est un p-groupe opérant sur un ensemble fini X alors $|Fix(G)| \equiv |X|$ (modulo p) si $Fix(G)$ est l'ensemble des points fixes.

Faisons donc opérer H sur $(\frac{G}{S})_g$ par translation. $|(\frac{G}{S})_g|$ et premier avec p et donc $Fix(G)$ n'est pas vide. Soit aS un point fixe. On a donc $HaS = aS$ soit le résultat .

Démonstration du Théoréme 3

Ceci est une conséquence du théoréme 2 car tout p-Sylow est un p-groupe et $|aSa^{-1}| = |S|$

Démonstration du Théoréme 4

Notons par $Syl(G)$ l'ensemble des p-Sylow de G. Cet ensemble n'est pas vide par les théorémes 1 et 3 on peut faire agir G sur $Syl(G)$ par conjuguaison.

Si S est un p-Sylow de G alors $|GS| = |Syl(G)|$ (Th3) et donc $|G| = |G_S||GS|$. Comme $S \subset G_S$ si $|G| = p^\alpha m$ et que $|S| = p^\alpha$ on a $|G_S| = kp^\alpha$. Donc s_p divise m.

Reste donc à démontrer la congruence. Pour l'instant admettons ce résultat.On verra la démonstration en fin de chapitre.

Corollaire des théorèmes de Sylow (théoréme de Cauchy)

Soit G un groupe fini et p un nombre premier divisant l'ordre de G alors G posséde un élément d'ordre p.

Preuve :
G posséde un p-Sylow d'ordre p^α donc il existe g de G d'ordre p^γ et $g^{p^{\gamma-1}}$ est d'ordre p

9.3. **Remarques utiles pour utiliser les théorèmes de Sylow.**

R1 : Si un groupe G posséde un seul p-Sylow celui-çi est distingué.

R2 : Un p-Sylow et un q-Sylow (p $\neq$q) ont une intersection réduite à $\{e\}$.

R3 : Si $|G| = p^\alpha m$ et $\alpha > 1$ on ne sait rien sur l'intersection des p-Sylow, mais par contre si $\alpha = 1$ alors l'intersection de deux p-Sylow est réduit à $\{e\}$

R4 : Si H et K sont deux sous-groupes distingués de G tels que
$$G = HK \text{ et } H \cap K = \{e\}$$
alors G est isomorphe au produit direct $H \times K$.
Remarquons que dans le cas fini la condition $G = HK$ peut etre remplaçée par $|G| = |H||K|$

9.4. **Quelques applications des théorèmes de Sylow.**

Apllication 1 :
Soit G un groupe tel que $|G| = 15$. Alors G est isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ donc à $\mathbb{Z}/15\mathbb{Z}$.

Démonstration :
Soit s_3 le nombre de 3-Sylow donc $s_3 \equiv 1 \pmod 3$ et divise 5 (théoréme 4) donc $s_3 = 1$ et par suite l'unique 3-Sylow, d'ordre 3, est distingu/'e (remarque 1) et isomorphe à $\dfrac{\mathbb{Z}}{3\mathbb{Z}}$. De même on a un unique 5-Sylow, distingué, isomophe à $\dfrac{\mathbb{Z}}{5\mathbb{Z}}$. Par la remarque 4 on conclue.

Application 2 :
Soit Gun groupe fini d'ordre pq où p et q sont deux premiers distincts tels que $q \not\equiv 1 \pmod p$. Alors G a un unique p-Sylow. On suppose de plus que $p \not\equiv 1 \pmod q$ montrer que alors G est cyclique.
Indication Si H (resp K) sont les uniques p-Sylow (resp q-Sylow) donc distingués, on conclue par la remarque 4 que G est isomorphe à $\dfrac{\mathbb{Z}}{pq\mathbb{Z}}$

Définition 9.4.1. Un groupe G est dit simple si ses seuls sous-groupes distingués sont $\{e\}$ et G.

Un exemple trivial de groupe simple sont les groupes $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ où p est premier. (Evidemment puisque un tel groupe n'a pas de sous-groupes propre). Un autre exemple sera détaillé dans le chapitre 8 à savoir A_n .

La classification de tous les groupes simples finis.(cf Atlas of finite simpe groupe) est connue depuis les années 60 mais il s'agit alors d'un problème difficile qui est hors de question pour un cours de licence. Ceci explique l'introduction de cette définition.

