http ://perso.wanadoo.fr/cyd60000
theoriedesgroupes@orange.fr

THEORIE DES GROUPES

Table des matières

Chapitre 1

Notions de base

Structure de groupe

Sous-groupes

Homomorphismes de groupes

Produit direct de groupes

1.1 Structure de groupe

1.1.1 Loi interne

Soit E un ensemble non vide.

Définitions *On appelle loi (de composition) interne sur E, une application de $E\times E$ dans E. Si f est une loi interne, le couple (E,f) est appelé magma.*

Notations *Par abus de language et d'écriture, quand il n'y pas de risque de confusion sur la loi interne f, le terme magma désignera l'ensemble E.*
Les lois internes sont notées en général . ou +.
Si on prend ., on parlera de notation multiplicative et, pour tous les x et y appartenant à E, on notera xy (ou x.y) plutôt que .(x,y). Si on prend +, on parlera de notation additive et, pour tous les x et y appartenant à E, on notera x+y plutôt que +(x,y) .

Définition *Soit . une loi interne sur E.*
Une partie A de E est stable par . si, pour tous les x et y appartenant à E, $xy\in A$.

Remarque *Si $A\subseteq E$ est stable par ., la restriction de . à $A\times A$ est une application de $A\times A$ dans A c'est à dire une loi interne sur A.*
On appelle alors cette loi, la loi induite par . sur A.

1.1.2 Groupes

Soit (E,.) un magma.

Définitions *On dit que . est associative si, pour tous les x, y et z appartenant à E, (xy)z=x(yz).*
On dit que . admet un élément neutre si, il existe un élément e de E tel que, pour tout x de E, xe=ex=x.
Si . est associative et possède un élément neutre, on dit que (E,.) est un monoïde.
On dit que la loi . est commutative, si pour tous les x et y appartenant à E, xy=yx.
Soit x appartenant à E. Si . admet un élément neutre e, on dit que x est inversible (pour .) si il existe y appartenant à E tel que xy=yx=e. y est alors appelé inverse de x.

Remarque *En notation additive, un élément neutre e de + vérifie : e+x=x+e=x pour tout x de E et, si x appartient à E, un inverse y de x vérifie x+y=y+x=e.*

Proposition 1.1.1 *1)Si . admet un élément neutre, alors celui-ci est unique.*
On suppose . associative.
2)Si x∈E est inversible alors x a un unique inverse.
3)Si x∈E est inversible alors son inverse y est inversible et l'inverse de y est x.

Démonstration *1)Soit e un élément neutre de E.*
Supposons qu'il existe e' appartenant à E tel que, pour tout x de E, xe'=e'x=x.
Alors, comme e appartient à E, on a ee'=e.
Mais, comme e est un élément neutre de E, ee'=e'. D'où e=e'.
2)Soient e l'élément neutre de E et y un inverse de x.
Supposons qu'il existe z appartenant à E tel que xz=zx=1.
Alors, comme . est associative,

$$\begin{aligned} y &= ye \\ &= y(xz) \\ &= (yx)z \\ &= ez \\ &= z. \end{aligned}$$

3)yx=xy=1 donc y est inversible d'inverse x. ♢

Définition *En notation multiplicative, l'élément neutre de . est noté 1 et si x est un élément de E, son inverse est noté* x^{-1}.
En notation additive, l'élément neutre de + est noté 0 et si x est un élément de E, son inverse est appelé opposé de x et est noté -x.

Proposition 1.1.2 *Si* $x_1, \ldots, x_n$ *sont des éléments inversibles de E alors* $x_1 \ldots x_n$ *est inversible d'inverse* ${x_n}^{-1} \ldots {x_1}^{-1}$.

Démonstration *Comme . est associative,*

$$\begin{aligned} (x_1 \ldots x_n)({x_n}^{-1} \ldots {x_1}^{-1}) &= (x_1 \ldots x_{n-1})(x_n{x_n}^{-1})({x_{n-1}}^{-1} \ldots {x_1}^{-1}) \\ &= (x_1 \ldots x_{n-1})1({x_{n-1}}^{-1} \ldots {x_1}^{-1}) \\ &= (x_1 \ldots x_{n-1})({x_{n-1}}^{-1} \ldots {x_1}^{-1}) \\ &\ldots \\ &= x_1{x_1}^{-1} \\ &= 1. \end{aligned}$$

De même, on a $({x_n}^{-1} \ldots {x_1}^{-1})(x_1 \ldots x_n)=1$.
D'où $(x_1 \ldots x_n)^{-1} = {x_n}^{-1} \ldots {x_1}^{-1}$. ♢

Notations *Soit x appartenant à E et n un entier.*
En notation multiplicative, on pose x^0=1 et si n est strictement positif, on note x^n à la place de x ... x (n fois) et x^{-n} au lieu de x^{-1} ... x^{-1} (n fois).
En notation additive, on pose 0x=0 et, si n est strictement positif, on note nx à la place de x+ ... +x (n fois) et -nx au lieu de (-x)+ ... +(-x) (n fois).

Définitions *Un monoïde (G,.) est appelé groupe si tous les éléments de G sont inversibles.*
Autrement dit, (G,.) est un groupe si . est une loi interne sur G, associative, possédant un élément neutre et telle que tout élément de G est inversible.
Si on utilise la notation multiplicative (respectivement additive), on dit que (G,.) est un groupe multiplicatif (respactivement additif).
Si . est commutative, on dit que (G,.) est un groupe abélien (ou commutatif).

Notation *Par abus d'écriture, le terme de groupe désignera l'ensemble G au lieu du couple (G,.) (si il n'y a pas de risque de confusion sur la loi).*

Proposition 1.1.3 *La correspondance σ d'un groupe G vers G, définie par $\sigma(g)=g^{-1}$, est une application bijective.*

Démonstration *Tout élément g de G possède une inverse et celle-ci est unique d'après la Proposition 1.1.1, donc σ est une application.*
D'après la Proposition 1.1.1, pour tout g de G, $g=(g^{-1})^{-1}$ donc σ est surjective.
Si g et g' sont deux éléments de G tels que $g^{-1}=g'^{-1}$ alors, σ étant une application, $(g^{-1})^{-1}=(g'^{-1})^{-1}$ c'est à dire g=g'. D'où, σ est injective.
σ est donc bijective. $\diamondsuit$

Exemples *1)$(\mathbb{N},+)$ et $(\mathbb{Z},\times)$ sont des monoïdes.*
2)$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes (additifs) abéliens.
3)$(\mathbb{Q}-\{0\},\times)$, $(\mathbb{R}-\{0\},\times)$ et $(\mathbb{C}-\{0\},\times)$ sont des groupes (multiplicatifs) abéliens.
4)Soit E et F deux ensembles.
Alors $(\{f : E \to F\},+)$ est un groupe abélien.
5)Soit E un ensemble.
Alors $(\{f : E \to E\},\circ)$ est un groupe non abélien en général.

Définition *On dit qu'un groupe G est fini si l'ensemble G est fini.*
Dans ce cas, le cardinal de G est appelé ordre de G et noté $|G|$.

Notation *Dans la suite (sauf mention contraire), on utilisera la notation multiplicative.*

1.2 Sous-groupes

1.2.1 Définition

Soit G un groupe.

Définition *Une partie H non vide de G est un sous-groupe de G si :*
1)Pour tout couple (h,h') d'éléments de H, hh' appartient à H,
2)Pour tout h appartenant à H, h^{-1} appartient à H.

Exemples *G et $\{1\}$ sont des sous-groupes de G appelés sous-groupes triviaux de G.*

Définition *Soit H un sous-groupe de G.*
Si H est différent de G et $\{1\}$, on dit que H est un sous-groupe propre de G.

1.2.2 Propriétés

Soit G un groupe.

Propriété 1.2.1 *Soit H un sous-groupe de G. Alors,*
1)1 appartient à H.
2)H est un groupe pour la loi induite sur H par G .

Démonstration *1)Soit h appartenant à H. Alors, h^{-1} appartient à H et donc $hh^{-1}=1$ appartient à H.*
2). est associative sur $G\times G$ donc sur $H\times H$.
D'après le 1), la restriction de . à $H\times H$ admet un élément neutre.
Comme H est un sous-groupe, tout élément de H admet un inverse dans H, pour la restriction de . à $H\times H$.
D'où, H est un groupe pour . restreinte à $H\times H$. $\diamondsuit$

Proposition 1.2.2 *Une partie non vide H de G est un sous-groupe de G si et seulement si pour tout couple (h,h') d'éléments de H, hh'^{-1} appartient à H.*

Démonstration *($\Rightarrow$) Découle de la définition d'un sous-groupe.*
($\Leftarrow$) Pour tout couple (h,h') d'éléments de H, hh'^{-1} appartient à H.
D'où, en prenant h=1, appartenant à H d'après la Propriété précédente, $1h'^{-1}=h'^{-1}$ appartient à H pour tout h' dans H.
Donc, pour tout couple (h,h') d'éléments de H, $h(h'^{-1})^{-1}=hh'$ appartient à H. $\diamondsuit$

Proposition 1.2.3 *Soient H et K deux sous-groupes de G d'intersection non vide. Alors, $H\cap K$ est un sous-groupe de G.*

Démonstration *H∩K n'est pas vide car 0 appartient à H∩K.*
Soient x et y appartenant à H∩K.
Comme H et K sont des sous-groupes de G, xy^{-1} appartient à H et à K donc à H∩K.
D'où, H∩K est un sous-groupe de G. ♢

Remarques *1)Cette Proposition s'étend au cas d'une famille quelconque de sous-groupes de G, d'intersection non vide.*
2)H∪K n'est pas en général un sous-groupe de G.
Par exemple, soient H la droite d'équation (y=0) et K la droite d'équation (x=0) dans $\mathbb{R}^2$, groupe additif.
Alors H et K sont des sous-groupes de ($\mathbb{R}^2$,+) mais pas H∪K car (1,0)+(0,1)=(1,1) n'appartient pas à H∪K.

1.2.3 Sous-groupe engendré

Soit G un groupe.

Définition *Soit A une partie non vide de G.*
Alors, on appelle sous-groupe engendré par A et on note <A>, le plus petit sous-groupe (au sens de l'inclusion) de G contenant A.
Si g appartient à G, on note <g> à la place de <{g}>.

Exemples *<∅>={1}, <G>=G et <1>={1}.*

Proposition 1.2.4 *<A> est l'intersection des sous-groupes de G contenant A.*

Démonstration *Soit M=∩K où l'intersection porte sur les sous-groupes K de G contenant A. D'après la Proposition 1.2.3, M est un sous-groupe de G.*
De plus, M contient A.
Soit N un sous-groupe de G contenant A.
Alors, N fait partie de l'ensemble des sous-groupes sur lequel porte l'intersection définissant M. D'où, M étant inclus dans tout sous-groupe de G contenant A, M est inclus dans N.
Par conséquent, M est le plus petit sous-groupe de G contenant A c'est à dire <A>.
♢

Proposition 1.2.5 *Pour toute partie non vide A de G,*
<A>=$\{g_1 \ldots g_n \ / \ n \in \mathbb{N}, \forall 1 \leq i \leq n \ g_i \in A \ \ ou \ \ {g_i}^{-1} \in A\}$.

Démonstration *Montrons que* $H=\{g_1 \ldots g_n \ / \ n \in \mathbb{N}, \forall 1 \leq i \leq n \ g_i \in A \ \text{ ou } {g_i}^{-1} \in A\}$ *est un sous-groupe de G contenant A.*
Soit a appartenant à A (A non vide).
Alors, a appartient à H (n=1) et par conséquent, H est non vide et contient A.
Soient $x=g_1 \ldots g_n$ *et* $y=g'_1 \ldots g'_m$ *appartenant à H. Alors,* $xy^{-1}=g_1 \ldots g_n \ {g'_m}^{-1} \ldots {g'_1}^{-1}$ *appartient à H car, pour tous les i compris entre 1 et n et j compris entre 1 et m,* g_i *ou* ${g_i}^{-1}$ *et* g'_j *ou* ${g'_j}^{-1}$ *appartient à A.*
D'où H est un sous-groupe de G contenant A. Par suite, $<A>$ *étant le plus petit sous-groupe de G contenant A,* $<A>$ *est inclus dans H.*
Montrons l'autre inclusion : soit $x=g_1 \ldots g_n$ *appartenant à H.*
Soit i compris entre 1 et n. Si g_i *appartient à A alors* g_i *appartient à* $<A>$ *puisque* $<A>$ *contient A. Si* ${g_i}^{-1}$ *appartient à A alors* ${g_i}^{-1}$ *appartient à* $<A>$. *Mais* $<A>$ *est un sous-groupe de G, donc* $({g_i}^{-1})^{-1} = g_i$ *appartient aussi à* $<A>$. *D'où, pour tout i compris entre 1 et n,* g_i *appartient à* $<A>$. *Comme* $<A>$ *est un sous-groupe de G, on en déduit que* $x=g_1 \ldots g_n$ *appartient à H. H est inclus dans* $<A>$. $<A>=H$. $\diamondsuit$

Corollaire 1.2.6 *Soit g appartenant à G. Alors,* $<g>=\{g^m \ / \ m \in \mathbb{Z}\}$.

Démonstration *On rappelle que, pour tout entier* $m<0$, *on note* g^m *a la place de* $(g^{-1})^n$ *où* $n=-m$.
D'après la Proposition précédente, les éléments de $<g>$ *sont de la forme* $g_1 \ldots g_n$ *avec* $g_i=g$ *ou* ${g_i}^{-1}=g$ *pour tout i compris entre 1 et n. Donc, en simplifiant tant que c'est possible les g avec les* g^{-1}, *les éléments de* $<g>$ *sont de la forme* g^m, m *dans* $\mathbb{Z}$. $\diamondsuit$

1.2.4 Ordre d'un élément dans un groupe fini

Soit G un groupe non réduit à l'élément neutre.

Définition *Soit g appartenant à G.*
Si le sous-groupe $<g>$ *est fini, on appelle <u>ordre</u> de g et on note o(g), l'ordre de* $<g>$.

Remarque $o(g)=1$ *si et seulement si* $g=1$.

Proposition 1.2.7 *Soit g un élément de G distinct de 1 et d'ordre fini.*
Alors, $<g>=\{g^n \ / \ 1 \leq n < o(g)\}$.

Démonstration *D'après le Corollaire 1.2.6,* $<g>=\{g^m \ / \ m \in \mathbb{Z}\}$.
Comme $<g>$ *est fini, il existe un entier strictement positif a tel que* $g^a = 1$.
On pose k : le plus petit entier strictement positif a tel que $g^a = 1$.
Pour tout entier m, il existe, par division euclidienne, un couple (i,n) d'entiers avec $0 \leq n < k$ *tel que* $m=ik+n$.

D'où,

$$\begin{aligned} g^m &= g^{ik+n} \\ &= g^{ik}g^n \\ &= g^{ki}g^n \\ &= (g^k)^i g^n \\ &= 1^i g^n \\ &= 1g^n \\ &= g^n. \end{aligned}$$

On en déduit que <g>=$\{g^n$ / $1 \leq n < k\}$.
Il reste à montrer que k=o(g). <g> est de cardinal o(g) par définition de o(g).
Si 1≤i<j<k sont tels que $g^i = g^j$ alors $g^j(g^i)^{-1} = g^{j-i}$=1.
D'où, comme j-i>0, on a, par hypothèse sur k, j-i≥k.
Mais j<k donc j-i<k. Contradiction.
D'où, si 1≤i<j<k, $g^i \neq g^j$.
On en déduit que <g>=$\{g^n$ / $1 \leq n < k\}$ est de cardinal k et donc k=o(g). ♢

Dans la démonstration précédente, on a prouvé la proposition suivante :

Proposition 1.2.8 *Soit g un élément d'ordre fini du groupe G.*
Alors, l'ordre de g est le plus petit entier strictement positif k tel que g^k=1.

Remarques *1)Un groupe infini peut avoir des éléments d'ordre fini.*
Par exemple, -1 est d'ordre 2 dans $(\mathbb{R}, \times)$.
2)On démontre de la même façon, en notation additive, que si g est distinct de 0 et d'ordre fini alors <g>=$\{ng$ / $1 \leq n < o(g)\}$ et o(g) est le plus petit entier strictement positif k tel que kg=0 (propriété vérifiée également par 0).

Le résultat suivant est très important :

Proposition 1.2.9 *Soient G un groupe, g un élément de G d'ordre fini et n un entier strictement positif tel que g^n=1.*
Alors, l'ordre de g divise n.

Démonstration *On pose x=o(g). Par division euclidienne, il existe deux entiers a et b tels que n=ax+b avec 0≤b<x.*
D'où, $1=g^n = g^{ax+b} = g^{ax}g^b = (g^x)^a g^b = g^b$.
Si b n'est pas nul, b contredit la Proposition 1.2.8.
D'où, b=0 et o(x) divise n. ♢

1.2.5 Sous-groupes de $\mathbb{Z}$ et sous-groupes de $\mathbb{R}$

On utilise la notation additive.

Propriété 1.2.10 *$\mathbb{Z}$=<1>*

Démonstration *Par propriété de construction de $\mathbb{N}$ (axiomes de Peano), $\mathbb{Z}$ vérifie la définition de <1> du Corollaire 1.2.6, avec les notations de la remarque précédente.* ♢

Proposition 1.2.11 *Tout sous-groupe de $\mathbb{Z}$ est de la forme <n> où n est un entier positif.*

Démonstration *Soit H un sous-groupe de $\mathbb{Z}$ distinct de $\mathbb{Z}$.*
Si H=0 alors H=<0>.
Si H=$\mathbb{Z}$, H=<1>
On suppose que H est un sous-groupe propre de $\mathbb{Z}$. Soit n le plus petit élément strictement positif de H.
Montrons que <n>=H : n appartient à H sous-groupe de $\mathbb{Z}$ donc <n> est inclus dans H (<n> plus petit sous-groupe de $\mathbb{Z}$ contenant n).
Montrons que H est inclus dans <n> : soit x appartenant à H.
D'après la division euclidienne, il existe un couple d'entiers (i,j) avec 0≤j<n tel que x=in+j. Si i est positif, in=n+ ... +n appartient à H car n appartient à H et H sous-groupe de $\mathbb{Z}$.
Si i est négatif, in=(-n)+ ... +(-n) appartient à H car n appartient à H et H sous-groupe de $\mathbb{Z}$.
Comme x appartient à H sous-groupe de $\mathbb{Z}$, j=x-in appartient à H.
Or j est positif et strictement inférieur à n et n est le plus petit entier strictement positif appartenant à H donc j=0.
D'où, x=in et x appartient donc à <n>.
H est inclus dans <n>. H=<n>. ♢

Notation *<n> est noté n$\mathbb{Z}$.*

Explicitons maintenant les sous-groupes de ($\mathbb{R}$,+) :

Proposition 1.2.12 *Soit H un sous-groupe de ($\mathbb{R}$,+). Alors,*
1)Ou H est de la forme x$\mathbb{Z}$ avec x réel positif,
2)Ou H est dense dans $\mathbb{R}$ c'est à dire pour tous les réels x<y, H$\cap]x,y[$ n'est pas vide.

Démonstration *Si H=$\{0\}$, alors H=0$\mathbb{Z}$.*
Supposons que H est différent de $\{0\}$.
On pose $H^+ = \{h \in H \ / \ h>0 \}$.

Comme H n'est pas réduit à $\{0\}$, il existe h appartenant à H avec $h \neq 0$.
Si $h>0$ alors h appartient à H^+.
Si $h<0$ alors, comme H est un sous-groupe de $(\mathbb{R},+)$, $-h>0$ et donc -h appartient à H^+. D'où H^+ est non vide.
On considére $m=Inf_{h\in H^+}\ h$.
Montrons que si $m=0$, $H=m\mathbb{Z}$:
Montrons d'abord, par l'absurde, que m appartient à H^+ :
Supposons que m n'appartient pas à H^+.
Par définition de la borne inférieure, il existe un réel h appartenant à H^+ tel que $m<h<2m$. De même, il existe un élément h' de H^+ tel que $m<h'<h$.
On pose $g=h-h'$. Comme H est un sous-groupe de $(\mathbb{R},+)$, g appartient à H et comme g est strictement positif, g appartient à H^+.
Mais comme $h<2m$ et $-h'<-m$, on a $g=h-h'<m$ ce qui contredit la définition de m.
D'où, m appartient à H^+.
Donc, comme H est un sous-groupe de $(\mathbb{R},+)$, $m\mathbb{Z}$ est inclus dans H.
Montrons l'autre inclusion : soit h appartenant à H.
On pose $g=E(\frac{h}{m})\in \mathbb{Z}$ où E désigne la partie entière ($m>0$).
m étant strictement positif, on a, par définition de la partie entière, $mg\leq h<m(g+1)$.
D'où $0\leq h-mg<m$.
Montrons que $h-mg=0$:
Si $h-mg>0$ alors, comme h et m appartiennent à H, h-mg appartient à H^+.
Or, $h-mg<m$ ce qui contredit la définition de m, donc $h-mg=0$ c'est à dire $h=mg\in \mathbb{Z}$.
H est inclus dans $m\mathbb{Z}$ d'où $H=m\mathbb{Z}$.
Il reste à étudier le cas où $m=0$: Soient x et y deux réels tels que $x<y$.
Par définition de la borne inférieure, il existe un élément h de H^+ tel que $0<h<y-x$.
On pose $n=E(\frac{x}{h})\in \mathbb{Z}$. On a alors, puisque $h>0$, $hn\leq x<h(n+1)=hn+h$ par définition de la partie entière. $h<y-x$ et $hn\leq x$ donc $x<hn+h\leq x+h<y$.
On pose $g=h(n+1)$. On a $x<g<y$ donc $g\in]x,y[$.
Comme $n+1\in \mathbb{Z}$ et comme H est un sous-groupe de $(\mathbb{R},+)$, g appartient à H.
D'où g appartient à $H\cap]x,y[$ et par conséquent $H\cap]x,y[$ n'est pas vide. $\diamondsuit$

Corollaire 1.2.13 *$\mathbb{Q}$ est dense dans $\mathbb{R}$.*

Démonstration *$\mathbb{Q}$ est un sous-groupe de $(\mathbb{R},+)$ puisque $\mathbb{Q}$ n'est pas vide et si $\frac{a}{b}$ et $\frac{c}{d}$ sont des éléments de $\mathbb{Q}$ ($a,c\in \mathbb{Z}$, $b,d\in \mathbb{N}-\{0\}$), $\frac{a}{b}-\frac{c}{d}=\frac{ad-cb}{bd}$ appartient à $\mathbb{Q}$.*
Il suffit donc de montrer, d'après la Proposition précédente, que $\mathbb{Q}$ ne s'écrit pas sous la forme $x\mathbb{Z}$ où x est un réel positif.
Supposons que $\mathbb{Q}=x\mathbb{Z}$ avec x réel positif.
Comme $\mathbb{Q}$ n'est pas réduit à $\{0\}$, x n'est pas nul.
$\frac{1}{2}$ appartient à $\mathbb{Q}$ donc, il existe un entier non nul n tel que $\frac{1}{2}=xn$ c'est à dire $x=\frac{1}{2n}$.
D'où, $\mathbb{Q}=\frac{1}{2n}\mathbb{Z}=\{\frac{m}{2n}\ /\ m\in \mathbb{Z}\}$.
Soit p un nombre premier distinct de 2 et ne divisant pas n. Alors, p ne divise pas 2n et donc il n'existe pas d'entier m tel que $mp=2n$.
D'où, $\frac{1}{p}$ ne peut s'écrire sous la forme $\frac{m}{2n}$ avec m entier, bien que ce soit un élément de $\mathbb{Q}$. Contradiction.
$\mathbb{Q}$ ne s'écrit pas sous la forme $x\mathbb{Z}$, avec x réel positif, donc, d'après la Proposition précédente, $\mathbb{Q}$ est dense dans $\mathbb{R}$. $\diamondsuit$

1.3 Homomorphismes de groupes

Nous allons étudier les applications qui conservent la structure de groupe.

1.3.1 Définition

Soient G et G' deux groupes.

Définition *Une application f : G → G' est un homomorphisme de groupes si pour tous les les x et y de G f(xy)=f(x)f(y).*
L'ensemble des homomorphismes de G dans G' est noté Hom(G,G').

Exemple *L'application f de $(\mathbb{Z},+)$ dans $(\mathbb{R},\times)$ définie par $f(n)=2^n$ est un homomorphisme de groupes.*

Propriété 1.3.1 *Soit f : G → G' un homomorphisme de groupes.*
Alors, 1)$f(1_G)=1_{G'}$.
2)Pour tout élément x de G, $f(x^{-1})=f(x)^{-1}$.
3)Pour tout entier non nul n, $f(x^n)=f(x)^n$ et, si on définit x^{-n} par $(x^n)^{-1}$, $f(x^{-n})=f(x)^{-n}$.

Démonstration *1)f(1)=f(1.1)=f(1)f(1). D'où, f(1) étant inversible dans G' car G' est un groupe, f(1)=1.*
2)$f(x)f(x^{-1})=f(xx^{-1})=f(1)=1=f(x^{-1})f(x)$ donc $f(x^{-1})=f(x)^{-1}$.
3)Pour $f(x^n)$ on procède par récurrence, et pour $f(x^{-n})$ on utilise la Propriété 2 et le cas n positif. ♢

Proposition 1.3.2 *Soient H un groupe, et f : G → G' et g : G' → H des homomorphismes de groupes.*
Alors, g∘f : G → H est un homomorphisme de groupes.

1.3.2 Noyau et image d'un morphisme

Soient G et G' deux groupes et f : G → G' un homomorphisme de groupes.

Définitions *On appelle noyau de f, et on note Ker f, l'ensemble $\{x\in G \ / \ f(x)=1\}$.*
On appelle image de f, et on note Im f, l'ensemble $\{f(x) \ / \ x\in G\}$.

Proposition 1.3.3 *Pour tout sous-groupe H de G, f(H) est un sous-groupe de G' et, pour tout sous-groupe H' de G', $f^{-1}(H')$ est un sous groupe de G.*
En particulier Im f est un sous-groupe de G et Ker f est un sous-groupe de G.

Démonstration *1 appartient à H (car H est un sous-groupe de G) et f(1)=1 donc f(H) est non vide. Soient h_1 et h_2 appartenant à H.*
$f(h_1)f(h_2)^{-1} = f(h_1)f(h_2^{-1}) = f(h_1h_2^{-1}) \in f(H)$.
D'où f(H) est un sous-groupe de G'.
1 appartient à H' et f(1)=1 donc f^{-1}(H') est non vide.
Soient g_1 et g_2 appartenant à f^{-1}(H').
Il existe alors h'_1 et h'_2 dans H' tels que $f(g_1) = h'_1$ et $f(g_2) = h'_2$
Donc

$$\begin{aligned} f(g_1g_2^{-1}) &= f(g_1)f(g_2^{-1}) \\ &= f(g_1)f(g_2)^{-1} \\ &= h'_1{h'_2}^{-1} \in H'. \end{aligned}$$

D'où $g_1{g_2}^{-1}$ appartient à f^{-1}(H') et par conséquent, f^{-1}(H')est un sous-groupe de G'. ♢

Proposition 1.3.4 *Ker f=$\{1\}$ si et seulement si f est injective.*

Démonstration *(⇒) On suppose que Ker f=$\{1\}$.*
Soient g_1 et g_2 appartenant à G tels que f(g_1)=f(g_2).
On a alors $f(g_1)f(g_2)^{-1}$=1 c'est à dire $f(g_1{g_2}^{-1})$=1 puisque f est un homomorphisme.
D'où $g_1{g_2}^{-1}$ appartient à Ker f=$\{1\}$.
Par conséquent, $g_1{g_2}^{-1}$=1 et donc g_1=g_2.
(⇐) On suppose que f est injective.
Soit g appartenant à Ker f.
On a alors f(g)=1=f(1).
D'où, comme f est injective, g=1 et Ker f est par conséquent inclus dans $\{1\}$.
Comme f(1)=1, 1 appartient à Ker f et donc f=$\{1\}$. ♢

1.3.3 Isomorphismes

Soient G et G' deux groupes et f : G → G' un homomorphisme de groupes.

Définitions *Si (G,.)=(G',.), on dit que f est un endomorphisme de G.*
L'ensemble des endomorphismes de G est noté Hom(G).
Si f est bijective, on dit que f est un isomorphisme de G dans G'.
Dans ce cas, on dit que G et G' sont isomorphes (ou que G est isomorphe à G').
Si (G,.)=(G',.) et f est bijective, on dit que f est un automorphisme de G.
L'ensemble des automorphismes de G est noté Aut(G).

Proposition 1.3.5 *Soient G et G' deux groupes isomorphes.*
Alors, G est abélien si et seulement si G' est abélien.

Démonstration *Soit f un isomorphisme de G dans G'.*
Soient g'_1 et g'_2 appartenant à G'.
f étant bijective, il existe g_1 et g_2 dans G tels que $g'_1 = f(g_1)$ et $g'_2 = f(g_2)$.
f étant un homomorphisme, on a $g'_1 g'_2 = f(g_1)f(g_1) = f(g_1 g_2)$.
D'où, si G est abélien,

$$\begin{aligned} g'_1 g'_2 &= f(g_1 g_2) \\ &= f(g_2 g_1) \\ &= f(g_2)f(g_1) \\ &= g'_2 g'_1 \end{aligned}$$

et donc G' est abélien.
Si G' est abélien,

$$\begin{aligned} f(g_1 g_2) &= g'_1 g'_2 \\ &= g'_2 g'_1 \\ &= f(g_2)f(g_1) \\ &= f(g_2 g_1) \end{aligned}$$

et donc, comme f est injective, $g_1 g_2 = g_2 g_1$ et par conséquent G est abélien. $\diamondsuit$

Proposition 1.3.6 *Aut(G) est un groupe pour la composition.*

Démonstration *Aut(G) n'est pas vide car il contient l'identité.*
On a vu, à la Proposition 1.3.2, que la composée de deux éléments de Hom(G), donc de deux éléments de Aut(G) (Aut(G) est inclus dans Hom(G)), est un élément de Hom(G).
De plus, si f_1 et f_2 sont des applications bijectives alors $f_1 \circ f_2$ est bijective d'inverse $(f_1 \circ f_2)^{-1} = {f_2}^{-1} \circ {f_1}^{-1}$.
D'où, la composée de deux éléments de Aut(G) est encore un élément de Aut(G).
Soit f appartenant à Aut(G). Posons $\theta = f^{-1}$.
Montrons que θ appartient à Hom(G) : soient g et g' deux éléments de G.
f étant un homomorphisme, $f(\theta(g)\theta(g')) = f(\theta(g))f(\theta(g')) = gg' = f(\theta(gg'))$ par définition de θ. D'où, f étant injective (car bijective), $\theta(gg') = \theta(g)\theta(g')$.
De plus, θ est bijective d'inverse f donc θ appartient à Aut(G).
(Aut(G),$\circ$) est un groupe. $\diamondsuit$

1.4 Produit direct de groupes

1.4.1 Définition

Soient G_1 et G_2 deux groupes.

Proposition 1.4.1 *L'ensemble $G_1 \times G_2$ muni de la loi interne $(g_1, g_2)(g'_1, g'_2) = (g_1 g'_1, g_2 g'_2)$ est un groupe.*

Démonstration *Soient g_1, g'_1 et $g"_1$ appartenant à G_1 et g_2, g'_2 et $g"_2$ appartenant à G_2. Alors, comme G_1 et G_2 sont des groupes,*

$$\begin{aligned}((g_1, g_2)(g'_1, g'_2))(g"_1, g"_2) &= (g_1 g'_1, g_2 g'_2)(g"_1, g"_2)\\ &= ((g_1 g'_1)g"_1, (g_2 g'_2)g"_2)\\ &= (g_1(g'_1 g"_1), g_2(g'_2 g"_2))\\ &= (g_1, g_2)(g'_1 g"_1, g'_2 g"_2)\\ &= (g_1, g_2)((g'_1, g'_2)(g"_1, g"_2)).\end{aligned}$$

D'où, la loi sur $G_1 \times G_2$ est associative.
Cette loi admet l'élément (1,1) comme élément neutre et tout élément (g_1, g_2) de $G_1 \times G_2$ est inversible d'inverse $({g_1}^{-1}, {g_2}^{-1})$ donc $G_1 \times G_2$ est un groupe. $\diamondsuit$

Définition *Le groupe $G_1 \times G_2$ est appelé produit direct des groupes G_1 et G_2.*

Propriété 1.4.2 *$G_1 \times G_2$ est abélien si et seulement si G_1 et G_2 sont abéliens.*

Démonstration *$G_1 \times G_2$ est abélien si et seulement si pour tous les g_1 et g'_1 appartenant à G_1 et g_2 et g'_2 appartenant à G_2, $(g_1, g_2)(g'_1, g'_2) = (g'_1, g'_2)(g_1, g_2)$ c'est à dire $(g_1 g'_1, g_2 g'_2) = (g'_1 g_1, g'_2 g_2)$.*
D'où $G_1 \times G_2$ est abélien si et seulement si $g_1 g'_1 = g'_1 g_1$ pour tous les g_1 et g'_1 appartenant à G_1 et $g_2 g'_2 = g'_2 g_2$ pour tous les g_2 et g'_2 appartenant à G_2, c'est à dire si et seulement si G_1 et G_2 sont abéliens. $\diamondsuit$

Remarque *La notion de produit direct se généralise à une famille (non vide) quelconque (éventuellement infinie) de groupes.*
Si $(G_i)_{i \in I}$ est une telle famille alors le produit cartésien $\prod_{i \in I} G_i$ muni de la loi : $(x_i)_{i \in I}(y_i)_{i \in I} = (x_i y_i)_{i \in I}$ est un groupe.
Ce groupe est abélien si et seulement si chacun des groupes G_i, $i \in I$, est abélien.

1.4.2 Projections canoniques

Soient G_1, ... , G_n des groupes (n$\in \mathbb{N} - \{0\}$).

Définition *Pour tout i appartenant à 1, ... , n, on appelle projection canonique de $G_1\times$ ... $\times G_n$ sur G_i, l'application p_i de $G_1\times$ ... $\times G_n$ dans G_i définie par $p_i(g_1, \ldots, g_n)=g_i$.*

Propriété 1.4.3 *Pour tout i compris entre 1 et n, p_i est un homomorphisme de groupes surjectif.*

Démonstration *Soit i compris entre 1 et n.*
Soient $(g_1, \ldots, g_n)$ et $(g'_1, \ldots, g'_n)$ appartenant à $G_1\times$ ... $\times G_n$.
Alors,

$$\begin{aligned} p_i((g_1, \ldots, g_n)(g'_1, \ldots, g'_n)) &= p_i(g_1g'_1, \ldots, g_ng'_n) \\ &= g_ig'_i \\ &= p_i(g_1, \ldots, g_n)p_i(g'_1, \ldots, g'_n). \end{aligned}$$

et par conséquent, p_i est un homomorphisme de groupes.
Tout g_i de G_i est l'image de $(1, \ldots, g_i, 1, \ldots, 1)$ par p_i donc p_i est surjectif. $\diamondsuit$

Proposition 1.4.4 (Proriété universelle du produit direct) *Soient G un groupe et, pour i compris entre 1 et n, f_i un homomorphisme de groupes de G dans G_i.*
Alors, il existe un unique homomorphisme de G dans $G_1\times$ ... $\times G_n$ tel que $f_i = p_i \circ f$ pour tout i compris entre 1 et n.

Démonstration *Soit f une application de G dans $G_1\times$ ... $\times G_n$ telle que $f_i = p_i \circ f$.*
Alors, pour tout g de G et pour tout i compris entre 1 et n, $p_i(f(g))=f_i(g)$ donc la seule application f possible est celle définie par $f(g)=(f_1(g), \ldots, f_n(g))$.
Montrons que f est un homomorphisme : soient g et g' appartenant à G.
Alors, comme les f_i sont des homomorphismes,

$$\begin{aligned} f(gg') &= (f_1(gg'), \ldots, f_n(gg')) \\ &= (f_1(g)f_1(g'), \ldots, f_n(g)f_n(g')) \\ &= (f_1(g), \ldots, f_n(g))(f_1(g'), \ldots, f_n(g')) \\ &= f(g)f(g'). \end{aligned}$$

D'où, f est un homomorphisme de G dans $G_1\times$ ... $\times G_n$.
f est l'unique homomorphisme de G dans $G_1\times$ ... $\times G_n$ tel que $f_i = p_i \circ f$ pour tout i compris entre 1 et n. $\diamondsuit$

Remarque *Cette Propriété Universelle reste valable pour un famille infinie de groupes.*

1.5 Exercices du Chapitre I

Exercice 1 : On considère la loi $*$ interne sur $\mathbb{R}$ par : a$*$b=a+b-ab.
1)Montrer que $*$ est associative.
2)Montrer que $*$ possède un élément neutre.
Cet élément neutre est-il unique ?
3)$(\mathbb{R}, *)$ est-il un groupe ?

Exercice 2 : Soit E un ensemble non vide.
On note par P(E) l'ensemble des parties de E.
1)Montrer que l'ensemble P(E) muni de l'union de deux ensembles est un monoïde. Est-ce un groupe ?
2)Montrer que l'ensemble P(E) muni de l'intersection de deux ensembles est un monoïde. Est-ce un groupe ?

Exercice 3 : Soit G un groupe.
Montrer G est abélien si et seulement si $(gg')^{-1} = g^{-1}g'^{-1}$ pour tout couple (g,g') d'éléments de G.

Exercice 4 : On définit l'ensemble $\mathbb{D}$ des décimaux par $\{\frac{a}{10^n}$ / a$\in \mathbb{Z}$ et n$\in \mathbb{N}\}$.
Montrer que $(\mathbb{D},+)$ est un sous-groupe de $(\mathbb{Q},+)$.
$(\mathbb{D} - \{0\}, \times)$ est-il un sous-groupe de $(\mathbb{Q} - \{0\}, \times)$?

Exercice 5 : Soit G un groupe dont tous les éléments sont d'ordre 2.
1)Montrer que g=g^{-1} pour tout élément g de G.
2)Montrer que G est abélien.

Exercice 6 : Montrer qu'un groupe d'ordre 4 ne possède pas d'élément d'ordre 3.