Application 3 :

Montrer que tout groupe G d'ordre 56 est non simple.

Preuve

comme 56 $=2^3 7$ le nombre s_2 de 2-Sylow est 1 ou 7 et le nombre s_7 de 7-Sylow est 1 ou 8. Supposons que $s_7 = 8$. Si H et $H^{'}$ sont deux 7-Sylow de G alors $H \cap H^{'} = \{e\}$. On a donc 8.6 $=48$ éléments d' ordre 7. Comme tout 2-Sylow contient 8 éléments et a une intersection trivial avec tout 7-Sylow on a alors $s_2 = 1$ et donc le 2-Sylow est distingué. Sinon $s_7 = 1$ et le 7-Sylow est distingué.

9.5. **Le cas d'un groupe abélien fini.**

Soit G un groupe abélien fini. Comme G est abélien tous ses p-Sylow sont distingués.

Proposition 9.5.1. *G est le produit direct de ses p-Sylow.*

Preuve :

Soit $|G| = p_1^{\alpha_1}...p_k^{\alpha_k}$, G étant abélien. Notons par $S_i 1 \leq i \leq k$ l'unique p_i-Sylow de G.

Considérons

$$f : \prod_{i=1}^{i=k} S_i \to G$$

définie par $f(h_1, ..., h_k) = \prod_{i=1}^{i=k} h_i$.

f est un morphisme car G est abélien. On a $S_i \cap S_j = \{e\}$ donc $|S_1 \times ... \times S_k| = |G|$. Il suffit donc de montrer que f est injective pour montrer que f est un isomorphisme.

Ker($f = \{(h_1, ..., h_k)/f(h_1, ..., h_k) = e\}$. Donc $(h_1, ..., h_k) \in$ Ker(f) si et seulement si $h_1^{-1} = h_2...h_k$. Or h_1 est d'ordre $p_1^{\beta_1}$ et $h_2...h_k$ est d'ordre $ppcm(p_2^{\beta_2}, ..., p_k^{\beta_k}$ (les p_i sont premiers entre eux et les h_i commutent entre eux). Donc la seule possibilité est $h_1 = e$. En continuant on Ker(f) $= \{e\}$.

Un exemple d'application : Trouver tous les groupes abéliens d'ordre 12.

Comme $12 = 2^2 3$ on a un 2-Sylow d'prdre 4 donc isomorphe à $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ ou $\frac{\mathbb{Z}}{4\mathbb{Z}}$ et un 3-Sylow d'orde 3 donc isomorphe à $\frac{\mathbb{Z}}{3\mathbb{Z}}$. Appliquant la proposition prédédente les groupes abéliens d'ordre 12 sont donc isomorphes à $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{6\mathbb{Z}}$ ou $\frac{\mathbb{Z}}{12\mathbb{Z}}$. On utilisera le théoréme chinois.

9.6. **Liste de tous les groupes finis simples d'ordre < 60.**

Remarquons d'abord que tout groupe d'ordre p (p premier) est simple. Nous allons éliminer au fur et à mesure les groupes d'ordre n non simples pour montrer qu'il ne reste que les groupes cycliques d'ordre p premier.

Lemme 9.6.1. *Tout groupe G d'ordre $p^\alpha, (\alpha > 1)$ est non simple.*

Preuve

Soit G est abélien alors G posséde un élément d'ordre p (Cauchy) donc le sous-groupe engendré par cet élément est distingué et n'est ni $\{e\}$ ni G, soit G n'est pas abélien donc $Z(G) \neq G$ et en faisant agir G sur G par conjuguaison on sait que $Z(G) \neq \{e\}$. Or $Z(G)$ est un sous-groupe distingué de G.

Lemme 9.6.2. *Tout groupe G d'ordre pq (p et q premiers distincts) est non simple.*

Preuve
Supposons p < q. Si s_p est le nombre de p-Sylow de G alors s_p =1 ou q et comme $s_p \equiv 1$ (mod p) on a $s_p = 1$ donc l'unique p-Sylow est distingué.

Lemme 9.6.3. *Tout groupe G d'odre p^2q (p et q premiers distincts) est non simple.*

Preuve
Supposons p < q. $s_q = 1, p$ ou p^2. Si $s_q \neq 1$ comme p < q on a s_q= p^2 donc $p^2(q-1)$ éléments d'ordre q et donc comme tout p-Sylow contient p^2 éléments $s_p = 1$ et le p-Sylow est distingué.
Si p > q alors $s_p = 1$ et donc le p-Sylow est distingué.