Exercice 7 : Soient G un groupe et H un ensemble non vide inclus dans G.
On appelle injection canonique de H dans G, l'application ι de H dans G définie par ι(h)=h.
Montrer que H est un sous-groupe de G si et seulement si H est un groupe et ι est un homomorphisme de groupes.

Exercice 8 : Soient G un groupe et f l'application de G dans G définie par f(g)=g^2.
Montrer que f est un endomorphisme de G si et seulement si G est abélien.

Exercice 9 : On appelle matrice carrée réelle d'ordre 2, tout tableau de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où a, b, c et d sont des réels.
L'ensemble des matrices carrées réelles d'ordre 2 est noté $M_2(\mathbb{R})$.
On définit les lois internes + et . sur $M_2(\mathbb{R})$ par : $\begin{pmatrix} a & b \\ c & d \end{pmatrix}+\begin{pmatrix} e & f \\ g & h \end{pmatrix}=\begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$ et $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}=\begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$.
1)Montrer que $(M_2(\mathbb{R}),+)$ est un groupe abélien.
2)Montrer que $(M_2(\mathbb{R}),.)$ est un monoïde.
3)La loi . est-elle commutative ?
4)Donner un exemple de matrice n'admettant pas d'inverse pour la loi .
5)On définit l'application det, appelée déterminant, de $M_2(\mathbb{R})$ dans $\mathbb{R}$ par
$\det(\begin{pmatrix} a & b \\ c & d \end{pmatrix})$=ad-bc.
L'image d'une matrice par l'application det est appelée déterminant de cette matrice.
Montrer que quelles que soient les matrices M et N, det(MN)=det(M)det(N).
6)En déduire qu'un élément M de $M_2(\mathbb{R})$ inversible pour la loi . est de déterminant non nul.
7)Soit M=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice de déterminant non nul.
On définit la matrice N par N=$\begin{pmatrix} \frac{d}{det(M)} & \frac{-b}{det(M)} \\ \frac{-c}{det(M)} & \frac{a}{det(M)} \end{pmatrix}$.
Montrer que N est la matrice inverse de M pour la loi .
8)On note par $GL_2(\mathbb{R})$, le sous-ensemble de $M_2(\mathbb{R})$ formé des matrices inversibles.
Montrer que $(GL_2(\mathbb{R}),.)$ est un groupe (ce groupe est appelé groupe linéaire réel d'ordre 2).
9)Montrer que pour tout élément de $GL_2(\mathbb{R})$, $\det(M^{-1})=\frac{1}{det(M)}$.
10)On note par $SL_2(\mathbb{R})$, le sous-ensemble de $GL_2(\mathbb{R})$ formé des matrices de déterminant 1.
Montrer de deux manières différentes que $SL_2(\mathbb{R})$ est un sous-groupe de $GL_2(\mathbb{R})$ (ce sous-groupe est appelé groupe spécial linéaire réel d'ordre 2).

Exercice 10 : 1)Montrer que si G_1 et G_1' sont deux groupes isomorphes et G_2 et G_2' sont également deux groupes isomorphes alors $G_1 \times G_2$ est isomorphe à $G_1' \times G_2'$.
2)En déduire que pour tout entier strictement positif n, $\mathbb{C}^n$(=$\mathbb{C}\times$ ... $\times\mathbb{C}$, n fois) est isomorphe à $\mathbb{R}^{2n}$ (=$\mathbb{R}\times$ ... $\times\mathbb{R}$, 2n fois).

Chapitre 2

Cyclicité

Groupe $\mathbb{Z}/n\mathbb{Z}$

Groupes cycliques

2.1 Groupe $\mathbb{Z}/n\mathbb{Z}$

2.1.1 Congruence

Soit n un entier positif.

Proposition 2.1.1 *La relation R définie sur $\mathbb{Z}$ par $xRy \Leftrightarrow \exists k \in \mathbb{Z}$ / x-y=kn, est une relation d'équivalence.*

Démonstration *R est réflexive : xRx en prenant k=0.*
R est symétrique : si xRy par l'entier k alors yRx par l'entier -k.
R est transitive : si xRy par l'entier k et yRz par l'entier m alors xRz par l'entier k+m. $\diamondsuit$

Définition *Cette relation est appelée relation de congruence modulo n.*
Deux entiers x et y en relation sont dits congrus l'un à l'autre modulo n et on note alors $x \equiv y \bmod n$ (ou $x \equiv y$ [n]).

Remarques *1)La relation de congruence modulo 0 est l'égalité.*
2)$x \equiv 0 \bmod n$ si et seulement si n divise x.

Propriété 2.1.2 *Soient x, y, z et t des entiers.*
1)Si $x \equiv y \bmod n$ et $z \equiv t \bmod n$ alors $(x+z) \equiv (y+t) \bmod n$.
2)Si $x \equiv y \bmod n$ et $z \equiv t \bmod n$ alors $xz \equiv yt \bmod n$.

Démonstration *Par hypothèse, il existe deux entiers k et m tels que $x=y+kn$ et $z=t+mn$. On a alors $x+z=y+t+(k+m)n$ c'est à dire $(x+z) \equiv (y+t) \bmod n$ et $xz=yt+(ym+kt+km)n$ c'est à dire $xz \equiv yt \bmod n$.* $\diamondsuit$

2.1.2 Groupe $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier positif.

Définition *Soit x appartenant à $\mathbb{Z}$. On note par $\overline{x}$ la classe d'équivalence de x pour la relation de congruence modulo n.*
On note par $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences de la relation de congruence modulo n.

Proposition 2.1.3 *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de la correspondance $((\overline{x},\overline{y}) \to \overline{x+y})$ est un groupe abélien.*

Démonstration *Notons par + la correpondance* $((\overline{x},\overline{y}) \to \overline{x+y})$.
On note $\overline{x}+\overline{y}$ *à la place de* $+(\overline{x},\overline{y})$.
Commençons par montrer que la correspondance + est une loi interne sur $\mathbb{Z}/n\mathbb{Z}$ *c'est à dire une application : soient* $(\overline{x},\overline{z})$ *et* $(\overline{y},\overline{t})$ *deux couples égaux d'éléments de* $\mathbb{Z}/n\mathbb{Z}$.
On a alors $\overline{x}=\overline{y}$ *c'est à dire* $x \equiv y \ mod\ n$ *et* $\overline{z} = \overline{t}$ *c'est à dire* $z \equiv t \ mod\ n$.
D'où, d'après la première Propriété 2.1.2, $(x+z) \equiv (y+t) \ mod\ n$ *c'est à dire* $\overline{x+z} = \overline{y+t}$. *On a donc* $\overline{x}+\overline{z}=\overline{y}+\overline{t}$.
D'où, la correpondance + est une loi interne sur $\mathbb{Z}/n\mathbb{Z}$.
Montrons que la loi + est associative : soient x, y et z des entiers.
Il découle de l'associativité de $\mathbb{Z}$ *que*
$(\overline{x}+\overline{y})+\overline{z} = \overline{x+y}+\overline{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \overline{x}+\overline{y+z} = \overline{x}+(\overline{y}+\overline{z})$.
Donc, la loi + est associative.
Pour tout entier x, $\overline{x}+\overline{0} = \overline{x+0} = \overline{x}$ *et de même* $\overline{0}+\overline{x}=\overline{x}$, *donc* $\overline{0}$ *est l'élément neutre de la loi +.*
Soit x un entier. $\overline{x}+\overline{-x} = \overline{x-x} = \overline{0}$ *et de même* $\overline{-x}+\overline{x}=\overline{0}$, *donc* $\overline{x}$ *est inversible d'inverse* $\overline{-x}$.
D'où, $(\mathbb{Z}/n\mathbb{Z},+)$ *est un groupe.*
Soient x et y deux entiers.
$\overline{x}+\overline{y}=\overline{x+y} = \overline{y+x}=\overline{y}+\overline{x}$ *donc* $(\mathbb{Z}/n\mathbb{Z},+)$ *est un groupe abélien.* $\diamondsuit$

Remarques *Pour tout entier x,* $\overline{x}=x+n\mathbb{Z}$.
En particulier, $\overline{0}=n\mathbb{Z}$.

Définition *On appelle surjection canonique de* $\mathbb{Z}$ *sur* $\mathbb{Z}/n\mathbb{Z}$, *l'application* π *qui à tout entier x associe sa classe d'équivalence* $\overline{x}$.

Proposition 2.1.4 π *est un homomorphisme de groupes surjectif de noyau* $n\mathbb{Z}$.

Démonstration π *est clairement surjective puisqu'à une classe de conjugaison corrspond un de ses représentants comme antécédent.*
Soient $\overline{x}$ *et* $\overline{y}$ *appartenant à* $\mathbb{Z}/n\mathbb{Z}$.
Alors, par définition de la loi de $\mathbb{Z}/n\mathbb{Z}$, $\pi(x+y) = \overline{x+y}=\overline{x}+\overline{y}=\pi(x)+\pi(y)$.
Donc, π *est un homomorphisme.*
Déterminons le noyau de π :

$$\begin{aligned} Ker\ \pi &= \{x \in \mathbb{Z} \ / \ \pi(x) = 0\} \\ &= \{x \in \mathbb{Z} \ / \ x \equiv 0 mod n\} \\ &= \{x \in \mathbb{Z} \ / \ \exists k \in \mathbb{Z} \ tq \ x = kn = nk\} \\ &= n\mathbb{Z}. \end{aligned}$$

$\diamondsuit$

On suppose que n est non nul.

Corollaire 2.1.5 $\mathbb{Z}/n\mathbb{Z}$ *est engendré par* $\overline{1}$.

Démonstration *Soit $\overline{x}$ appartenant $\mathbb{Z}/n\mathbb{Z}$.*
Si $\overline{x}=\overline{0}$, on a $\overline{x}=0.\overline{1}$ (convention pour la notation additive sur un groupe G, 0.g=0 pour tout g de G).
Si x est strictement positf, on a

$$\begin{aligned}\overline{x} &= \pi(x)\\ &= \pi(x.1)\\ &= \pi(1+\ ...\ +1)\ x\ fois\\ &= \pi(1)+\ ...\ +\pi(1)\ x\ fois\ (par\ homomorphie)\\ &= x\pi(1)\\ &= x\overline{1}.\end{aligned}$$

Si x est strictement négatif, on a

$$\begin{aligned}\overline{x} &= \pi(x)\\ &= \pi(x.(-1))\\ &= \pi((-1)+\ ...\ +(-1))\ x\ fois\\ &= \pi(-1)+\ ...\ +\pi(-1)\ x\ fois\ (par\ homomorphie)\\ &= -\pi(1)+\ ...\ -\pi(1)\ x\ fois\ (par\ homomorphie)\\ &= -x\pi(1)\\ &= -x\overline{1}.\end{aligned}$$

D'où, $\mathbb{Z}/n\mathbb{Z}$ est engendré par $\overline{1}$. $\diamondsuit$

Proposition 2.1.6 *$|\mathbb{Z}/n\mathbb{Z}|=n$.*

Démonstration *Si n=1, il est clair que tous les entiers sont congrus entre eux puisque 1 engendre $\mathbb{Z}$. Il n'y a donc qu'une seule classe d'équivalence et par conséquent $|\mathbb{Z}/1\mathbb{Z}|=1$.*
On suppose que n>1.
On a vu que la classe d'équivalence d'un entier x est l'ensemble $x+n\mathbb{Z}$.
Montrons que cette classe a un représentant compris entre 0 et n-1 : par l'algorithme d'Euclide, il existe un couple d'entiers (i,j) avec $0\leq j<n$ tel que $x=in+j$.
Ce j est congru à x modulo n et donc $\overline{x}=\overline{j}$.
De plus, si i et j sont deux entiers distincts compris entre 0 et n-1 alors i et j ne sont pas congrus modulo n (i-j compris entre -n+1 et n-1 et est différent de 0).
D'où on a n classes distinctes et donc $|\mathbb{Z}/n\mathbb{Z}|=n$. $\diamondsuit$

2.1.3 Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier strictement positif.

Proposition 2.1.7 *Tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est engendré par un de ses éléments.*

Démonstration *Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.*
Si H=0 alors H=<0> et si H=$\mathbb{Z}/n\mathbb{Z}$ alors H=<1>.
On suppose que H est un sous-groupe propre de $\mathbb{Z}/n\mathbb{Z}$.
Alors, puisque π est un homomorphisme de groupes, K=π^{-1}(H) est un sous-groupe de $\mathbb{Z}$ (d'après la Proposition 1.3.3).
On a vu (Proposition 1.2.11) que tout sous-groupe de $\mathbb{Z}$ est de la forme k$\mathbb{Z}$=<k> donc, comme π est un homomorphisme surjectif, on a :

$$\begin{aligned} H &= \pi(\pi^{-1}(H)) \\ &= \pi(K) \\ &= \pi(< x >) \\ &= < \pi(x) > \\ &= < \overline{x} > . \end{aligned}$$

H est donc un sous-groupe engendré par un de ses éléments. $\diamondsuit$

Proposition 2.1.8 *Soit $\overline{x}$ appartenant à $\mathbb{Z}/n\mathbb{Z}$ avec x$\neq$0.*
Si pgcd(x,n)=p alors <$\overline{x}$>=<$\overline{p}$>.

Démonstration *Examinons le cas où x est négatif : x-xn est alors positif.*
Dans $\mathbb{Z}/n\mathbb{Z}$,On a $\overline{x - xn} = \overline{x} - x\overline{n} = \overline{x}$.
Montrons que p est le pgcd de x-xn et n : p divise x et n donc p divise x-xn.
Si q divise x-xn et n alors il existe deux entiers r et s tels que x-xn=qr et n=qs.
D'où, x=qr-xn=q(r-xs) et donc q divise x.
On en déduit que p divise q puisque p=pgcd(x,n). Par conséquent, p=pgcd(x-xn,n).
On se ramène donc à montrer que <$\overline{x - xn}$>=<$\overline{p}$> où x-xn est positif et pgcd(x-xn,n)=p autrement dit, on se ramène à la démonstration de la proposition pour un entier x positif.
On prend x positif et on pose x=ps (l'entier s existe car p divise x).
Alors, comme π est un homomorphisme (Proposition 2.1.4) ,

$$\begin{aligned} \overline{x} &= \pi(x) \\ &= \pi(sp) \\ &= \pi(p + \ \ldots \ + p) \ s \ fois \\ &= \pi(p) + \ \ldots \ + \pi(p) \ s \ fois \\ &= s\pi(p) \\ &= s\overline{p} \in < \overline{p} > . \end{aligned}$$

D'où <$\overline{x}$>$\subset$<$\overline{p}$> (<$\overline{x}$> est le plus petit sous-groupe contenant $\overline{x}$)
D'après l'Identité de Bezout, il existe deux entiers a et b tels que ax+bn=p.
D'où, comme π est un homomorphisme de noyau n$\mathbb{Z}$ (Proposition 2.1.4),

$$\begin{aligned} \overline{p} &= \pi(p) \\ &= \pi(ax + bn) \\ &= a\pi(x) + b\pi(n) \\ &= a\pi(x) \\ &= a\overline{x}. \end{aligned}$$

Par conséquent, $\overline{p}$ appartient à $<\overline{x}>$ et donc $<\overline{p}>\subset<\overline{x}>$.
D'où, $<\overline{x}>=<\overline{p}>$. ♢

Corollaire 2.1.9 *Soit $\overline{x}$ appartenant à $\mathbb{Z}/n\mathbb{Z}$ avec $x\neq 0$.*
Alors, l'ordre de $\overline{x}$ dans $\mathbb{Z}/n\mathbb{Z}$ est égal à $\frac{n}{pgcd(x,n)}$.

Démonstration *On a vu dans la démonstration de la Proposition précédente qu'il suffit d'étudier le cas où x est positif.*
$o(\overline{x})=|<\overline{x}>|=|<\overline{p}>|=o(\overline{p})$.
$o(\overline{p})$ est le plus petit entier strictement positif m tel que $m\overline{p}=\overline{0}$. Or p divise n donc $\frac{n}{p}.\overline{p}=\overline{\frac{n}{p}.p}=\overline{n}=\overline{0}$. De plus, $\frac{n}{p}$ est le seul entier compris entre 1 et n-1 tel que $\frac{n}{p}.p=n$, donc $\frac{n}{p}$ est le plus petit entier strictement positif m tel que m.p est multiple de n c'est à dire $m\overline{p}=\overline{0}$. D'où, $o(\overline{p})=\frac{n}{p}$. ♢

Remarque *En particulier, si x divise n alors $o(\overline{x})=\frac{n}{x}$.*

Exemple *Pour $\mathbb{Z}/6\mathbb{Z}$, le tableau des ordres des éléments est :*

$\overline{x}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$o(\overline{x})$	1	6	3	2	3	6

.

Proposition 2.1.10 *Pour tout diviseur positif d de n, il existe un et un seul sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d.*

Démonstration *Soit $m=\frac{n}{d}$.*
Alors, il est clair que d est le plus petit entier tel que $d\overline{m}=0$ puisque $dm=n$.
Donc, le groupe engendré par $\overline{m}$, $<\overline{m}>$, est d'ordre d.
Soit H un sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$.
D'après la Proposition 2.1.7, H est de la forme $<\overline{x}>$.
Montrons que $\overline{x}$ appartient à $<\overline{m}>$:
$<\overline{x}>$ est d'ordre d donc $d\overline{x}=\overline{dx}=0$ c'est à dire n divise dx.
Par conséquent, il existe un entier k tel que $dx=kn$.
D'où, d divisant n, $x=k(\frac{n}{d})=km$ et donc $\overline{x}=\overline{km}=k\overline{m}$ appartient à $<\overline{m}>$.
Par conséquent, H est inclus dans $<\overline{m}>$ (H est le plus petit sous-groupe contenant $\overline{x}$).
Or, ces deux groupes ont le même ordre c'est à dire le même cardinal, donc $H=<\overline{m}>$.
Il n'y a qu'un seul sous-groupe d'ordre d. ♢

2.1.4 Identification

Soit n un entier strictement positif.

On a prouvé dans la démonstration de la Proposition 2.1.6 que $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble $\{\overline{0},\ \overline{1},\ \ldots\ ,\ \overline{n-1}\}$.
Si on restreint π à $\{0,\ 1,\ \ldots\ ,\ \text{n-1}\}$, π devient une bijection de cet ensemble dans $\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\ \overline{1},\ \ldots\ ,\ \overline{n-1}\}$ puisque les entiers compris entre 0 et n-1 ne sont pas congrus entre eux (ce qui rend π injective).
Soit φ l'inverse de cette restriction de π.
Si $\overline{x}$ et $\overline{y}$ sont deux éléments de $\mathbb{Z}/n\mathbb{Z}$, alors $\varphi(\overline{x}+\overline{y})=\varphi(\overline{x})+\varphi(\overline{y})$ si on pose comme loi interne sur $\{0,\ 1,\ \ldots\ ,\ \text{n-1}\}$, la loi de congruence : x+y=z où z est l'entier tel que x+y≡z mod n.
Cette propriété (propriété d'homomorphie) confère à l'ensemble $\{0,\ 1,\ \ldots\ ,\ \text{n-1}\}$ muni de la loi de congruence, la structure de groupe (additif) abélien et comme on a un groupe, φ est un isomomorphisme de groupes.
On a donc $\mathbb{Z}/n\mathbb{Z}$ isomorphe au groupe $\{0,\ 1,\ \ldots\ ,\ \text{n-1}\}$ muni de la loi de congruence (x+y=z où z est l'entier tel que x+y≡z mod n, par l'isomorphisme $\varphi = {\pi_{|\{0,\ 1,\ \ldots\ ,\ n-1\}}}^{-1}$
Par abus de langage, le groupe $\mathbb{Z}/n\mathbb{Z}$ désigne en général le groupe
$\{0,\ 1,\ \ldots\ ,\ \text{n-1}\}$ muni de la loi de congruence.

Ainsi $\mathbb{Z}/4\mathbb{Z}$ peut être identifié à l'ensemble $\{0,\ 1,\ 2,\ 3\}$ muni de la loi + définie par la table :

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

2.2 Groupes cycliques

2.2.1 Groupes monogènes et groupes cycliques

Définition *Un groupe est dit monogène si il est engendré par un de ses éléments. Cet élément est appelé générateur de ce groupe.*
Un groupe monogène fini est dit cyclique.

Proposition 2.2.1 *Un élément d'un groupe cyclique est un générateur de ce groupe si et seulement si son ordre est égal à l'ordre du groupe.*

Démonstration *Soit G un groupe cyclique d'ordre n et g un élément de G.*
g est un générateur de G si et seulement si <g>=G.
Puisque <g> est toujours inclus dans G, <g>=G si et seulement si Card(<g>)=Card(G) c'est à dire si et seulement si l'ordre de g est égal à l'ordre de G. $\diamondsuit$

Corollaire 2.2.2 *Soit n un entier strictement positif.*
$\mathbb{Z}/n\mathbb{Z}$ *est un groupe cyclique d'ordre n dont les générateurs sont les éléments* $\overline{x}$ *où x et n sont premiers entre eux.*

Démonstration *D'après le Corollaire 2.1.5 et la Proposition 2.1.6,* $\mathbb{Z}/n\mathbb{Z}$ *est un groupe cyclique d'ordre n.*
D'après la Proposition 2.1.9, l'ordre d'un élément $\overline{x}$ *de* $\mathbb{Z}/n\mathbb{Z}$ *est égal à* $\frac{n}{pgcd(x,n)}$.
D'où, d'après la Proposition précédente, $\overline{x}$ *est un générateur de* $\mathbb{Z}/n\mathbb{Z}$*si et seulement si* $\frac{n}{pgcd(x,n)} = n$ *c'est à dire pgcd(x,n)=1.* $\diamondsuit$

Remarques *1)Tout élément d'un groupe monogène G=<g> est de la forme* g^n *où n est un entier.*
2)Tout élément d'un groupe cyclique G=<g> d'ordre n est de la forme g^m *où m est un entier compris entre 0 et n-1.*

Exemples *1)*$\mathbb{Z}$ *est un groupe monogène engendré par 1.*
2)Tout sous-groupe de $\mathbb{Z}$ *est monogène.*
3)Pour tout entier strictement positif n, $\mathbb{Z}/n\mathbb{Z}$ *est un groupe cyclique. dont les générateurs sont, d'après la Proposition 2.1.9, les* $\overline{m}$ *avec m entier compris entre 0 et n-1 et m premier avec n.*

Propriété 2.2.3 *Tout groupe monogène est abélien.*

Démonstration *Soient G=<g> un groupe monogène et* g^n *et* g^m *deux éléments de G. Alors, on a* $g^n g^m = g^{n+m} = g^{m+n} = g^m g^n$ *et G est donc abélien.* $\diamondsuit$

Proposition 2.2.4 *Soient G et G' deux groupes et f : G → G' un homomorphisme de groupes surjectif.*
Si G est cyclique engendré par g alors G' est cyclique engendré par f(g).

Démonstration *Comme G est fini, G' est fini car f est surjective (Card G'<Card G). Soit g le générateur de G.*
Comme f est surjective, tout élément de G' s'écrit sous la forme $f(g^n)$ où n est un entier compris entre 1 et $|G|-1$. D'où, f étant un homomorphisme, $f(g^n)=f(g)^n$.
G' est donc un groupe cyclique engendré par f(g). ♢

Corollaire 2.2.5 *Soient G et G' deux groupes isomorphes.*
Alors, G est cyclique si et seulement si G' est cyclique.

Démonstration *Soit f l'isomorphisme de G vers G'.*
D'après la Proposition précédente, comme f est surjective, si G est cyclique alors G' est cyclique.
Comme f^{-1} est surjective, si G' est cyclique alors G est cyclique.
D'où G est cyclique si et seulement si G' est cyclique. ♢

Proposition 2.2.6 *1)Un groupe monogène est isomorphe à $\mathbb{Z}$.*
2)Un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Démonstration *1)Soit G=<g> un groupe monogène.*
Alors, l'application φ de G dans $\mathbb{Z}$ définie par $\varphi(g^n)=n$ est clairement un isomorphisme.
2)Soit G=<g> un groupe cyclique d'ordre n.
Alors, l'application ψ de G dans $\mathbb{Z}/n\mathbb{Z}$ définie par $\psi(g^m)=\overline{m}$ est clairement un isomorphisme. ♢

Proposition 2.2.7 *Soient G et G' deux groupes cycliques d'ordre m et n respectivement. Si m et n sont premiers entre eux alors G×G' est un groupe cyclique d'ordre mn.*

Démonstration *Soient g le générateur de G et g' le générateur de G'.*
g est donc d'ordre m dans G et g' d'ordre n dans G'. Soit k l'ordre de (g,g') dans G×G'.
$(g,g')^k=(g^k,g'^k)$*=(1,1) donc* $g^k=1$ *et* g'^k*=1.*
D'où m et n divisent k.
Par suite, comme m et n sont premiers entre eux, mn divise k.
Or G×G' est d'ordre mn donc k est inférieur à mn.
D'où mn=k et donc (g,g') engendre G×G'.
G×G' est cyclique. ♢

2.2.2 Sous-groupes d'un groupe cyclique

Proposition 2.2.8 *Tout sous-groupe d'un groupe monogène (respectivement cyclique) est monogène (respectivement cyclique).*

Démonstration *Soit G un groupe monogène.*
D'après la Proposition précédente, G est isomorphe à $\mathbb{Z}$ par un isomorphisme φ.
Soit H un sous-groupe de G.
Comme φ est un homomorphisme, $\varphi(H)$ est un sous-groupe K de $\mathbb{Z}$.
Or tout sous-groupe de $\mathbb{Z}$ est monogène donc, comme $H=\varphi^{-1}(K)$, H est monogène d'après la Proposition précédente.
Soit G un groupe cyclique d'ordre n.
D'après la Proposition précédente, G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ par un isomorphisme ψ.
Soit H un sous-groupe de G.
Comme ψ est un homomorphisme, $\psi(H)$ est un sous-groupe K de $\mathbb{Z}/n\mathbb{Z}$.
Or tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$est cyclique, d'après la Proposition 2.1.7 donc, comme $H=\psi^{-1}(K)$, H est cyclique d'après la Proposition précédente. $\diamondsuit$

2.2.3 Une propriété arithmétique

Soit n un entier strictement positif.

Définition *On appelle indicateurd'Euler de n, et on note $\varphi(n)$, le nombre d'entiers, compris entre 1 et n, premiers avec n.*

Exemples *1)$\varphi(6)=2$.*
2)Si p est un nombre premier, $\varphi(p)=p-1$.

le résultat suivant découle de la Proposition 2.2.2 :

Proposition 2.2.9 *$\mathbb{Z}/n\mathbb{Z}$ admet $\varphi(n)$ générateurs.*

Corollaire 2.2.10 *$\mathbb{Z}/n\mathbb{Z}$ possède $\varphi(d)$ éléments d'ordre d.*

Démonstration *Un élément x de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre d si et seulement si il engendre un groupe d'ordre d c'est à dire si et seulement si il est générateur de l'unique (d'après la Proposition 2.1.10) sous-groupe H de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. D'après la Proposition 2.2.6, H est isomorphe à $\mathbb{Z}/d\mathbb{Z}$ donc d'après la Proposition 2.2.4, les générateurs de $\mathbb{Z}/d\mathbb{Z}$ sont en bijection avec les générateurs de H.*
Par conséquent, le nombre d'éléments de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d est égal au nombre de générateurs de $\mathbb{Z}/d\mathbb{Z}$ c'est à dire $\varphi(d)$ d'après la Proposition précédente. $\diamondsuit$

Proposition 2.2.11 $n=\sum_{\substack{1\leq d\leq n \\ d\,diviseur\,de\,n}} \varphi(d)$.

Démonstration *Regroupons les éléments de* $\mathbb{Z}/n\mathbb{Z}$ *selon leur ordre.*
D'après la Proposition 2.1.9, l'ordre d'un élément divise n.
On a donc $n=\sum_{d|n}$ *Card* $\{$*éléments d'ordre d*$\}$.
Mais, d'après le Corollaire précédent, Card $\{$*éléments d'ordre d* $\} = \varphi(d)$ *donc* $n=\sum_{d|n}\ \varphi(d)$.
$\diamondsuit$

2.2.4 Automorphismes de $\mathbb{Z}/n\mathbb{Z}$

Proposition 2.2.12 *Si f est un automorphisme de* $\mathbb{Z}/n\mathbb{Z}$ *alors f(1) est un générateur de* $\mathbb{Z}/n\mathbb{Z}$.

Démonstration *Soit f un endomorphisme de* $\mathbb{Z}/n\mathbb{Z}$.
Pour tout entier s compris entre 1 et n, f(s)=f(s.1)=f(1+ ... +1)=f(1)+ ... +f(1)=sf(1).
donc f est déterminé par f(1).
Supposons maintenant que f est un automorphisme. f est donc surjective.
Alors, comme 1 engendre $\mathbb{Z}/n\mathbb{Z}$, *f(1) est un générateur de* $\mathbb{Z}/n\mathbb{Z}$ *d'après la Proposition 2.2.4.* $\diamondsuit$

Corollaire 2.2.13 *Le nombre d'automorphismes de* $\mathbb{Z}/n\mathbb{Z}$ *est égal à* $\varphi(n)$.

Démonstration *Le nombre d'automorphismes de* $\mathbb{Z}/n\mathbb{Z}$ *est égal au nombre de générateurs de* $\mathbb{Z}/n\mathbb{Z}$ *c'est à dire* $\varphi(n)$ *d'après la Proposition 2.2.9.* $\diamondsuit$

Remarque *Si n et m sont des entiers distincts, il n'y a pas d'isomorphismes entre* $\mathbb{Z}/n\mathbb{Z}$*et* $\mathbb{Z}/m\mathbb{Z}$ *puisque ces deux groupes ont des cardinaux différents.*

2.3 Exercices du Chapitre 2

Exercice 1 : 1)Montrer que tout entier naturel n est congru à la somme de ses chiffres modulo 9.
2)En déduire un critère de divisibilité d'un entier naturel par 9.

Exercice 2 : Déterminer la véracité de la proposition suivante :
Si n et m sont deux entiers tels que n<m alors $\mathbb{Z}/n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}/m\mathbb{Z}$.

Exercice 3 : 1)Calculer le nombre d'automorphismes de $\mathbb{Z}/6\mathbb{Z}$.
2)Expliciter ces automorphismes.

Exercice 4 : Soit E un ensemble non vide.
On désigne par P(E) l'ensemble des parties de E.
Pour tout élément A de P(E), on note par Φ_A l'application de E dans $\mathbb{Z}/2\mathbb{Z}$ définie par

$$\begin{aligned}\Phi_A(x) &= \overline{1}\, si\ x \in A \\ &= \overline{0}\, sinon.\end{aligned}$$

On note par Φ l'application, de P(E) dans l'ensemble F des fonctions de E dans $\mathbb{Z}/2\mathbb{Z}$, qui à une partie A de E associe l'application Φ_A.
1)Montrer que l'application Φ est bijective.
2)Montrer que l'ensemble F, muni de la loi interne f+g : x$\rightarrow f(x)+g(x)$, est un groupe abélien.
3)Soient A et B deux parties de E.
Quel est l'antécédent pour Φ de l'application $\Phi_A+\Phi_B$?
4)En déduire que l'on peut définir une structure de groupe sur P(E) en prenant pour loi la différence symétique : AΔB=A$\cup$B/A$\cap$B.

Exercice 5 : Soit n un entier strictement positif.
Montrer que l'ensemble des racines complexes $n^{èmes}$ de l'unité (c'est à dire l'ensemble des racines complexes du polynôme X^n-1) muni de la multiplication usuelle est un groupe cyclique d'ordre n.

Exercice 6 : Soit G un groupe fini non réduit à l'élément neutre.
Montrer que si les seuls sous-groupes de G sont {1} et G alors G est un groupe cyclique d'ordre un nombre premier.
Remarque : Nous verrons dans la Section *Sous-groupes normaux* du Chapitre 3 que si l'ordre de G est un nombre premier alors G est cyclique et les seuls sous-groupes de G sont G et {1}.

Exercice 7 : Soit p un nombre premier.
Montrer que pour tout entier n$\geq$1, $\varphi(p^n) = (p-1)p^{n-1}$.

Dans les trois exercices suivants, on utilisera le Théorème de Bezout :
Si n et m sont deux entiers non nuls alors n et m sont premiers entre eux si et seulement si il existe deux entiers u et v tels que un+vm=1.

Exercice 8 : Soit n un entier strictement positif.
1)Montrer que l'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de la correspondance $((\overline{x},\overline{y})\rightarrow \overline{xy})$ est un monoïde commutatif.
2)Soit $\overline{x}$ un élément non nul de $\mathbb{Z}/n\mathbb{Z}$.
Montrer que $\overline{x}$ est inversible si et seulement si x est premier avec n.
3)On note par $U(\mathbb{Z}/n\mathbb{Z})$, l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.
Montrer que $(U(\mathbb{Z}/n\mathbb{Z}),.)$ est un groupe abélien.
4)Montrer que $Aut(\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $U(\mathbb{Z}/n\mathbb{Z})$.
5)En déduire que $Aut(\mathbb{Z}/n\mathbb{Z})$ est abélien.

Exercice 9 : Le but de cet exercice est la résolution, dans $\mathbb{Z}$, des systèmes de congruences de la forme (S) : $\left\{ \begin{array}{l} x \equiv a \ mod \ n \\ x \equiv b \ mod \ m \end{array} \right.$ où n et m sont deux entiers positifs premiers entre eux, a un entier compris entre 0 et n-1 et b un entier compris entre 0 et m-1.
1)Il existe, d'après le Théorème de Bezout, deux entiers u et v tels que un+vm=1.
Vérifier que bun+avm est solution du système (S).
On note cette solution x_0.
2)Soit x une solution du système (S).
Montrer que n et m divisent x-x_0.
3)En déduire que nm divise x.
4)Montrer que l'ensemble des solutions du système (S) est l'ensemble
$\{x_0 + knm \ / \ k \in \mathbb{Z}\}$.
5)Application : Résoudre le système de congruences : $\left\{ \begin{array}{l} x \equiv 2 \ mod \ 3 \\ x \equiv 1 \ mod \ 5 \end{array} \right.$.

Exercice 10 : A)Théorème Chinois (version groupes)
Soient n et m deux entiers strictement positifs et premiers entre eux.
Soit x un entier. On note par $\overline{x}$ (respectivement $\hat{x}$, $\check{x}$), la classe de x dans $\mathbb{Z}/nm\mathbb{Z}$ (respectivement $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$).
On considère la correspondance f de $\mathbb{Z}/nm\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ définie par : $f(\overline{x})=(\hat{x},\check{x})$.
1)Montrer que f est une application.
2)Montrer que f est un homomorphisme de groupes.
3)Montrer que si n et m divisent un entier x alors nm divise également x.
4)En déduire que f est un homorphisme injectif.
5)Montrer que f est un isomorphisme de groupes.
6)En déduire que $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est un groupe cyclique.
B)Soient n et m deux entiers non premiers entre eux.
1)Soit $(\hat{x},\check{y})$ un élément de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
Montrer que l'ordre de (x,y) est le ppcm des ordres de x et de y.
2)Montrer que $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ n'est pas un groupe cyclique.
Indication : On pourra utiliser la propriété suivante : si a et b sont deux entiers non nuls alors ab=pgcd(a,b)ppcm(a,b).

Chapitre 3

Groupes quotients

Sous-groupes normaux

Groupes quotients

Théorèmes d'isomorphisme

Produit semi-direct

Groupe dérivé, groupes résolubles

3.1 Sous-groupes normaux

La normalité est l'une des notions les plus importantes en Théorie des groupes.

3.1.1 Relations R_H et ${}_HR$

Soient G un groupe et H un sous-groupe de G.

Proposition 3.1.1 *La relation ${}_HR$ (respectivement R_H) définie sur $G\times G$ par $g_HRg' \Leftrightarrow g^{-1}g' \in H$ (respectivement $gR_Hg' \Leftrightarrow gg'^{-1} \in H$) est une relation d'équivalence.*

Démonstration *On démontre cette proposition pour la relation ${}_HR$ (la démonstration est similaire pour le cas R_H).*
${}_HR$ est réflexive : pour tout élément g de G, $g^{-1}g = 1 \in H$.
${}_HR$ est symétrique : si g et g' appartiennent à G et g_HRg' alors $g^{-1}g' \in H$ donc, comme H est un sous-groupe de G, $(g^{-1}g')^{-1} = g'^{-1}g \in H$ c'est à dire g'_HRg.
${}_HR$ est transitive : si g, g' et g" sont des éléments de G tels que g_HRg' et $g'_HRg"$ alors $g^{-1}g' \in H$ et $g'^{-1}g" \in H$ donc, comme H est un sous-groupe de G, $(g^{-1}g')(g'^{-1}g") = g^{-1}g" \in H$ c'est à dire $g_HRg"$. ♢

Proposition 3.1.2 *La relation ${}_HR$ est compatible à gauche avec la loi de G c'est à dire, si g et g' sont des éléments de G tels que g_HRg' alors, pour tout élément g" de G, $g"g_HRg"g'$.*
La relation R_H est compatible à droite avec la loi de G c'est à dire, si g et g' sont des éléments de G tels que gR_Hg' alors, pour tout élément g" de G, $gg"R_Hg'g"$.

Démonstration *On démontre la proposition pour la relation ${}_HR$ (le cas R_H se montrant de manière similaire). Soient g et g' deeux éléments de G tels que g_HRg'. On a alors $g^{-1}g' \in H$. Mais, pour tout élément g" de G, $g^{-1}g' = g^{-1}g"^{-1}g"g'$, donc $g^{-1}g"^{-1}g"g' = (g"g)^{-1}(g"g') \in H$ c'est à dire $g"g_HRg"g'$ de G.* ♢

Proposition 3.1.3 *Soit g appartenant à G.*
La classe d'équivalence de g pour la relation ${}_HR$ est l'ensemble
$gH=\{gh \ / \ h\in H\}$.
La classe d'équivalence de g pour la relation R_H est l'ensemble
$Hg=\{hg \ / \ h\in H\}$.
En particulier, la classe de 1 pour les relations ${}_HR$ et R_H est H.