Ces trois résultats nous permettent d'éliminer un certain nombre de groupes . Reste les cas où $|G| \in \{30, 42, 54, 36, 24, 40, 48, 56\}$

Elimination des cas 30 42 54

Lemme 9.6.4. *Soit G un groupe d'ordre pair et S un 2-Sylow. Alors $|G| = k|S|$ avec k impair (faire agir S sur G par translation).*

Preuve
Remarquons que le résultat est ue conséquence du théoréme de Lagrange et du fait que S étant un 2-Sylow donc de cardinal 2^α si $|G| = 2^\alpha m$, avec 2 et m premiers entre eux, k est donc impair. Cependant en vue de la suite on a besoin d'une précision sur k.
Soit k le nombre d'orbites de l'action de S sur G par translation. $|G| = \sum_{1 \leq i \leq k} |Sg_i|$ si g_i est un représentant de la i^{eme} orbite. Or $|Gg_i| = |S|$. On retrouve donc $|G| = k|S|$.

Lemme 9.6.5. *Soit G un groupe d'ordre pair tel que $|G| > 2$ et possédant un 2-Sylow cyclique, S. Alors G n'est pas simple*

Preuve
On fait agir G sur G par translation et donc on a un morphisme $\gamma : G \to S_G$ qui composé avec la signature d'une permutation ϵ donne un morphisme de G dans $\{1, -1\}$. On va montrer que $ker(\epsilon \circ \gamma)$ est un sous-groupe propre de G.
$ker(\epsilon \circ \gamma) \neq \{e\}$ sinon par le premier théoréme d'isomorphisme G serait isomorphe à un sous groupe de $\{1, -1\}$ ce qui est impossible car $|G| > 2$. Reste donc à montrer que $ker(\epsilon \circ \gamma) \neq G$.
On a donc la situation suivante :

$$\epsilon \circ \gamma : G \to S_G \to \{1, -1\}$$

où $\gamma(g) = \gamma_g$ avec $\gamma_g(h) = gh$
Soit s un générateur de S. Examinons $\epsilon \circ \gamma(s)$. On a $\epsilon(\gamma_s)$ =-1 si γ_s est la permutation assoçiée à s par γ. En effet toute γ_s orbite c'est à dire $\{\gamma_s^k / k \in \mathbb{Z}\}$ est une orbite pour l'action de S sur G par translation donc si on a k orbites $\epsilon(\gamma_s) = (-1)^{(|G|-k)}$ et comme k est impair vu a) γ_s est une permutation impair.
On déduit que si G est un groupe d'ordre pair dont le cardinal n'est pas divisible par 4 alors G est non simple car G a un 2-Sylow qui est isomophe à $\frac{\mathbb{Z}}{2\mathbb{Z}}$ donc cyclique.
Remarquons que les cas n = 30 et 42 auraient pu se démontrer en utilisant le fait que ce sont des groupes d'ordre pqr, p,q,r premiers distincts. (cf les exercices).

Elimination des cas 24, 36, 48, 56
Le cas de 56 a déja été trité par l'application 3.

Lemme 9.6.6. *Tout groupe G d'ordre 24 est non simple.*

Preuve

$24 = 2^3 8$. Soit s_2 =1 ou 3. Si $s_2 = 1$ alors G est non simple. examinons le cas $s_2 = 3$. Faisons agir G sur l'ensemble des 2-Sylow par conjuguaison et donc considérons le morphisme γ associé de G dans S_3. Ce morphisme est non trivial sinon $\forall g \in G$ et $\forall S$ S un 2-Sylow $gSg^{-1} = S$ et donc S est distingué ce qui contredit le fait que $s_2 = 3$. De plus on ne peut pas avoir $ker(\gamma) = \{e\}$ sinon G d'ordre 24 serait isomorphe à un sous-groupe de S_3 qui es d'ordre 6. Donc $s_2 = 1$ et le 2-Sylow est distingué.

La même démonstration tient pour les cas 36 et 48.

Reste donc le cas des groupes d'ordre 40

$40 = 2^3 5$. Donc $s_5 = 1$ et par suite l'unique 5-Sylow est distingué.

Résumé :

Les seuls groupes simples d'ordre < 60 sont les groupes cycliques d'ordre p, p premier< 60.On verra par la suite que le groupe A_5 est simple. Hormis ce groupe toutes les démonstrations précédentes s'appliquent pour montrer que les seuls groupes simples d'ordre ≤ 100 et $\neq 60$ sont les groupes cycliques d'ordre p, p premier ≤ 100.

9.7. **Normalisateur et démonstration du théoréme 4.**

Définition 9.7.1. Soit S une partie non vide du groupe G. On appele normalisateur de S dans G, noté $N_G(S)$ l'ensemble $\{g \in G / gSg^{-1} = S\}$.

On vérifiera que $N_G(S)$ est un sous-groupe de G, et que si H est un sous-groupe de G alors H est un sous-groupe distingué de $N_G(H)$.

Proposition 9.7.1. *Soit H un sous-groupe de G et K un sous-groupe de $N_G(H)$. Alors HK est un sous-groupe de G.*

Preuve

Il suffit de montrer que $HK = KH$. Si K est un sous-groupe de $N_G(H)$ alors tout k de K vérifie $kHk^{-1} = H$ donc $\forall h \in H, \exists h' \in H$ tel que $khk^{-1} = h'$ donc $HK \subset KH$. De même $k^{-1} \in N_G(H)$ donc $k^{-1}Hk = H$ soit $KH \subset HK$.

Proposition 9.7.2. *Soit H et K deux sous-groupes de G. On suppose que K est d'ordre p^n (p premier) et $[G : H] = r$ (p ne divisant pas r). Alors K est contenu dans un conjugué de H.*

Preuve

On fait agir K sur $(\frac{G}{H})_g$ par translation. On sait que $|Fix(K)| \equiv r \pmod p$ et comme$p$ ne divise pas r,$|Fix(K)| \neq 0$Soit donc gH un point fixe, on a $\forall k \in K kgH = gH$ et donc $k \in gHg^{-1}$.

Proposition 9.7.3. *Soit G un groupe fini et S un p-Sylow de G. Alors S est l'unique p-Sylow de $N_G(S)$.*

Preuve

Remarquons que $S \subset N_G(S)$ donc un p-sous-groupe de $N_G(S)$ et même un p-Sylow de $N_G(S)$. Soit K un p-Sylow de $N_G(S)$, par la proposition précédente, $K \subset gSg^{-1}$ pour un $g \in G$ or $S \subset N_G(S)$ donc $K \subset gSg^{-1} = S$ et $|K| = |S|$ donc $K = S$.

Démonstration du théoréme 4

Soit $Syl(G) =$ { p-Sylow(G) }. On fait agir S sur $Syl(G)$ par conjuguaison. On a $|Fix(G| \equiv |Syl(G)|$ (modulo p). Soit donc S' un p-Sylow, $S' \in Fix(S)$ donc $\forall s \in S, S' = sS's^{-1}$ donc $S \subset N_G(S)$ et par la proposition précédente $S = S'$ soit $|Fix(S)| = 1$.

10. Simplicité du groupes A_5

Le but est de montrer que A_5 ne posséde pas de sous-groupes distingués.

Lemme 10.0.4. *: Les éléments de A_5 sont d'ordre 1,2,3 ou 5.*

Preuve

On a évidemment un élément d'ordre 1 à savoir l'idendité.

Examinons les éléments d'ordre 2 : Ce sont les permutations du type (a,b)(c,d)(e). En effet un élément d'ordre 2 est un produit pair de transpositions et les transpositions ne peuvent etre que des transpositions disjointes car (a,b)(b,c) - (a,b,c) donc un cycle d'ordre 3.

Le nombre d'éléments d'ordre 2 est donc $(C_5^2C_3^2)/2.= 15$. La division par 2 s'expliquant par le fait que la transposition (a,b) est aussi la transposition (b,a).

Examinons les éléments d'ordre 3 : Ce sont donc les cycles d'ordre 3 et leur nombre est $2C_5^3 = 20$.

Examinons les éléments d'ordre 5 : Ce sont donc les cycles d'ordre 5 et leur nombre est $4 \times 5 = 24$.

On a donc $1 + 15 + 20 + 24 = 60$ éléments soit $|A_5|$.