Démonstration *La classe de g pour la relation ${}_HR$ est l'ensemble*
$\{g'\in G \ / \ g^{-1}g' \in H\} = \{g'\in G \ / \ g' \in gH\} = gH$.
La classe de g pour la relation R_H est l'ensemble
$\{g'\in G \ / \ g'g^{-1} \in H\} = \{g'\in G \ / \ g' \in Hg\} = Hg$.
♢

Définition *La classe gH est appelée classe à gauche de g modulo H et la classe Hg est appelée classse à droite de g modulo H.*
On note $(G/H)_g$ (respectivement $(G/H)_d$) l'ensemble quotient de G par la relation ${}_HR$ (respectivement R_H).

Remarques *1)Si H=G alors ${}_HR$ et R_H sont la relation triviale c'est àdire, pour tout couple (g,g') d'éléments de G, g_HRg' et $g'R_Hg$.*
2)Si H=$\{1\}$ alors tout élément de G n'est en relation qu'avec lui même pour les relations ${}_HR$ et R_H

3.1.2 Théorème de Lagrange

Soient G un groupe et H un sous-groupe.

Définition *On appelle indice de H dans G, et on note $[G : H]$, le nombre de classes d'équivalences pour la relation ${}_HR$.*

Remarques *1)$[G : G]$=1.*
2)Si G est fini, $[G : \{1\}] = |G|$.

Proposition 3.1.4 (Formule des indices)*Soit K un sous-groupe de H.*
$[G : K]$ est fini si et seulement si $[G : H]$ et $[H : K]$ sont finis.
Dans ce cas, $[G : K] = [G : H][H : K]$.

Démonstration *Supposons $[G : K]$ fini.*
Comme H est inclus dans G, $[H : K] \leq [G : K]$ et $[H : K]$ est fini.
Si g et g' appartiennent à G et sont dans la même classe d'équivalence pour la relation ${}_KR$, alors g et g' sont dans la même classe d'équivalence pour la relation ${}_HR$ puisque H contient K.
D'où la correspondance $\varphi : gK \to gH$ est une application des classes de la relation ${}_KR$ vers les classes de la relation ${}_HR$. Cette application est surjective (puisque chaque gH admet la classe gK comme antécédent) donc $[G : H] \leq [G : K]$ et $[G : H]$ est fini.
Supposons r=$[G : H]$ et s=$[H : K]$ finis.
Soient $\{g_1, \ldots, g_r\}$ un système de représentants des classes de la relation ${}_HR$ sur G et $\{h_1, \ldots, h_s\}$ un système de représentants des classes de la relation ${}_KR$ sur H.
Montrons que $\{g_ih_j\ 1\leq i\leq r,\ 1\leq j\leq s\}$ est un système de représentants des classes de la relation ${}_KR$ sur G.
Puisque les classes d'équivalences $g_1H, \ldots, g_rH$ forment une partition de G, pour tout élément de G, il existe un unique i compris entre 1 et r tel que $g\in g_iH$.
$g\in g_iH$ donc il existe un unique h appartenant à H tel que $g=g_ih$.
Mais, les classes d'équivalences $h_1K, \ldots, h_sK$ forment une partition de H, donc il existe un unique j appartenant compris entre 1 et s tel que $h \in h_jK$.
$h\in h_jK$ donc il existe un unique k appartenant à K tel que $h=h_jk$.

Finalement, il existe un unique i compris entre 1 et r, un unique j compris entre 1 et s et un unique k appartenant à K tel que g=$g_i h_j k$.
Par conséquent, l'ensemble $\{g_i h_j K\ 1 \leq i \leq r,\ 1 \leq j \leq s\}$ est une partition de G.
D'où, $\{g_i h_j\ 1 \leq i \leq r,\ 1 \leq j \leq s\}$ est un système de représentants des classes de la relation ${}_K R$ sur G et, par suite, $[G : K] = [G : H][H : K]$ est fini. $\diamondsuit$

Proposition 3.1.5 (Formule de Lagrange) *Si G est fini, $|G| = [G : H]|H|$*

Démonstration *Les $[G : H]$ classes d'équivalences de la relation ${}_H R$ forment une partition de G et sont de cardinal $|H|$ donc $|G| = [G : H]|H|$.* $\diamondsuit$

Remarque *On peut aussi utiliser la Formule des indices en prenant H=$\{1\}$ et K=H.*

Le théorème suivant est très utilisé en Théorie des groupes.

Théorème 3.1.6 (Théorème de Lagrange) *Dans un groupe fini, l'ordre de tout sous-groupe divise l'ordre du groupe.*

Démonstration *Découle directement de la Formule de Lagrange.* $\diamondsuit$

Corollaire 3.1.7 *Dans un groupe fini, l'ordre de tout élément divise l'ordre du groupe.*

Démonstration *L'ordre d'un élément est égal à l'ordre du sous-groupe qu'il engendre donc il divise l'ordre du groupe d'après le Corollaire précédent.* $\diamondsuit$

Corollaire 3.1.8 *Soit G un groupe fini d'ordre n.*
Alors, quel que soit l'élément g de G, $g^n = 1$.

Démonstration *D'après le Corollaire précédent o(x) divise n donc il existe un entier m tel que n=o(x)m.*
D'où,

$$\begin{aligned} g^n &= g^{o(x)m} \\ &= (g^{o(x)})^m \\ &= 1^m \\ &= 1. \end{aligned}$$

$\diamondsuit$

Corollaire 3.1.9 *Un groupe d'ordre un nombre premier est un groupe cyclique ne possèdant pas de sous-groupes propres.*

Démonstration *Soit $|G|=p$ avec p premier.*
Soit g un élément du groupe, différent de 1 (g existe car $|G|>1$).
D'après le Corollaire 3.1.7, l'ordre de g, o(g), divise $|G|=p$.
Mais p est premier, donc $o(g)=p$ ($o(g)\neq 1$ car $g\neq 1$).
D'où, par définition, $|<g>|=o(g)=p$ et par conséquent $<g>=G$.
G est donc cyclique.
Soit H un sous-groupe de G.
D'après le Théorème de lagrange, $|H|$ divise p.
Or p est un nombre premier donc $|H|=1$ ou $|H|=p$.
D'où, $H=\{1\}$ ou $H=G$. $\diamondsuit$

3.1.3 Sous-groupes normaux

Soient G un groupe et H un sous-groupe normal de G.

Définition *On dit que H est un sous-groupe <u>normal</u> (ou distingué) de G, et on note $H \lhd G$, si ${}_HR=R_H$.*

Remarques *1)G et $\{1\}$ sont des sous-groupes normaux de G.*
2)Si G est commutatif alors tout sous-groupe de G est normal dans G.

Proposition 3.1.10 *Si H est d'indice 2 dans G alors H est normal dans G.*

Démonstration *Comme H est d'indice 2 dans G, il y a deux classes à gauche : H et gH avec g n'appartenant pas à H, et deux classes à droite : H et Hg' avec g' n'appartenant pas à H.*
Il suffit donc de montrer que gH=Hg' : g' appartient à G mais pas à H donc g' appartient à gH (les classes forment une partition de G).
D'où il existe un élément h de H tel que g'=gh.
Par conséquent, pour tout h' de H, $gh'=ghh^{-1}h' \in g'H$.
gH est donc inclus dans Hg'.
Or ces deux ensembles ont le même cardinal ($|H|$) donc gH=g'H.
Les classes à gauche et à droite sont égales donc ${}_HR=R_H$ et par conséquent H est normal dans G. $\diamondsuit$

Proposition 3.1.11 *H est normal dans G si et seulement si pour tout élément g de G et pour tout élément h de H, ghg^{-1} appartient à H.*

Démonstration *($\Rightarrow$) On suppose que H est normal dans G.*
On a alors ${}_HR=R_H$ c'est à dire les classes d'équivalences de ${}_HR$ sont identiques à celles de R_H.
Par conséquent, pour tout élément g de G, gH=Hg d'après la Propsition 3.1.3.
D'où pour tout élément h de H, gh appartient à Hg c'est à dire ghg^{-1} appartient à H.

($\Leftarrow$) On suppose que pour tout élément g de G et pour tout élément h de H, ghg^{-1} appartient à H.
On a alors gHg^{-1} inclus dans H c'est à dire gH inclus dans Hg.
Mais gHg^{-1} inclus dans H entraîne aussi que H est inclus dans $g^{-1}Hg$ pour tout g de G. Mais cette propriété étant vraie pour tout g de G et l'application qui associe à un élément de G son inverse étant bijective, on a la propriété : H inclus dans gHg^{-1} c'est à dire Hg inclus dans gH.
D'où, pour tout élément g de G, gH=Hg et les relations ${}_HR$ et R_H sont donc identiques.
H est par conséquent normal dans G. $\diamondsuit$

Remarque *Pour montrer qu'un sous-groupe est normal dans un groupe, on utilise la caractérisation donnée par cette Proposition.*

Proposition 3.1.12 *On suppose que H est normal dans G.*
Alors, H est normal dans tout sous-groupe de G contenant H.

Démonstration *Soit K un sous-groupe de G contenant H.*
Comme K contient H, H est un sous-groupe de K.
Pour tout élément g de G et pour tout élément h de H, ghg^{-1} appartient à H.
Mais K étant inclus dans G, pour tout k appartenant à K, khk^{-1} est inclus dans H c'est à dire H est normal dans K. $\diamondsuit$

Remarque *! Si H est un sous-groupe normal de K et K un sous-groupe normal de G alors H n'est pas forcément normal dans G (la normalité n'est pas transitive) !*

Terminons par une définition :

Définition *Un groupe G est simple si il ne contient pas de sous-groupe normal non trivial.*

Exemple *Tout groupe d'ordre un nombre premier est simple.*

3.2 Groupes quotients

Si N est un sous-groupe normal d'un groupe G alors on peut munir l'ensemble quotient de G par la relation R_N ($= {}_NR$), c'est à dire l'ensemble des classes d'équivalences de cette relation, d'une structure de groupes.

3.2.1 Loi et groupe quotient

Soient G un groupe et N un sous-groupe normal de G.

Notations *On note par G/N l'ensemble quotient de G par la relation ${}_NR = R_N$.*
On note par π la surjection canonique de G sur G/N c'est à dire l'application qui à tout élément g de G associe sa classe d'équivalence.

Remarque *Soient g et g' appartenant à G.*
$\pi(g) = \pi(g')$ si et seulement si $g^{-1}g' \in N$.

Proposition 3.2.1 *Il existe une loi interne et une seule sur G/N qui permette à π de vérifier la propriété d'homomorphie sur G/N c'est à dire $\pi(gg') = \pi(g)\pi(g')$ pour tout couple (g,g') d'éléments de G.*

Remarque *G/N n'ayant pas encore de structure de groupe, on ne peut pas dire que π est un homorphisme de groupes.*

Démonstration *π étant surjective, tout élément de G/N s'écrit sous la forme $\pi(g)$ avec g dans G.*
On peut donc définir une correspondance f de $G/N \times G/N$ dans G/N par :
$f((\pi(g), \pi(g'))) = \pi(gg')$.
Dans la suite, on écrit $\pi(g)\pi(g')$ à la place de $f((\pi(g), \pi(g')))$.
On a donc $\pi(g)\pi(g') = \pi(g)\pi(g')$ par définition de f.
Montrons que cette correspondance est une loi interne sur G/N c'est à dire une application : soient g_1, g_2, g'_1 et g'_2 appartenant à G et tels que
$(\pi(g_1), \pi(g_2)) = (\pi(g'_1), \pi(g'_2))$.
On a alors $\pi(g_1) = \pi(g'_1))$ c'est à dire ${g_1}^{-1}g'_1 = n \in N$ et $\pi(g_2) = \pi(g'_2)$ c'est à dire ${g_2}^{-1}g'_2 = n' \in N$.
On a alors

$$\begin{aligned} {g_2}^{-1}{g_1}^{-1}g'_1g'_2 &= {g_2}^{-1}ng'_2 \; n \in N \\ &= ({g_2}^{-1}ng_2){g_2}^{-1}g'_2 \\ &= n'{g_2}^{-1}g'_2 \; n' \in N \; carN \lhd G \\ &= n'n" \; n', \; n" \in N. \end{aligned}$$

${g_2}^{-1}{g_1}^{-1}g'_1g'_2$ appartient à N c'est à dire $\pi(g_1)\pi(g_2) = \pi(g'_1)\pi(g'_2)$.
On a donc bien défini une loi interne sur G/N.

Il est clair qu'avec cette loi, π vérifie la propriété d'homomorphie.
Soit $\times$ une loi interne sur G/N qui permette à π de vérifier la propriété d'homomorphie. On a alors, pour tout couple (g,g') d'éléments de G, $\times(\pi(g), \pi(g')) = \pi(g) \times \pi(g') = \pi(gg') = \pi(g)\pi(g') = .(\pi(g), \pi(g'))$.
Par conséquent, la loi $\times$ est égale à la loi définie précédemment. $\diamondsuit$

Définition *La loi, définie dans la Proposition précédente, est appelée loi quotient de G par N.*

Proposition 3.2.2 *L'ensemble G/N muni de la loi quotient est un groupe.*

Démonstration *Comme on utilise la loi quotient, π vérifie la propriété d'homomorphie. Soient g, g' et g" appartenant à G.*

$$\begin{aligned}(\pi(g)\pi(g'))\pi(g") &= \pi(gg')\pi(g") \\ &= \pi((gg')g") \\ &= \pi(g(g'g")) \text{ car } G \text{ est un groupe} \\ &= \pi(g)\pi(g'g") \\ &= \pi(g)(\pi(g')\pi(g"))\end{aligned}$$

donc la loi quotient est associative.
Pour tout élément g de G, $\pi(g)\pi(1) = \pi(g1) = \pi(g)$ et $\pi(1)\pi(g) = \pi(1g) = \pi(g)$ donc la loi quotient admet comme élément neutre $\pi(1)$ (c'est à dire N).
Pour tout élément g de G, $\pi(g)\pi(g^{-1}) = \pi(gg^{-1}) = \pi(1)$ et $\pi(g^{-1})\pi(g) = \pi(g^{-1}g) = \pi(1)$ donc tout élément de G/N admet un inverse pour la loi quotient.
D'où, l'ensemble G/N muni de la loi quotient est un groupe. $\diamondsuit$

Définition *Ce groupe est appelé groupe quotient de G par N.*

Remarques *1)π est un homomorphisme de groupes surjectif de G vers le groupe quotient G/N, de noyau N.*
Ainsi, tout sous-groupe normal est le noyau d'un homomorphisme de groupes.
Nous avons vu dans la section Sous-groupes normaux *que tout noyau d'un homomorphisme de groupes partant de G est un sous-groupe normal de G donc, un sous-groupe de G est normal si et seulement si ce sous-groupe est le noyau d'un homomorphisme de groupes ayant G comme groupe de départ.*
2)L'ordre de G/N est par définition l'indice de N dans G.
Si G est fini, on a $|G/N| = \frac{|G|}{|N|}$ d'après la Formule de Lagrange.
3)Si N=G alors $G/N=\{1_{G/N}\} = \{N\}$ et si N=$\{1\}$ alors G/N est isomorphe à G (via l'isomorphisme $(\{g\} \leftrightarrow g)$).

Exemple *On considère $G=\mathbb{Z}$ et $N=n\mathbb{Z}$ avec n non nul.*
Comme $\mathbb{Z}$ est commutatif, $n\mathbb{Z}$ est un sous-groupe normal.
Deux entiers x et y sont en relation pour la relation ${}_NR$ ssi x-y appartient à $n\mathbb{Z}$ c'est à dire x et y congrus modulo n.
On a donc bien cohérence des notations : $G/N=\mathbb{Z}/n\mathbb{Z}$.

Propriété 3.2.3 *1)Si G est cyclique alors G/N est cyclique.*
2)Si G est abélien alors G/N est abélien.

Démonstration *1)π étant surjective, le résultat découle de la Proposition 2.2.4.*
2)Soient g et g' deux éléments de G. On a

$$\begin{aligned} \pi(g)\pi(g') &= \pi(gg') \\ &= \pi(g'g) \text{ car } G \text{ est commutatif} \\ &= \pi(g')\pi(g) \end{aligned}$$

donc G/N est abélien. $\diamondsuit$

La notion de groupe quotient intervient très souvent en Théorie des groupes comme nous le verrons par la suite.

3.2.2 Sous-groupes d'un groupe quotient

Soient G un groupe, N un sous-groupe normal de G et π la surjection canonique de G dans G/N.

La proposition suivante donne l'ensemble des sous-groupes du groupe quotient G/N.

Proposition 3.2.4 *1)Les sous-groupes de G contenant N sont en bijection, par π, avec les sous-groupes de G/N.*
2)Les sous-groupes normaux de G contenant N sont en bijection, par π, avec les sous-groupes normaux de G/N.

Démonstration *1)π étant un homorphisme, π envoie un sous-groupe de G vers un sous-groupe de G/N.*
Montrons que π met en bijection l'ensemble des sous-groupes de G contenant N avec l'ensemble des sous-groupes de G/N :
Commençons par montrer que l'application π définie sur l'ensemble des sous-groupes de G contenant N est injective : Soiet H et H' deux sous-groupes de G contenant N tels que $\pi(H) = \pi(H')$.
Soit h un élément de H.
Alors, puisque $\pi(H) = \pi(H')$, il existe un élément h' de H' tel que $h^{-1}h'$ appartient à N. D'où h est appartient à h'N. Or, N est inclus dans H' donc h'N est inclus dans H'. On en déduit que H est inclus dans H'.
On montre de même que H' est inclus dans H.
D'où, H=H' et l'application π définie sur l'ensemble des sous-groupes de G contenant N est injective.
π étant un homomorphisme, l'image réciproque d'un sous-groupe de G/N est un sous-groupe de G.

Soit $\overline{H}$ un sous-groupe de G/N.
π étant surjective, $\overline{H} = \pi(\pi^{-1}(\overline{H}))$ donc $\overline{H}$ est l'image par π du sous-groupe $H=\pi^{-1}(\overline{H})$ de G.
Montrons que H contient N : $\overline{H}$ contient $1_{G/N}$ donc $H=\pi^{-1}(\overline{H})$ contient $\pi^{-1}(1_{G/N})=Ker\ \pi=N$.
D'où, l'application π est une bijection entre l'ensemble des sous-groupes de G contenant N et les sous-groupes de G/N.
2)Soit H un sous-groupe normal de G contenant N.
Alors $\overline{H} = \pi(H)$ est un sous-groupe de G/N.
Montrons que $\overline{H}$ est un sous-groupe normal :
Soient $\pi(h)$ appartenant à $\overline{H}$ ($h\in H$) et $\pi(g)$ appartenant à G/N.
$\pi(g)\pi(h)(\pi(g))^{-1} = \pi(ghg^{-1}) \in \overline{H}$ car H est normal dans G.
D'où, $\overline{H}$ est un sous-groupe normal de G/N. Soient $\overline{H}$ un sous-groupe normal de G/N et $H=\pi^{-1}(\overline{H})$.
H est un sous-groupe de G contenant N dont l'image par π est $\overline{H}$ d'après le 2).
Montrons que H est normal dans G : soient h appartenant à H et g appartenant à G.
$\pi(ghg^{-1}) = \pi(g)\pi(h)(\pi(g))^{-1}$ appartient à $\overline{H}$ car $\overline{H}$ est normal dans G/N.
D'où, ghg^{-1} appartient à $\pi^{-1}(\overline{H})=H$.
H est normal dans G. $\diamondsuit$

Exemple *Il y a 3 sous-groupes dans $\mathbb{Z}/4\mathbb{Z}$. En effet, les sous-groupes de $\mathbb{Z}/4\mathbb{Z}$ sont en bijection avec les sous-groupes de $\mathbb{Z}$ contenant $4\mathbb{Z}$.*
Or dans $\mathbb{Z}$, il n'y a que les sous-groupes $\mathbb{Z}$, $\{0\}$ et $2\mathbb{Z}$ qui contiennent $4\mathbb{Z}$.
Par conséquent, $\mathbb{Z}/4\mathbb{Z}$ a trois sous-groupes : $\pi(\mathbb{Z}) = \mathbb{Z}/4\mathbb{Z}$, $\pi(\{0\})=0$ et $\pi(2\mathbb{Z})=<\pi(2)>$.