Lemme 10.0.5. *Les éléments d'ordre 2,3 ou 5 sont conjugués dans A_5.*

Preuve Pour les éléments d'ordre 2 :

Soit τ = (a,b)(c,d)(e) et $\tau' = (a',b')(c',d')(e')$ deux éléments d'ordre 2 de A_5.Alors si σ est tel que $\sigma(a) = a', \sigma(b) = b', \sigma(e) = e'$ et $\sigma(\{c,d\}) = \{c'd'\}$ alors $\sigma \in A_5$ et $\tau' = \sigma\tau\sigma^{-1}$.

Pour les éléments d'ordre 3 ou 5 :

Remarquons que $60 = 2^2 \times 3 \times 5$ donc que si σ est un élément d'ordre 3 (respectivement 5) alors le sous-groupe $< \sigma >$ est un 3- Sylow (respectivement 5-Sylow) de A_5. Or deux p-Sylow d'un groupe G sont conjugués d'ou le résultat.

Lemme 10.0.6. *Si H est un sous-groupe distingué dans A_5 $H \neq \{e\}$ alors $H = A_5$.*

Preuve

Tous les éléments, hormis l'élément neutre de H sont d'ordre 2,3 ou 5 et comme H est distingué si il contient une permutation , il contient aussi ses conjugués. Comme $|H|$ divise 60 H ne peut que contenir au moins des éléments d'ordre 2 et 3 ou 2 et 5 ou 3 et 5. Donc dans tous les cas, $|H| \geq 15 + 20 + 1 = 36$ ce qui est impossible. Donc $H = A_5$.

11. Groupes diédraux $\mathrm{D}_n (n \geq 3)$

Dans toute la suite on notera par P le plan affine euclidien muni de la distanced.

Définition 11.0.2 (définitions et prés requis)**.** On appelle isométrie de P toute application f : $P \to P$ qui conserve les distances. On montre que toute isométrie est une bijection et donc un élément de $S_P$et que l'ensemble des ces isométries est un sous-groupe de S_P noté Is(P). En particulier toute rotation et toute symétrie par rapport à une droite est une isométrie.

Soit $\mathcal{P}_n$ un polygone régulier de n sommets. On notera par D_n l'ensemble des isométries de P qui conservent globalement $\mathcal{P}_n$ donc qui conservent globalement les sommets. $\mathcal{P}_n$. D_n est un sous-groupe de Is(P). (Toutes les affirmations précedentes résultent du fait qu'une isométrie du plan est une application affine et donc conserve les barycentres).

Proposition 11.0.7. *Le groupe D_n est fini d'ordre 2n.*

Soit O le centre du polygone $\mathcal{P}_n$ et $A_1, \ldots, A_n$ ses sommets. Considérons dans le plan P le repère orthormé Oxy tel que A_1 soit sur Ox.En prenant comme unité de longueur le rayon du cercle circonscrit à $\mathcal{P}_n$, les sommets peuvent être considérés comme les images des racines n-imes de l'unité dans le plan complexe.

Preuve : Elle repose sur trois lemmes.

Lemme 11.0.8. *Notons par r_k la rotation de centre O et d'angle $\dfrac{2k\Pi}{n}$. Si $\Gamma_n = \{r_k / 0 \leq k \leq n-1$ alors Γ_n est un sous-groupe cyclique d'ordre n de D_n, isomorphe à U_n. Un générateur étant r_1.*

Lemme 11.0.9. *Notons par s la symétrie par rapport à Ox. Alors pour $0 \leq k \leq n-1$ $r_1^k \circ s$ sont tous distincts et éléments de D_n. De plus ils ne sont pas éléments de Γ_n. On en déduit que D_n contient au mois 2n éléments distincts.*

Lemme 11.0.10. *O, A_1, A_2 formant un repère affine, tout élément de D_n est uniquement déterminé par les images de A_1 et A_2 et par suite D_n contient exactement 2n éléments.*

On en déduit une description du groupe D_n par générateurs et relations à savoir

$$D_n = < r, s > \text{ où } r \text{ est d'ordre n, } s \text{ est d'ordre 2 et } rs = sr^{n-1}$$

Exercice 13. a) Tout groupe G engendré par deux éléments a et b tels que a soit d'ordre n, b d'ordre 2 et ab d'ordre 2 est isomorphe à D_n.

b) Le groupe D_{18} , groupe diédral d'ordre 36 est-il isomorphe à $S_3 \times S_3$?

c) Montrer que chaque 2-Sylow de S_4 est isomorphe à D_4.