Remarque *Si H est un sous-groupe de G, un mauvais réflexe consisterait à dire que $\pi(H)=H/N$. Or H/N n'a de sens que si H contient le sous-groupe N (N est alors un sous-groupe normal de H d'après la proposition* **??***)*

Définition *Soit H un sous-groupe de G.*
On note par NH l'ensemble $\{nh$ / $n\in N$ et $h\in H\}$.

On admet, pour l'instant, que l'ensemble NH est un sous-groupe de G. ce résultat sera démontré dans la section *Produit semi-direct*.
N est inclus dans NH puisque pour tout élément n de N, n=n1 et n1 appartient à NH.
D'où, le groupe quotient NH/N existe.

Proposition 3.2.5 *Pour tout sous-groupe H de G, $\pi(H)=NH/N$.*

Démonstration *Commençons par montrer que $\pi(H)=\pi(NH)$:*
Soient h un élément de H et n un élément de N.
Puisque N est un sous-groupe normal de G, $h^{-1}nh$ appartient à N donc $\pi(h)=\pi(nh)$ et par conséquent, $\pi(H)$ est égal à $\pi(NH)$.
On a par définition de π et par la Proposition 3.1.3, $\pi(NH)=\{\pi(nh)$ / $n\in N$, $h\in H\}=$ $\{nhN$ / $n\in N$, $h\in H\}$ = $\psi(NH)=NH/N$ où ψ est la surjection canonique de NH sur NH/N.
On a donc $\pi(H)=\pi(NH)=NH/N$. $\diamondsuit$

3.2.3 Propriété universelle du groupe quotient

Soient G un groupe, N un sous-groupe normal de G et π la surjection canonique de G dans G/N.

Proposition 3.2.6 (Propriété universelle du groupe quotient) *Soient G' un groupe et $f : G \to G'$ un homomorphisme de groupes dont le noyau contient N.*
Alors, il existe un unique homorphisme $\overline{f}$ de G/N dans G' tel que $f=\overline{f}\circ\pi$.
De plus, Ker $\overline{f}$=Ker f/N et Im $\overline{f}$=Im f.

Démonstration *Supposons que $\overline{f}$ existe.*
On a alors, pour tout $\pi(g)$ de G/N, $\overline{f}(\pi(g))=f(g)$.
D'où, comme π est surjective, $\overline{f}$ est entièrement et uniquement déterminé par $\overline{f}(\pi(g))=f(g)$.
Montrons que la correspondance $\overline{f}$ de G/N dans G' définie par $\overline{f}(\pi(g))=f(g)$ est une application : soient g_1 et g_2 appartenant à G. Si $\pi(g_1) = \pi(g_2)$ alors $\pi(g_1{g_2}^{-1})=1$ et donc $g_1{g_2}^{-1}$ appartient à N puisque Ker π=N. N étant inclus dans Ker f, on a $f(g_1{g_2}^{-1})=1$ c'est à dire $f(g_1)=f(g_2)$. D'où, $\overline{f}(\pi(g_1))=\overline{f}(\pi(g_2))$ et $\overline{f}$ est une application. Montrons que $\overline{f}$ est un homomorphisme : soient g_1 et g_2 appartenant à G.
On a

$$\begin{aligned}\overline{f}(\pi(g_1)\pi(g_2)) &= \overline{f}(\pi(g_1g_2))\\ &= f(g_1g_2)\\ &= f(g_1)f(g_2)\\ &= \overline{f}(\pi(g_1))\overline{f}(\pi(g_1))\end{aligned}$$

donc $\overline{f}$ est un homomorphisme de G dans G/N.
$\overline{f}$ est l'unique homomorphisme de G dans G/N tel que $f=\overline{f}\circ\pi$.
De plus,

$$\begin{aligned}Ker\overline{f} &= \{\pi(g) \ / \ g \in G, \ \overline{f}(\pi(g)) = 1\}\\ &= \{\pi(g) \ / \ g \in G, \ f(g) = 1\}\\ &= \pi(Kerf)\\ &= Kerf/N \ car \ N \ est \ inclus \ dans \ Kerf.\end{aligned}$$

et

$$\begin{aligned}Im\overline{f} &= \{\overline{f}(\pi(g)) \ g \in G\}\\ &= \{f(g) \ g \in G\}\\ &= Imf.\end{aligned}$$

♢

Le caractère "universel" du groupe quotient provient de la proposition suivante :

Proposition 3.2.7 *Le couple (G/N,π) est l'unique couple (H,φ), à isomorphisme près, formé d'un groupe H et d'une application surjective φ de G dans H, tel que pour tout groupe G' et tout homomorphisme f de G dans G', il existe un unique homomorphisme ψ de H dans G' vérifiant f=ψ ∘ φ.*

Démonstration *Supposons qu'il existe un couple (H,φ) vérifiant la condition (U) : pour tout groupe G' et tout homomorphisme f de G dans G', il existe un unique homomorphisme ψ de H dans G' vérifiant f=ψ ∘ φ (1).*
Si on prend G'=G/N et f=π, il existe un homomorphisme ψ de H dans G/N tel que π = ψ ∘ φ (1).
D'après la Proposition précédente, il existe un homomorphisme $\overline{\varphi}$ de G/N dans H tel que φ = $\overline{\psi}$ ∘ π (2).
Montrons que ψ est un isomorphisme d'inverse $\overline{\varphi}$: $\overline{\varphi} \circ \psi$ va de H dans H et vérifie φ = ($\overline{\varphi} \circ \psi$) ∘ φ d'après les égalités (1) et (2).
Or l'identité sur H est un homomorphisme vérifiant l'égalité φ = $Id_H \circ \varphi$. D'où, comme on a unicité dans la condition (U), on a $\overline{\varphi} \circ \psi = Id_H$.
De même, ψ ∘ $\overline{\varphi}$ et Id_G sont deux homomorphsimes f de G/N dans G/N vérifiant π = f ∘ π.
D'où, comme on a unicité dans la condition (U), on a $\psi \circ \overline{\varphi} = Id_G$.
Ainsi, H est isomorphe à G/N par l'isomorphisme ψ d'inverse $\overline{\varphi}$ et φ = $\overline{\varphi} \circ \pi$ d'après l'égalité (1). ♢

On a ainsi une caractérisation des groupes quotients.

Proposition 3.2.8 *Soient G' un groupe, N' un sous-groupe normal de G', p la surjection canonique de G' sur G'/N' et f : G → G' un homomorphisme tel que f(N) est inclus dans N'.*
Alors, il existe un unique homorphisme $\overline{f}$ de G/N dans G'/N' tel que p∘f=$\overline{f}$ ∘ π.

Démonstration *p et f étant des homomorphismes, l'application p∘f de G dans G'/N' est un homomorphisme.*
Comme f(N) est inclus dans N' et comme N' est le noyau de p, N est inclus dans le noyau de p∘f.
D'où, d'après la Propriété universelle du groupe quotient, il existe un unique homomorphisme $\overline{f}$ de G/N dans G'/N' tel que $\overline{f} \circ \pi$ = p∘f. ♢

On a ainsi "quotienter" des homomorphismes afin de travailler avec les groupes quotients, ce qui peut être plus pratique car les groupes quotients ont des ordres inférieurs aux ordres des groupes quotientés.

3.3 Théorèmes d'isomorphisme

Nous allons démontrer trois théorèmes dûs à Emmy Noether.

3.3.1 Premier Théorème d'isomorphisme

Soient G et G' deux groupes et f : G $\rightarrow$ G' un homormorphisme de groupes.
On rappelle que Ker f est un sous-groupe de G et que par conséquent, le groupe quotient G/Ker f existe.

Le théorème suivant est l'un des plus importants et des plus utilisés de la théorie des groupes.

Théorème 3.3.1 (Premier Théorème d'isomorphisme)
G/Ker f est isomorphe à Im f.

Démonstration *D'après la Propriété universelle du groupe quotient (Proposition 3.2.6), il existe un homomorphisme $\overline{f}$ de G/Ker f dans G'.*
De plus, Ker $\overline{f}$=Ker f/Ker f=$\{1\}$ et Im $\overline{f}$=Im f.
On en déduit que $\overline{f}$ est injective et surjective de G/Ker f vers Im f.
D'où, $\overline{f}$ est un isomorphisme entre G/Ker f et Im f. $\diamondsuit$

3.3.2 Deuxième Théorème d'isomorphisme

Soient G, H un sous-groupe de G et N un sous-groupe normal de G.

On rappelle que l'on note par NH l'ensemble {nh / n$\in$N et h$\in$H}. On démontrera dans la section *Produit semi-direct* que l'ensemble NH est un sous-groupe de G.
On rappelle également que N est un sous-groupe normal de NH et que par conséquent, le groupe quotient NH/N existe.

Lemme *H$\cap$N est un sous-groupe normal de H.*

Démonstration *Puisque H et N sont des sous-groupes de G, H$\cap$N est un sous-groupe de G. H$\cap$N étant inclus dans H, H$\cap$N est un sous-groupe de H.*
Soient n appartenant à H$\cap$N et h appartenant à H.
Alors, hnh^{-1} appartient à H car H est un sous-groupe de G et hnh^{-1} appartient à N car N est un sous-groupe normal de G.
D'où, H$\cap$N est un sous-groupe normal de H. $\diamondsuit$

Théorème 3.3.2 (Deuxième Théorème d'isomorphisme)
NH/N est isomorphe à H/H∩N.

Démonstration *D'après le Lemme précédent, le groupe quotient H/H∩N existe.*
Soient π la surjection canonique de G vers G/N et ϕ la restriction de π à H.
π étant un homomorphisme, ϕ est un homomorphisme.
D'après la Proposition 3.2.5, l'image de ϕ est $\pi(H)$=NH/N.
Cherchons le noyau de ϕ :

$$\begin{aligned} Ker\ \phi &= \{h \in H \ / \ \phi(h) = N\} \\ &= \{h \in H \ / \ hN = N\} \\ &= \{h \in H \ / \ h \in N\} \\ &= H \cap N. \end{aligned}$$

D'où, d'après le Premier Théorème d'isomorphisme, H/H∩N est isomorphe à NH/H.
♢

3.3.3 Troisième Théorème d'isomorphisme

Soient G, H un sous-groupe normal de G et K un sous-groupe normal de G inclus dans H.

Lemme *H/K est un sous-groupe normal de G/K.*

Démonstration *Soit π la surjection canonique de G sur G/K.*
Puisque K est un sous-groupe normal de G inclus dans H, on a, d'après la Proposition 3.2.5, π(H)=H/K.
On en déduit le lemme d'après la Proposition 3.2.5. ♢

Théorème 3.3.3 (Troisième Théorème d'isomorphisme)
(G/K)/(H/K) est isomorphe à G/H.

Démonstration *D'après le Lemme précédent, le groupe quotient (G/K)/(H/K) existe.*
Soit ϕ la correspondance de G/K dans G/H définie par ϕ(gK)=gH pour tout g de G.
Montrons que ϕ est une application : soient g et g' deux éléments de G vérifiant que gK=g'K.
On a alors $g^{-1}g'$ appartenant à K. Mais K est inclus dans H donc $g^{-1}g'$ appartenant à H. D'où, gH=g'H et donc ϕ(gK)=ϕ(g'K).
ϕ est une application.

Montrons que ϕ est un homomorphisme : soient g et g' appartenant à G.

$$\begin{aligned} \phi(gKg'K) &= \phi(gg'K) \\ &= gg'H \\ &= gHg'H \\ &= \phi(gK)\phi(g'K) \end{aligned}$$

donc ϕ est un homomorphisme de groupes.
ϕ est clairement surjectif.
Cherchons le noyau de ϕ :

$$\begin{aligned} Ker\ \phi &= \{gK\ g \in G\ /\ \phi(gK) = H\} \\ &= \{gK\ g \in G\ /\ gH = H\} \\ &= \{gK\ g \in G\ /\ g \in H\} \\ &= \{hK\ h \in H\} \\ &= H/K. \end{aligned}$$

D'où, d'après le Premier Théorème d'isomorphisme, (G/K)/(H/K) est isomorphe à G/H. $\diamondsuit$

3.4 Produit semi-direct

Commençons par étudier les ensembles de la forme HK où H et K sont deux sous-groupes d'un groupe donné :

3.4.1 Produit de sous-groupes

Soient G un groupe et H et K deux sous-groupes de G.

Définition *On note par HK l'ensemble* $\{hk \ / \ h \in H \text{ et } k \in K\}$.

Remarque *H et K sont inclus dans HK puisque pour tout élément h de H et pour tout élément k de K,* $h=h1 \in HK$ *et* $k=1k \in HK$.

Les deux questions qu'on peut se poser sur l'ensemble HK sont les suivantes :
"A t'on KH=HK ?" et "HK est-il un sous-groupe de G ?".
La proposition suivante montre que ces deux questions ont les mêmes réponses :

Proposition 3.4.1 *KH=HK si et seulement si HK est un sous-groupe de G .*

Démonstration *(⇒) On suppose que KH=HK.*
H et K n'étant pas vides, HK n'est pas vide.
Soient (h,h') un couple d'éléments de H et (k,k') un couple d'éléments de K.
Puisque KH=HK, kh' appartient à HK.
Il existe donc un élément h" de H et un élément k" de K tels que kh'=h"k".
D'où, hkh'k'=hh"k"k' appartient à HK.
$(hk)^{-1} = k^{-1}h^{-1}$ *appartient à KH puisque K et H sont des sous-groupes de G.*
D'où, puisque KH=HK, $(hk)^{-1}$ *appartient à HK.*
HK est par conséquent un sous-groupe de G.
(⇐) On suppose que HK est un sous-groupe de G.
Soient h un élément de H et k un élément de K.
H et K sont des sous-groupes de G donc h^{-1} *appartient à H et* k^{-1} *à K.*
HK étant un sous-groupe de G, $kh=(h^{-1}k^{-1})^{-1}$ *appartient à HK.*
On en déduit que KH est inclus dans HK.
Soit x un élément de HK. Puisque HK est un sous-groupe de G, x^{-1} *appartient aussi à HK. Par conséquent, il existe un élément h de H et un élément k de K tels que* $x^{-1}=hk$. *On en déduit que* $x=(x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1}$.
$k^{-1}h^{-1}$ *étant des sous-groupes de G,* $k^{-1}h^{-1}$ *appartient à KH donc x appartient à KH.*
D'où, HK est inclus dans KH.
HK=KH. ♢

Les trois corollaires suivants donnent des conditions suffisantes pour que HK soit un sous-groupe de G.

Corollaire 3.4.2 *Si G est abélien alors HK est un sous-groupe de G.*

Démonstration *Puisque G est abélien, on a HK=KH donc HK est un sous-groupe de G d'après la Proposition précédente.* $\diamondsuit$

Définition *On dit que K <u>normalise</u> H si pour tout k de K et pour tout h de H, khk^{-1} appartient à H.*

Corollaire 3.4.3 *Si K normalise H alors HK est un sous-groupe de G.*

Démonstration *Nous allons montrer que KH=HK.*
Soient k un élément de K et h un élément de H.
Puisque K normalise H, khk^{-1} appartient à H. Il existe donc un élément h' de H tel que khk^{-1}=h'. On en déduit que kh=h'k appartient à HK et par conséquent, KH est inclus dans HK.
K normalisant H, $k^{-1}hk$ appartient à H. Il existe donc un élément h' de H tel que $k^{-1}hk$=h'. On en déduit que hk=kh' appartient à KH et par conséquent, HK est inclus dans KH.
D'où, KH=HK et HK est un sous-groupe de G d'après la Proposition 3.4.1. $\diamondsuit$

Remarque *HK étant un sous-groupe de G, HK est un groupe.*
Dans le cas où K normalise H, la loi de HK est : hk.h'k'=(hkhk^{-1})(kk').
Dans le cas particulier où G est abélien, la loi de HK est hk.h'k'=hh'kk'.

Corollaire 3.4.4 *Si H est un sous-groupe normal de G alors HK est un sous-groupe de G.*

Démonstration *Puisque H est normal dans G, H est normalisé par n'importe quel sous-groupe de G et en particulier par K.*
D'où, d'après le Corollaire précédent, HK est un sous-groupe de G. $\diamondsuit$

Proposition 3.4.5 *On suppose que K normalise H.*
Alors, le sous-groupe HK est le sous-groupe de G engendré par H$\cup$K.

Démonstration *H et K sont inclus dans HK donc H$\cup$K est inclus dans HK.*
D'où, puisque HK est un sous-groupe de G, <H$\cup$K> est inclus dans HK.
Pour tout élément h de H et pour tout élément k de K, hk appartient à <H$\cup$K>= $\{g_1 \ldots g_n \ / \ n \in \mathbb{N}, \forall 1 \leq i \leq n \ g_i \in H \cup K \text{ ou } {g_i}^{-1} \in H \cup K\}$ *donc HK est inclus dans <H$\cup$K>. D'où, HK=<H$\cup$K>.* $\diamondsuit$

Proposition 3.4.6 *Si H est un sous-groupe normal de G et si H et K sont finis alors le groupe HK est un groupe fini d'ordre* $\frac{|H||K|}{|H \cap K|}$.

Démonstration *H étant un sous-groupe normal de G, on peut appliquer le Deuxième Théorème d'isomorphisme : HK/K est isomorphe à H/H∩K.*
H et K étant finis, H∩K est fini et par conséquent, HK est un groupe fini d'ordre $\frac{|H||K|}{|H\cap K|}$. ♢

Proposition 3.4.7 *Si H et K sont normaux dans G alors HK est un sous-groupe normal de G.*

Démonstration *Comme H est normal dans G, HK est un sous-groupe de G d'après le Corollaire 3.4.4.*
Soient g appartenant à G et hk appartenant à HK.
On a $ghkg^{-1} = ghg^{-1}gkg^{-1}$.
H et K étant normaux dans G, ghg^{-1} *appartient à H et* gkg^{-1} *appartient à K donc* $ghkg^{-1} = ghg^{-1}gkg^{-1}$ *appartient à HK.*
Par conséquent, HK est un sous-groupe normal de G. ♢

Proposition 3.4.8 *Si H et K sont normaux dans G et si H∩K=*$\{1\}$ *alors HK est isomorphe à H×K.*

Démonstration *Puisque H est normal dans G, HK est un groupe d'après le Corollaire 3.4.4.*
Montrons que pour tout élément (h,k) de $H \times K$, *hk=kh : H étant normal dans G,* khk^{-1} *appartient à H donc,* $hkh^{-1}k^{-1}$ *appartient à H.*
De même, puisque K est normal dans G, hkh^{-1} *appartient à K et par conséquent,* $hkh^{-1}k^{-1}$ *est un élément de K.*
D'où, $hkh^{-1}k^{-1}$ *appartient à H∩K. Or H∩K=*$\{1\}$, *donc* $hkh^{-1}k^{-1}$*=1 c'est à dire hk=kh.*
Soit f l'application de $H \times K$ *dans HK définie par f(h,k)=hk.*
Montrons que f est un homomorphisme : soient (h,k) et (h',k') appartenant à $H \times K$. *On a*

$$\begin{aligned} f((h,k)(h',k')) &= f(hh',kk') \\ &= hh'kk' \\ &= hkh'k' \\ &= f(h,k)f(h',k') \end{aligned}$$

donc f est un homomorphisme de groupes.
Montrons que f est injective : soit (h,k) un élément de $H \times K$, *appartenant au noyau de f. Alors, f(h,k)=hk=1 et donc* $h=k^{-1}$.
D'où, h appartient à H∩K=$\{1\}$. *On en déduit que h=1 et* $k=h^{-1}=1$.
On a (h,k)=(1,1) donc Ker f=$\{1\}$ *et par conséquent, f est injective.*
f est clairement surjective puisque si h appartient à H et k à K, hk=f(h,k).
D'où, f est un isomorphisme entre $H \times K$ *et HK.* ♢

3.4.2 Produit semi-direct de sous-groupes

Soient G un groupe, H un sous-groupe normal de G et K un sous-groupe de G.