12. Produit semi-direct

Ce chapitre donne une méthode de construction de nouveaux groupes à partir de groupes connus et permet aussi de ramener l'étude d'un groupe à l'étude de groupes plus petits.

Tous les groupes seront notés multiplicativement et l'élément neutre d'un groupe G par e_G.

12.1. **Préliminaires.**

Proposition 12.1.1. *Soit N et H deux groupes et α un morphisme de H dans $Aut(N)$. Alors le produit cartésien $N \times H$ est muni d'une structure de groupe pour la loi*

$$(n,h)(n^{'},h^{'}) = (n\alpha(h)(n^{'}), hh^{'})$$

Un tel groupe sera noté $N \rtimes_\alpha H$ et dit produit semi-direct de N par H.

Preuve

L'asssociativité se vérifie aisément.

L'élément neutre est (e_N, e_H).

L'inverse de (n,h) est $(\alpha(h^{-1})(n^{-1}), h^{-1})$.

Définition 12.1.1 (suites exactes et extension)**.**

Soit G, H, N trois groupes. On appelle suite exacte courte la donnée de deux applications i, r tels que i soit un morphisme injectif de N dans G et r un morphisme surjectif de G dans H vérifiant $\mathrm{Ker}(s) = \mathrm{Im}(i)$. Une telle donnée sera schématisée par :

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{r} H \longrightarrow 1$$

On dit alors que G est une extension de N par H.

On dira que la suite est scindée s' il existe un morphisme $s : H \to N$ tel que $r \circ s = Id$. Dans ce cas le morphisme s est appellé section de r. (Remarquons que s est injective)

Remarque 12.1. $i(N) = Im(i)$ est un sous-groupe distingué de G car noyau de r. D'autre part $\dfrac{G}{Im(i)}$ est isomorphe à H.

Lemme 12.1.2. *Soit N et H deux groupes et $N \rtimes_\alpha H$ un produit semi direct de N par H.*

Alors on a une suite exacte scindée

$$1 \longrightarrow N \xrightarrow{i} N \rtimes_\alpha H \xrightarrow{r} H \longrightarrow 1$$

.

Preuve

Il suffit de poser $i(n) = (n, e_H)$ et $r(n,h) = h$. On vérifie facilement que l'on obtient une suite exacte et en posant $s(h) = (e_N, h)$ que s est une section.

Proposition 12.1.3. *Soit la suite exacte courte :*

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{r} H \longrightarrow 1$$

Cette suite est scindée si et seulement si il existe un sous-groupe $H^{'}$ de G tel que $H^{'} \cap Im(i) = \{e_G\}$ et $Im(i)H^{'} = G$.

Preuve

a) Supposons que la suite soit scindée et soit s une section de r. Posons $H^{'} = s(H)$.

Si $g \in H^{'} \cap Im(i)$ alors il existe $h \in H$ tel que $g = s(h)$ et $Im(i) = Ker(r) impliquequer(g) = r(s(h)) = h = e_H$. Donc $g = s(e_H) = e_G$.

Montrons que $Im(i)H^{'} = G$. Soit $g \in G$, on doit montrer qu'il existe $n \in N$ et $h \in H$ tel que $g = i(n)s(h)$. Si tel est le cas on aura $r(g) = r(i(n))r(s(h)) = h$ car $Im(i) = Ker(r)$ et $r \circ s = Id$.

Donc $h = r(g)$, n sera donné par $i(n) = g(s(h)^{-1})$. Or $r(g(s(h)^{-1})) = e_G$ donc $g(s(h)^{-1})$ appartient à $Ker(r) = Im(i)$ d'où l'existence de n élément de N.

b) Montrons la réciproque.

Notons par $r' = r|_{H'}$ donc la restriction de r à $H^{'}$. Montrons que $r^{'}$ est un isomorphisme de $H^{'}$ sur H.

$r^{'}$ est injective car si $h^{'} \in H^{'}$ et $r^{'}(h^{'}) = e_G$ alors $h^{'} \in H^{'} \cap Ker(r) = Im(i)$ donc $h^{'} = e_G$.

$r^{'}$ est surjective car si $h \in H$, comme r est surjective, il existe $g \in G$ tel que $r(g) = h$.

Comme $Im(i)H^{'} = G$, il existe $n \in N$ et $h^{'} \in H^{'}$ tel que $g = i(n)h^{'}$. Donc $h = r^{'}(g) = r^{'}(i(n))r^{'}(h^{'}) = r^{'}(h^{'})$.

On a une section de r en considérant $s = j \circ r^{'}$ si j est l'injection canonique de $H^{'}$ dans G.

Proposition 12.1.4. *Soit la suite exacte scindée :*

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{r} H \longrightarrow 1$$

Si s est un section de r, tout élément g de G s'écrit de façon unique $g = i(n)s(h)$ où $n \in N$ et $h \in H$.

Preuve

Vu la proposition précédente si $H^{'} = s(H)$, $G = Im(i)s(H)$ d'ou l'écriture de $g = i(n)s(h)$. Cette écriture est unique car si $g = i(n_1)s(h_1) = i(n_2)s(h_2)$ alors $n_2^{-1}n_1 \in Im(i) \cap Ker(s) = e_G$ donc $n_1 = n_2$ et $h_1 = h_2$.

13. Produit semi-direct d'un sous-groupe distingué par un autre sous-groupe

Soit G un groupe et N un sous-groupe distingué de G tel que la suite exacte

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{r} \frac{G}{N} \longrightarrow 1$$

soit scindée.

Vu la proposition 1.1.3, considérons un sous-groupe H de G tel que $G = NH$ et $N \cap H = \{e_G\}$. On sait donc que tout élément de G s'écrit de fa çon unique $g = nh$ avec $n \in N$ et $h \in H$. Soit donc g_1 et g_2 deux éléments de G, g_1g_2 est donc de la forme $nh = n_1h_1n_2h_2$ que l'ont peut écrire sous la forme $n_1(h_1n_2h_1^{-1})h_1h_2$.

Ce qui montre que G est isomophe à $N \rtimes_\alpha H$ si α est le morphisme de Hdans $Aut(N)$ induit par l'action de H sur N par conjuguaison.

Résumons : Si on a une courte suite exacte scindée $1 \longrightarrow N \xrightarrow{i} G \xrightarrow{r} H \longrightarrow 1$ telle que $i(N)$ soit distingué dans G alors G est isomorphe à i$i(N) \rtimes_\alpha H$ avec $\alpha : s(H) \to Aut(i(N))$ donnée par $s(h)(n) = hnh^{-1}$ (s étant la section de r).

13.1. **Exemples.**

Exemple 13.1.1 (le groupe diédral D_n $n \geq 3$)**.**

Rappelons que D_n est le groupe des isom/'etries d'un polygone régulier de n cotés (cf le chapitre sur les groupes diédraux). Ce groupe,d'ordre 2n,est engendr/'e par r et s où r est un élément d'ordre n, s un élément d'ordre 2 et $rs = sr^{n-1}$.

Soit $N =< r >$. Ce sous-groupe est distingué car d'indice 2. Si $H =< s >$ on vérifie aisément que $D_n = NH$ et que $N \cap H = e$. Donc $D_n = N \rtimes_\alpha H$ où $\alpha :< s > \to Aut(< r >)$ est définie par $\alpha(s) : r \to srs^{-1}$.

Comme $< r >$ est isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ et que $< s >$ est isomorphe à $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$, D_n est isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \rtimes_\beta \dfrac{\mathbb{Z}}{2\mathbb{Z}}$ où $\beta : \dfrac{\mathbb{Z}}{2\mathbb{Z}} \to Aut(\dfrac{\mathbb{Z}}{n\mathbb{Z}})$. β est d efinie par $\beta(\bar{1}) : \bar{a} \to -\bar{a}$.

Exemple 13.1.2 (le groupe,G, des isométries de $\mathbb{R}^n, n \geq 1$)**.** On sait que les éléments de ce groupe sont les $t_{\overrightarrow{u}} \circ \overrightarrow{f}$ où $t_{\overrightarrow{u}}$ est une translation de vecteur $\overrightarrow{u}$ et $\overrightarrow{f}$ un élément du groupe $H = O(n, \mathbb{R})$.

Soit N le sous-groupe de G des translations.Ce sous-groupe est distingué car si $h \in H$ alors $ht_{\overrightarrow{u}}h^{-1} = t_{\overrightarrow{h(u)}}$. Que $G = NH$ résulte de la forme des éléments de G. Enfin $N \cap H = \{e_G\}$ car les éléments de l'intersection sont les translations qui fixent l'origine.