On a vu, dans la Section précédente, que dans ce cas, HK est un sous-groupe de G.

Définition *On dit que G est produit semi-direct des sous-groupes H et K si G=HK et H∩K={1}. Dans ce cas, on note G=H⋊K ou K⋉H.*

Proposition 3.4.9 *Soient G, H et K des groupes finis, ϕ un homomorphisme de H dans G et θ un homomorphisme de G dans K vérifiant Ker θ=Im ϕ.*
On suppose qu'il existe un homomorphisme σ de K dans G, tel que $\theta \circ \sigma = Id$
(σ est alors appelé section au dessus de θ).
Alors, G est le produit semi-direct de Im $\phi = \phi(H)$ par Im $\sigma = \sigma(K)$.

Démonstration *ϕ et σ étant des homomorphismes de groupes, $\phi(H)$ et $\sigma(K)$ sont des sous-groupes de G.*
$\phi(H)$=Im ϕ=Ker θ donc $\phi(H)$ est un sous-groupe normal de G.
Montrons que $\phi(H) \cap \sigma(K)$ est réduit à $\{1\}$:
Soit $\phi(h)=\sigma(k)$ appartenant à $\phi(H) \cap \sigma(K)$.
Comme Ker θ=Im ϕ, $\theta(\phi(h))$=1.
Mais σ étant une section au dessus de θ, $\theta(\phi(h)) = \theta(\sigma(k))=k$ donc k=1 et par conséquent $\phi(h)=\sigma(k)=\sigma(1)=1$.
$\phi(H) \cap \sigma(K)$ est réduit à $\{1\}$.
Montrons que $G=\phi(H)\sigma(K)$:
Puisque Im ϕ=Ker θ, $G/\phi(H)=G/Ker\ \theta$.
D'où, d'aprés le Premier Théorème d'isomorphisme, $G/\phi(H)$ est isomorphe à Im θ.
On en déduit que $|G| = |\phi(H)||Im\,\theta|$.
Comme $\theta \circ \sigma = Id$, θ est surjective (si k appartient à K, $k=\theta(\sigma(k))$) donc
Im θ=K.
Comme $\theta \circ \sigma = Id$, σ est injective (si $\sigma(k) = \sigma(k')$ alors $k=\theta(\sigma(k)) = \theta(\sigma(k'))=k'$) donc
K/Ker σ est isomorphe à K.
D'où, d'après le Premier Théorème d'isomorphisme, K est isomorphe à Im $\sigma = \sigma(K)$.
On en déduit que $|Im\ \theta| = |K| = |Im\ \sigma| = |\sigma(K)|$ et par conséquent
$|G| = |\phi(H)||\sigma(K)|$.
Puisque $\phi(H)$=Im ϕ=Ker θ, $\phi(H)$ est un sous-groupe normal de G.
D'où, d'après la Proposition 3.4.6, $|\phi(H)\sigma(K)| = |\phi(H)||\sigma(K)|$.
On en déduit que $|G| = |\phi(H)\sigma(K)|$.
$\phi(H)\sigma(K)$ est inclus dans G et $|G| = |\phi(H)\sigma(K)|$ donc $G=\phi(H)\sigma(K)$.
On en déduit que G est le produit semi-direct de $\phi(H)$ par $\sigma(K)$. ♢

Corollaire 3.4.10 *Soient H et K deux groupes.*
Alors, H×K est le produit semi-direct de H×{1} par {1}×K.

Démonstration *On prend, dans la Proposition précédente, $\phi=\iota_H$ l'injection canonique de H×{1} dans G, θ(g)=(1,p(g)) où p est la projection canonique de G sur K et $\sigma=\iota_K$ l'injection canonique de {1}×K dans G.* ♢

3.4.3 Produit semi-direct de groupes

Soient H et K deux groupes.
Soit ϕ un homomorphisme de K dans Aut(H).
Pour tout k appartenant à K, on note ϕ_kà la place ϕ(k).
Puisque ϕ_k(h') appartient à h pour tout élément h' de H, on peut définir une loi interne sur H×K en posant (h,k)(h',k')=(hϕ_k(h'),kk') pour tout couple (h,h') d'éléments de H et pour tout élément k de K.

Proposition 3.4.11 *L'ensemble H×K muni de la loi interne (h,k)(h',k')=(hϕ_k(h'),kk') est un groupe.*

Démonstration *Montrons que la loi . est associative : soient h, h' et h" appartenant à H et k, k' et k" appartenant à K.*
D'une part,

$$\begin{aligned}((h,k)(h',k'))(h",k") &= (h\phi_k(h'),kk')(h",k") \\ &= (h\phi_k(h')\phi_{kk'}(h"),kk'k") \\ &= (h\phi_k(h')\phi_k(\phi_{k'}(h")),kk'k") \text{ car } \phi \text{ est un homomorphisme.}\end{aligned}$$

D'autre part,

$$\begin{aligned}(h,k)((h',k')(h",k")) &= (h,k)(h'\phi_{k'}(h"),k'k") \\ &= (h\phi_k(h'\phi_{k'}(h")),kk'k") \\ &= (h\phi_k(h')\phi_k(\phi_{k'}(h")),kk'k") \text{ car } \phi_k \text{ est un homomorphisme.}\end{aligned}$$

D'où, ((h,k)(h',k'))(h",k")=(h,k)((h',k')(h",k")) et la loi est asoociative.
Pour tout élément h de H et pour tout élément k de K, (h,k)(1,1)=(hϕ_k(1),k1)=(h,Id(1),k)=(h,k) et (1,1)(h,k)=(ϕ_1(h),k)=(Id(h),k)=(h,k) car ϕ est un homomorphisme donc la loi . admet l'élément (1,1) comme élément neutre.
Soient h appartenant à H et k appartenant à K.
Comme ϕ_k est bijective, il existe un élément h' de H tel que ϕ_k(h')=h^{-1}.
D'où, $(h,k)(h',k^{-1}) = (hh^{-1},kk^{-1})$=(1,1).
Comme ϕ est un homomorphisme, ${\phi_k}^{-1} = \phi_{k^{-1}}$. D'où, $\phi_{k^{-1}}(h^{-1})$=h'.
$\phi_{k^{-1}}$ est un homomorphisme donc $\phi_{k^{-1}}(h) = \phi_{k^{-1}}((h^{-1})^{-1}) = \phi_{k^{-1}}(h^{-1})^{-1} = h'^{-1}$.
On en déduit que $(h',k^{-1})(h,k) = (h'h'^{-1},k^{-1}k)$=(1,1).
D'où, (h,k) admet $(\phi_{k^{-1}}(h^{-1}),k^{-1})$ comme inverse.
On en déduit que H×K est un groupe pour la loi (h,k)(h',k')=(hϕ_k(h'),kk'). ♢

Définition *Le groupe H×K muni de la loi (h,k)(h',k')=(hϕ_k(h'),kk') est appelé produit semi-direct de H par K relativement à ϕ et est noté $H\rtimes_\phi K$.*

Proposition 3.4.12 *Soient H'=H×{1} et K'={1}×K.*
Alors, H⋊K est le produit semi-direct de H' par K'.

Démonstration *H' n'est pas vide puisque (1,1) appartient à H'.*
Soient (h,1) et (h',1) appartenant à H.
On a

$$\begin{aligned}(h,1)(h',1)^{-1} &= (h,1)(\phi_{1^{-1}}(h'^{-1}),1^{-1})\\ &= (h,1)(Id(h'^{-1}),1)\\ &= (h,1)(h'^{-1},1)\\ &= (h\phi_1(h'^{-1}),1)\\ &= (hId(h'^{-1}),1)\\ &= (hh'^{-1},1)\end{aligned}$$

donc $(h,1)(h',1)^{-1}$ *appartient à H' et par conséquent, H' est un sous-groupe de* $H\rtimes K$.
Soit (x,1) appartenant à H' et (h,k) appartenant à $H\rtimes K$.
On a

$$\begin{aligned}(h,k)(x,1)(h,k)^{-1} &= (h\phi_k(x),k)(\phi_{k^{-1}}(h^{-1}),k^{-1})\\ &= (h\phi_k(x)\phi_k(\phi_{k^{-1}}(h^{-1})),kk^{-1})\\ &= (h\phi_k(x)\phi_{kk^{-1}}(h^{-1}),1)\\ &= (h\phi_k(x)Id(h^{-1}),1)\\ &= (h\phi_k(x)h^{-1},1).\end{aligned}$$

Comme $\phi_k(x)$ *appartient à H par définition de* ϕ, $h\phi_k(x)h^{-1}$ *appartient à h et par conséquent,* $(h\phi_k(x)h^{-1},1)$ *appartient à H'.*
D'où, H' est un sous-groupe normal de $H\rtimes K$.
K' n'est pas vide puisque (1,1) appartient à K'.
Soient (1,k) et (1,k') appartenant à K'.
On a

$$\begin{aligned}(1,k)(1,k')^{-1} &= (1,k)(\phi_{k'^{-1}}(1),k'^{-1})\\ &= (1,k)(1,k'^{-1})\\ &= (1\phi_k(1),kk'^{-1})\\ &= (1,kk'^{-1}).\end{aligned}$$

donc $(1,k)(1,k')^{-1}$ *et par conséquent, K' est un sous-groupe de* $H\rtimes K$.
Il est clair que $H'\cap K' = \{(1,1)\}$.
D'après la Proposition 3.4.6, $|H'K'| = \frac{|H'||K'|}{|H'\cap K'|} = |H||K| = |H\times K| = |H\rtimes K|$ *donc* $H\rtimes K = H'K'$. *D'où,* $H\rtimes K$ *est le produit semi-direct de H' par K'.* $\diamondsuit$

Proposition 3.4.13 *Soient H' un groupe isomorphe à H par un isomorphisme* σ *et K' un groupe isomorphe à K par un isomorphisme* θ.
Soit ϕ *l'application de K' dans* $\{f : H' \to H'\}$ *définie par* $\phi_{k'}(h') = \sigma^{-1}(\phi_{\theta(k')}(\sigma(h')))$ *où on a posé* $\phi_{k'} = \phi(k')$.
Alors, ϕ *est un homomophisme de K' dans Aut(H') et* $H'\rtimes_\phi K'$ *est isomorphe à* $H\rtimes_\phi K$.

Démonstration *Montrons que pour tout k' de K', $\phi_{k'}$ est un automorphisme de H' : Soient h' et h" appartenant à H'. On a*

$$\begin{aligned}
\phi'_k(h'h") &= \sigma^{-1}(\phi_{\theta(k')}(\sigma(h'h"))) \\
&= \sigma^{-1}(\phi_{\theta(k')}(\sigma(h')\sigma(h"))) \text{ car } \sigma \text{ est un homomorphisme} \\
&= \sigma^{-1}(\phi_{\theta(k')}(\sigma(h'))\phi_{\theta(k')}(\sigma(h")) \text{ car } \phi_{\theta(k')} \text{ est un homomorphisme} \\
&= \sigma^{-1}(\phi_{\theta(k')}(\sigma(h')))\sigma^{-1}(\phi_{\theta(k')}(\sigma(h'))) \text{ car } \sigma^{-1} \text{ est un homomorphisme} \\
&= \phi'_k(h')\phi'_k(h")
\end{aligned}$$

donc ϕ'_k est un endomorphisme de H'.
Soit h' appartenant à H'.

$$\begin{aligned}
\phi_{k'^{-1}}(\phi_{k'}(h')) &= \phi_{k'^{-1}}(\sigma^{-1}(\phi_{\theta(k')}(\sigma(h')))) \\
&= \sigma^{-1}(\phi_{\theta(k'^{-1})}(\sigma(\sigma^{-1}(\phi_{\theta(k')}(\sigma(h')))))) \\
&= \sigma^{-1}(\phi_{\theta(k'^{-1})}(\phi_{\theta(k')}(\sigma(h')))) \\
&= \sigma^{-1}(\phi_{(\theta(k'))^{-1}}(\phi_{\theta(k')}(\sigma(h')))) \\
&= \sigma^{-1}((\phi_{\theta(k')})^{-1}(\phi_{\theta(k')}(\sigma(h')))) \\
&= \sigma^{-1}(\sigma(h')) \\
&= h'
\end{aligned}$$

et de même, $\phi(\phi_{k'^{-1}}(h'))$=h' donc ϕ'_k est un automorphisme de H' d'inverse $\phi_{k'^{-1}}$.
Montrons que H'$\rtimes_\phi$K' est isomorphe à H$\rtimes_\phi$K : soit f l'application de H'$\rtimes_\phi$K' dans H$\rtimes_\phi$K définie par f(h',k')=$(\sigma(h'), \theta(k'))$.
Montrons que f est un isomorphisme : soient (h',k') et (h",k") appartenant à H'$\rtimes_\phi$K'.
On a

$$\begin{aligned}
f((h',k')(h",k")) &= f(h'\phi_{k'}(h"), k'k") \\
&= (\sigma(h'\phi_{k'}(h")), \theta(k'k")) \\
&= (\sigma(h')\sigma(\phi_{k'}(h")), \theta(k')\theta(k")) \text{ car } \sigma \text{ et } \theta \text{ sont des homomorphismes} \\
&= (\sigma(h')\sigma(\sigma^{-1}(\phi_{\theta(k')}(\sigma(h")))), \theta(k')\theta(k")) \\
&= (\sigma(h')\phi_{\theta(k')}(\sigma(h")), \theta(k')\theta(k")) \\
&= (\sigma(h'), \theta(k'))(\sigma(h"), \theta(k")) \\
&= f(h',k')f(h",k")
\end{aligned}$$

donc f est un homomorphisme.
Soit g l'application de H$\rtimes_\phi$K dans H'$\rtimes_\phi$K' définie par g(h,k)= $(\sigma^{-1}(h), \theta^{-1}(k))$.
Soient (h',k') appartenant à H'$\rtimes_\phi$K' et (h,k) à H$\rtimes_\phi$K.
$g(f(h',k')) = g(\sigma(h'), \theta(k')) = (\sigma^{-1}(\sigma(h')), \theta^{-1}(\theta(k'))) = (h',k')$
et $f(g(h,k)) = f(\sigma^{-1}(h), \theta^{-1}(k)) = (\sigma(\sigma^{-1}(h)), \theta(\theta^{-1}(k))) = (h,k)$.
D'où, f est un isomorphisme d'inverse g.
H'$\rtimes_\phi$K' est donc isomorphe à H$\rtimes_\phi$K. $\diamondsuit$

Terminons ce chapitre avec l'étude d'un sous-groupe particulier d'un groupe G et d'une classe particulière de groupes.

3.5 Groupe dérivé, groupes résolubles

3.5.1 Groupe dérivé

Soit G un groupe non réduit à l'élément neutre.

Définition *Soient g et g' appartenant à G.*
On appelle commutateur de g et g' et on note $[g, g']$, l'élément $gg'g^{-1}g'^{-1}$ de G.

Remarque *Si G est abélien, tout commutateur est égal à l'élément neutre de G.*

Propriété 3.5.1 *Soient g, g' et g" appartenant à G.*
1) $([g, g'])^{-1} = [g', g]$.
2) $g[g', g"]g^{-1} = [gg'g^{-1}, gg"g^{-1}]$.

Démonstration *1)* $([g, g'])^{-1} = (gg'g^{-1}g'^{-1})^{-1} = g'gg'^{-1}g^{-1} = [g', g]$.
2)On a

$$\begin{aligned} g[g', g"]g^{-1} &= gg'g"g'^{-1}g"^{-1}g^{-1} \\ &= (gg'g^{-1})(gg"g^{-1})(gg'^{-1}g^{-1})(gg"^{-1}g^{-1}) \\ &= [gg'g^{-1}, gg"g^{-1}]. \end{aligned}$$

♢

Définition *On appelle groupe dérivé de G, et on note D(G), le sous-groupe de G engendré par l'ensemble des commutateurs.*

Remarque *Si G est abélien alors D(G) est réduit à l'élément neutre.*

Proposition 3.5.2 *D(G) est normal dans G et G/D(G) est abélien.*

Démonstration *D'après la Propriété 2, D(G) est normal dans G.*
Soient π la surjection canonique de G dans G/D(G) et $\pi(g)$ et $\pi(g')$ deux éléments de G/D(G).
Comme $gg'g^{-1}g'^{-1} = [g, g']$ appartient à D(G)=Ker π, $\pi(g^{-1}g'^{-1})$=1.
D'où, π étant un homomorphisme de groupes, on a $\pi(gg') = \pi(g'g)$.
G/D(G) est abélien. ♢

Proposition 3.5.3 *1)Si N est un sous-groupe normal de G tel que G/N est abélien alors N contient D(G).*
2)Si H est un sous-groupe de G contenant D(G) alors H est normal dans G et G/H est abélien.

Démonstration *1)Puisque D(G) est engendré par les commutateurs, il suffit de montrer que ceux-ci sont inclus dans N.*
Soient π la surjection canonique de G dans G/N et (g,g') un couple d'éléments de G.
Comme G/N est abélien, $\pi(gg') = \pi(g'g)$ c'est à dire $\pi(gg'g^{-1}g'^{-1}) = \pi([g,g'])$=1.
D'où, comme Ker π=N, $[g,g']$ appartient à N.
N contient D(G).
2)Soient h appartenant à H et g à G.
$ghg^{-1} = ghg^{-1}h^{-1}h = [g,h]h$ appartient à H car D(G) est inclus dans H.
D'où, H est un sous-groupe normal de G et G/H existe.
Soient g et g' appartenant à G et π la surjection canonique de G dans G/H.
Comme Ker π=H et D(G) est inclus dans H, on a $\pi(gg'g^{-1}g'^{-1}) = \pi([g,g'])$=1. D'où, π étant un homomorphisme de groupes, $\pi(gg') = \pi(g'g)$.
G/H est abélien. $\diamondsuit$

Proposition 3.5.4 *Soient G' un groupe et f : G $\rightarrow$ G' un homomorphisme de groupes. Alors, 1)f(D(G)) est inclus dans D(G').*
2)Si f est surjectif alors f(D(G))=D(G').