Vu la proposition 1.1.4, G est isomorphe à $\mathbb{R}^n \rtimes_\beta O(n, \mathbb{R})$ où β est donné par $\beta(A)(x) = A(x)$.(cf l'exercice 4.0.9 ci dessous)

13.2. **Exercices.** Un rappel qui servira : Se donner un morphisme $\alpha : \frac{\mathbb{Z}}{n\mathbb{Z}} \to Aut(\frac{\mathbb{Z}}{m\mathbb{Z}})$ est équivalent à se donner a de $\frac{\mathbb{Z}}{m\mathbb{Z}}$ tel que pgcd(a,m) =1 et $a^n \equiv 1 \pmod m$.

Exercice 14. Construire un groupe d'ordre 21 non commutatif.(penser à Sylow pour trouver un sous-groupe distingué).

Exercice 15. Expliciter les produits semi-direct $\frac{\mathbb{Z}}{2\mathbb{Z}} \rtimes_\alpha \frac{\mathbb{Z}}{4\mathbb{Z}}$ et $\frac{\mathbb{Z}}{4\mathbb{Z}} \rtimes_\alpha \frac{\mathbb{Z}}{2\mathbb{Z}}$.

Dans le cas $\frac{\mathbb{Z}}{4\mathbb{Z}} \rtimes_\alpha \frac{\mathbb{Z}}{2\mathbb{Z}}$ montrer que le groupe non commutatif est isomorphe à D_4 (on pourra examiner l'ordre des éléments)

Exercice 16. Montrer qu'il existe deux groupes d'ordre $4\times$ 13 non isomorphes.

Indication : Considérer $\frac{\mathbb{Z}}{13\mathbb{Z}} \rtimes_\alpha \frac{\mathbb{Z}}{4\mathbb{Z}}$ pour des α convenables et l'ordre de l'élément $(\bar{1}, \bar{2})$.

Exercice 17. Montrer que le groupe S_n est isomorphe à $A_n \rtimes_\alpha \frac{\mathbb{Z}}{2\mathbb{Z}}$.

Exercice 18. Montrer que le groupe $GL(n, \mathbb{R})$ est isomorphe à $SL(n, \mathbb{R}) \rtimes_\alpha \mathbb{R}^*$ pour un certain α.

Exercice 19. Soit N et H deux groupes et $\alpha : H \to Aut(N)$ un morphisme.

Montrer que si σ est un automorphisme de H et $\beta = \alpha \circ \sigma$ alors $N \rtimes_\beta H$ est isomorphe à $N \rtimes_\alpha H$.

Exercice 20. Montrer qu'un produit semi-direct $N \rtimes_\alpha H$ est commutatif si et seulement si le produit est direct et N, H sont abéliens.

Exercice 21. Soit p et q deux entiers premiers (p < q) et G un groupe d'ordre pq.

a) Montrer qu'il existe un unique q-Sylow N dans G,et donc que$N$ est distingué.

b) Soit H un p-Sylow dans G. Montrer que G est isomorphe à $N \rtimes_\alpha H$, où $\alpha : H \to Aut(N)$ est l'opération de conjuguaison.

c) On suppose que p divise $q - 1$. Montrer, qu'à isomorphisme près, il y a exactement deux groupes d'ordre pq.

Indication : On rappelle que le groupe $Aut(\frac{\mathbb{Z}}{n\mathbb{Z}})$ est isomorphe au groupe $(\frac{\mathbb{Z}}{n\mathbb{Z}})^\times$(croupe des éléments inversibles de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ pour la multiplication).

Exercice 22. Soit K un corps et n un entier positif.

a) Montrer que la suite exacte courte $1 \longrightarrow Sl(n, K) \xrightarrow{i} GL(n, K) \xrightarrow{det} K^* \longrightarrow 1$ est scindée.

b) On suppose que n est impair. Montrer que $Gl(n, \mathbb{R})$ est isomorphe à $Sl(n, \mathbb{R}) \times \mathbb{R}^*$.

c) Déduire de la question précédente, q'un produit semi-direct $N \rtimes \alpha H$ avec un α non trivial peut peut être isomorphe au produit direct $N \times H$.