Démonstration *1)Soient g_1 et g_2 appartenant à G.*
Puisque f est un homomorphisme de groupes, on a
$f([g_1,g_2]) = f(g_1g_2g_1^{-1}g_2^{-1}) = f(g_1)f(g_2)(f(g_1))^{-1}(f(g_2))^{-1} = [f(g_1),f(g_2)]$.
D'où, f($[g_1,g_2]$) est inclus dans D(G').
Les commutateurs de G engendrant D(G) et f étant un homomorphisme de groupes, f(D(G)) est inclus dans D(G').
2)Soit (g_1',g_2') un couple d'élément de D(G').
Comme f est application surjective, il existe g_1 et g_2 dans G tels que $f(g_1) = g_1'$ et $f(g_2) = g_2'$. Alors,
$[g_1',g_2'] = f(g_1)f(g_2)(f(g_1))^{-1}(f(g_2))^{-1} = f(g_1g_2g_1^{-1}g_2^{-1}) = f([g_1,g_2])$.
D'où, $[g_1',g_2']$ appartient à f(D(G)).
Les commutateurs de G' engendrant D(G') et f étant un homomorphisme de groupes, D(G') est inclus dans f(D(G)).
D'où, puisque d'après le 1, f(D(G)) est inclus dans D(G'), f(D(G))=D(G'). $\diamondsuit$

3.5.2 Groupes résolubles

Soit G un groupe non réduit à l'élément neutre.

Définition *On pose $D^0(G)=G$.*
Soit n un entier supérieur ou égal à 1.
On définit $D^n(G)$ par $D^n(G)=D(D^{n-1}(G))$.

Définition *G est dit <u>résoluble</u> si il existe un entier positif n tel que $D^n(G)=\{1\}$.*

Remarque *Tout groupe abélien est résoluble.*

Proposition 3.5.5 *G est résoluble si et seulement si il existe une suite finie décroissante de sous-groupes de G : $\{1\} = H_n \subset H_n - 1 \subset ... \subset H_0 = G$ (n>0), tels que pour tout i compris entre 0 et n-1, H_{i+1} est normal dans H_i et H_i/H_{i+1} est abélien.*

Démonstration *($\Rightarrow$) Comme G est résoluble, il existe un entier n>0 ($G \neq \{1\}$) tel que $D^n(G)=\{1\}$.*
Pour tout i compris entre 0 et n, on pose $H_i = D^i(G)$.
$H_0=G$, $H_n = \{1\}$.
Puisque $D^{i+1}(G) = D(D^i(G))$ est inclus dans $D^i(G)$, $(H_i)_{0\leq i\leq n}$ est une suite décroissante. D'après la Proposition 3.5.2, D^{i+1} est normal dans $D^i(G)$ et $D^i(G)/D^{i+1}(G)$ est abélien donc H^{i+1} est normal dans H^i et H_{i+1}/H_i est abélien.
($\Leftarrow$) Soit $(H_i)_{0\leq i\leq n}$ (n>0) une suite finie décroissante de sous-groupes de G, telle que $H_0 = G$, $H_n = \{1\}$ et pour tout i compris entre 0 et n-1, H_{i+1} est normal dans H_i et H_i/H_{i+1} est abélien.
H_1 est normal dans H_0 et H_0/H_1 est abélien donc, d'après la Proposition 3.5.3, $D(H_0)$ c'est à dire $D(G)$ est inclus dans H_1.
H_2 est normal dans H_1 et H_1/H_2 est abélien donc, d'après la Proposition 3.5.3, $D(H_1)$est inclus dans H_2.
Comme $D(G)$ est inclus dans H_1, $D^2(G)=D(D(G))$ est inclus dans $D(H_1)$ (un commutateur de $D(G)$ est un commutateur de H_1) donc dans H_2.
En répétant le même procédé pour i=3, ... , n, on trouve que $D^n(G)$ inclus dans $H_n = \{1\}$ et par conséquent, $D^n(G) = \{1\}$. $\diamondsuit$

Les groupes résolubles jouent un grand rôle dans la Théorie de Galois car ils permettent de démontrer l'irrésolubilité de certaines équations par des radicaux.

3.6 Exercices du Chapitre 3

Exercice 1 : Soit G un groupe.
Un sous-groupe H de G est dit caractéristique si pour tout automorphisme α de G, α(H)=H.
1)Montrer que D(G) est un sous-groupe caractéristique de G.
2)Montrer que tout sous-groupe caractéristique de G est normal dans G.
3)Soient H un sous-groupe de G et K un sous-groupe de H.
Montrer que si K est caractérique dans H et si H est caractéristique dans G alors K est caractéristique dans G.
4)Soient N un sous-groupe normal de G et H un sous-groupe de N.
Montrer que si H est caractéristique dans N alors H est un sous-groupe normal de G.

Exercice 2 : Soient G un groupe et A une partie non vide de G.
On pose $N_A = \{(g_1 a_1 g_1^{-1})$ ... $(g_n a_n g_n^{-1})$ / n$\in \mathbb{N}$ et $\forall 1 \leq i \leq n$, $g_i \in$G et
($a_i \in$A ou $a_i^{-1} \in$A)$\}$.
1)Montrer que N_A est un sous-groupe normal de G contenant A.
2)Montrer que N_A est le plus petit sous-groupe normal de G contenant A.
N_A est appelé sous-groupe normal engendré par A.

Exercice 3 : Sous-groupes maximaux.
Soit G un groupe non réduit à l'élément neutre.
Un sous-groupe M de G, différent de G, est dit maximal si il vérifie la propriété suivante : "Si L est un sous-groupe de G contenant M alors L=M ou L=G".
1)Montrer que les sous-groupes p$\mathbb{Z}$, avec p premier, sont les sous-groupes maximaux de $\mathbb{Z}$.
2)Montrer que si G est fini alors G possède des sous-groupes maximaux et tout sous-groupe de G est inclus dans un sous-groupe maximal de G.
3)Soit N un sous-groupe normal de G.
Montrer que N est un sous-groupe maximal de G si et seulement si G/N est un groupe cyclique d'ordre un nombre premier.
Indication : On pourra utiliser l'Exercice 6 des cours Congruence-groupes cycliques.

Exercice 4 : Sous-groupes normaux maximaux.
Soit G un groupe non réduit à l'élément neutre.
Un sous-groupe normal de G, différent de G, est dit normal maximal si il vérifie la propriété suivante :
"Si L est un sous-groupe normal de G contenant N alors L=N ou L=G".
1)Montrer que si G est fini alors G possède des sous-groupes normaux maximaux et tout sous-groupe normal de G est inclus dans un sous-groupe normal maximal de G.
2)Soit N un sous-groupe normal de G, différent de G.
Montrer que N est un sous-groupe normal maximal de G si et seulement si G/N est un groupe simple.
3)Soit N un sous-groupe normal de G.
A t'on l'équivalence : "N est un sous-groupe maximal de G (cf Exercice 3) si et seule-

ment si N est un sous-groupe normal maximal de G" ?.

Exercice 5 : Sous-groupe de Frattini.
Soit G un groupe non réduit à l'élément neutre.
On note par Υ_G l'ensemble des sous-groupes maximaux de G (cf Exercice 3).
On appelle sous-groupe de Frattini de G, le sous-groupe Φ(G) défini par :
Φ(G)=$\cap_{M\in\Upsilon_G}$ M si $\Upsilon_G \neq \emptyset$ et Φ(G)=G si $\Upsilon_G = \emptyset$.
1)Décrire $\Phi(\mathbb{Z})$.
2)Montrer que Φ(G) est un sous-groupe caractéristique de G (cf Exercice 1).

Exercice 6 : Soient G un groupe, H un sous-groupe normal de G et f un automorphisme de G.
1)Montrer que f(H) est un sous-groupe normal de G.
2)Montrer que les groupes G/H et G/f(H) sont isomorphes.

Soient G_1 et G_2 deux groupes, H_1 un sous-groupe normal de G_1 et H_2 un sous-groupe normal de G_2.
1)Montrer que $H_1 \times H_2$ est un sous-groupe normal de $G_1 \times G_2$.
2)Montrer que $G_1 \times G_2/H_1 \times H_2$ est isomorphe à $G_1/H_1 \times G_2/H_2$.

Exercice 8 : Soit A l'ensemble des applications affines de $\mathbb{R}$ c'est à dire l'ensemble des applications de la forme (x$\rightarrow$ax+b) avec a réel non nul et b réel.
1)Montrer que A est un groupe pour la composition des applications.
2)Soit N l'ensemble des applications de la forme (x$\rightarrow$x+b) avec b réel.
Montrer que N est un sous-groupe normal de A.
3)Montrer que A/N est isomorphe à $\mathbb{R}^*$.

Exercice 9 : On désigne par $\mathbb{U}$ l'ensemble des nombres complexes de module 1.
1)Montrer que $\mathbb{U}$ est isomorphe au groupe $\mathbb{R}/\mathbb{Z}$.
2)Montrer que $\mathbb{C}^*/\mathbb{U}$ est isomorphe à $\mathbb{R}_+^*$.

Exercice 10 : Soit n un entier supérieur ou égal à 2.
Soient G un groupe et H_1, H_2, ... , H_n des sous-groupes distincts de G.
On note par $H_1H_2 \dots H_n$ l'ensemble $\{h_1h_2 \dots h_n \ / \ h_i \in H_i \ \forall i \in \{1, \dots, n\}\}$.
Montrer que si, pour tout couple d'entiers (i,j) avec 1$\leq$i$<$j$\leq$n, H_iH_j est un sous-groupe de G alors $H_1H_2 \dots H_n$ est un sous-groupe de G.

Chapitre 4

Opération

Groupe opérant sur un ensemble

Conjugaison

Transitivité

Opérations primitives

Sous-groupes de Sylow

4.1 Groupe opérant sur un ensemble

Dans cette partie, nous allons voir comment on peut appliquer un groupe sur un ensmble quelconque.
Il s'agit d'une des parties les plus importantes de la théorie des groupes puisqu'elle est utilisée dans d'autres domaines de l'Algèbre et permet de démontrer des formules très utilisées.
Les ensembles seront constitués d'éléments distincts.

Commençons par étudier un type particulier de groupes.

4.1.1 Groupes de permutations

Soit E un ensemble non vide.

Proposition 4.1.1 *1)L'ensemble S_E des applications bijectives de E dans E est un groupe pour la composition des fonctions.*
2)Si E est fini de cardinal n alors :
a)Card E=n !,
b)Si $n \geq 3$, S_E n'est pas abélien.

Démonstration *1)Immédiat.*
2)a)Soient x_1, ... , x_n les éléments de E et f appartenant à S_E.
$f(x_1)$ peut être n'importe quel des x_i ($1 \leq i \leq n$). On a donc n valeurs possibles.
$f(x_2)$ peut être n'importe quel des x_i ($1 \leq i \leq n$) hormis la valeur $f(x_1)$ puisque f est injective. On a donc n-1 valeurs possibles, ...
On arrive ainsi à $n \times n\text{-}1 \times \ldots \times 1 = n!$ bijections possibles.
b)Soient x, y et z trois éléments distincts de E.
Soit f une application bijective qui à x associe y, à y associe x et qui fixe z. Soit g une application bijective qui à x associe z, à z associe x et qui fixe y.
Alors, $(g \circ f)(x) = y$ et $(f \circ g)(x) = z$ donc $g \circ f \neq f \circ g$ et par conséquent S_E n'est pas abélien.
♢

Définition *Une application bijective de E dans E est appelée <u>permutation</u> de E. Le groupe S_E est appelé groupe des permutations de E.*
On appelle <u>groupe de permutations</u> (respectivement sous-groupe de permutations) tout groupe (respectivement tout sous-groupe d'un groupe) de la forme S_E où E est un ensemble non vide.
Si $E = \{1, \ldots, n\}$ où n est un entier strictement positif, le groupe S_E est appelé <u>groupe symétrique</u> de degré n et est noté S_n.

Proposition 4.1.2 *Si E est de cardinal n alors S_E est isomorphe à S_n.*

Démonstration *Notons E=$\{x_1, \ldots, x_n\}$.*
Soit σ appartenant à S_E. définissons ψ sur $\{1, \ldots, n\}$ par $\psi(i)=j$ où $\sigma(x_i)=x_j$. Alors, ψ appartient à S_n et l'application f de S_E dans S_n qui à σ associe ψ est clairement bijective. Il reste à montrer que cette application f est un homomorphisme. Soient σ et θ deux éléments de S_E. Soit i compris entre 1 et n.
$f(\sigma \circ \theta)(i)=j$ où $\sigma \circ \theta(x_i)=x_j$. $f(\sigma) \circ f(\theta)(i)=k$ où $\sigma(x_{f(\theta)(i)})=x_k$.
Mais par définition, $x_{f(\theta)(i)}=\theta(x_i)$ donc $\sigma(x_{f(\theta)(i)})=\sigma \circ \theta(x_i)$.
D'où, $x_k = x_i$ et par conséquent k=i.
Ainsi, $f(\sigma \circ \theta)(i)=f(\sigma) \circ f(\theta)(i)$ pour tout i compris entre 1 et n et f est donc un homomorphisme. f est un isomorphisme entre S_E et S_n. $\diamondsuit$

4.1.2 Opération

Soit G un groupe.

Définition *On dit que le groupe G opère sur E (ou que G agit sur E) si il existe un homomorphisme de groupes de G dans S_E.*

Donnons une caractérisation de l'opération d'un groupe sur un ensemble :

Proposition 4.1.3 *Soit . une application de $G \times E$ dans E.*
On note g.x à la place de .(g,x) pour tout couple (g,x) de $G \times E$.
Alors, G opère sur E si et seulement si l'application . vérifie les deux conditions suivantes : 1)Pour tout élément x de G, 1.x=x.
2)Pour tout triplet (g,g',x) de $G \times G \times E$, g.(g'.x)=gg'.x.

Démonstration *($\Rightarrow$) Soit φ l'homomorphisme de groupes de G dans S_E.*
Pour tout élément g de G et pour tout élément x de E, on pose $g.x=\varphi(g)(x)$.
Montrons que cette correspondance est une application : soient (g,x)=(g',y) appartenant à $G \times E$ (on a donc g=g' et x=y). Comme φ est une application, $\varphi(g)=\varphi(g')$. Comme $\varphi(g)$ est une application, $g.x=\varphi(g)(x)=\varphi(g)(y)=\varphi(g')(y)=g'.y$. On a bien défini une application.
Soit x appartenant à E. Puisque φ est un homomorphisme, $1.x=\varphi(1)(x)=Id(x)=x$.
L'application . vérifie donc la condition 1.
Soient g et g' appartenant à G et x appartenant à E.

$$\begin{aligned} g.(g'.x) &= \varphi(g)(g'.x) \\ &= \varphi(g)(\varphi(g')(x)) \\ &= (\varphi(g) \circ \varphi(g'))(x) \\ &= \varphi(gg')(x) \text{ car } \varphi \text{ est un homomorphisme} \\ &= gg'.x. \end{aligned}$$

La condition 2 est ainsi vérifiée.
($\Leftarrow$) Soit φ la correspondance, de G dans l'ensemble des fonctions de E dans E, définie par $\varphi(g) : x \to g.x$.

Montrons que φ est une application : soient g et g' deux éléments égaux de G.
Comme la correspondance . est une application, g.x=g'.x pour tout x de E. D'où φ(g)=φ(g') et φ est une application.
Si x et y sont deux éléments égaux de X alors, la corrspondance . étant une application, g.x=g.y pour tout élément g de G.
D'où φ est une application de G dans l'ensemble des applications de E dans E. Montrons que pour tout g de G, φ(g) est injective :
Soient x et y appartenant à E tels que φ(g)(x)=φ(g)(y).
On a alors, par définition de φ, g.x=g.y.
D'où, grâce aux conditions 1 et 2, x=1.x=g^{-1}g.x=g^{-1}.(g.x)=g^{-1}.(g.y)=g^{-1}g.y=1.y=y.
φ est donc injective.
Montrons que φ(g) est surjective : soit x un élément de E.
Grâce aux conditions 1 et 2, on a x=1.x=gg^{-1}.x=g.(g^{-1}.x)=φ(g)(g^{-1}.x) donc x possède un antécédent pour φ(g). φ(g) est donc surjective.
Pour tout élément g de G, φ(g) est bijective donc φ est une application de G dans S_E. Montrons que φ est un homomorphisme :
Pour tout triplet (g,g',x) de G×G×E,

$$\begin{aligned}\varphi(gg')(x) &= gg'.x \\ &= g.(g'.x) \text{ par la condition 2} \\ &= \varphi(g)(\varphi(g')(x)) \\ &= (\varphi(g)\circ\varphi(g'))(x)\end{aligned}$$

donc φ(gg')=φ(g) ∘ φ(g') et φ est un homomorphisme. ♢

Définition *L'application . est appelée <u>opération</u> de G sur E.*

Remarque *Dans la suite, on notera toutes les opérations par .*

Exemples *1)S_E et tous ses sous-groupes opèrent sur E par l'opération : f.x=f(x) pour tous f de S_E et x de E.*
2)Le groupe G opère sur lui-même par : translations à gauche : g.g'=gg' pour tout couple (g,g') d'éléments de G.
Translations à droite : g.g'=g'.g^{-1} pour tout couple (g,g') d'éléments de G.
3)Soit H un sous-groupe de G. On note par $(G/H)_g$ l'ensemble quotient de G par la relation H_R (cf Section Sous-groupes normaux *du Chapitre 3). G opère sur G/H via l'opération g.(g'H)=gg'H pour tout couple (g,g') d'éléments de G.*

Définition *Soit G un groupe opérant sur un ensemble E via un homomorphisme de groupes φ de G dans S_E.*
On appelle <u>noyau</u> de l'opération, le noyau de l'homomorphisme φ.
Si le noyau de l'opération est réduit à {1}, on dit que l'opération est <u>fidèle</u> (ou que G opère fidèlement sur E).

Remarque *Ker φ = {g ∈ G / ∀x ∈E, φ(g)(x)=x} = {g ∈ G / ∀x ∈E, g.x=x}.*

Exemples *1)L'opération de S_E sur E est fidèle.*
2)Les translations à gauche et à droite sont fidèles.
3)Le noyau de l'opération de G sur $(G/H)_g$ est $\cap_{x\in G}\ xHx^{-1}$.
En effet, l'élément g de G appartient au noyau de l'opération
si et seulement si $gxH{=}xH$
si et seulement si $x^{-1}gxH{=}H$
si et seulement si $x^{-1}gx{\in}H$
si et seulement si $g{\in}xHx^{-1}$ pour tout x de G.
En particulier, si H est normal dans G, le noyau de l'opération est H et par conséquent, si H est distinct de $\{1\}$, l'opération n'est pas fidèle.

Théorème 4.1.4 (Théorème de Cayley) *Tout groupe G est isomorphe à un sous-groupe de permutations.*

Démonstration *Soit G un groupe. G opère fidèlemnt sur lui-même par translations à gauche. Il existe donc un homomorphisme injectif φ de G dans S_G.*
D'où, par le Premier Théorème d'isomorphisme, $G/\{1\}$ est isomorphe à Im φ.
Mais G est isomorphe à $G/\{1\}$ et, comme φ est un homomorphisme, Im φ est un sous-groupe de S_G, donc G est isomorphe à un sous-groupe de S_G, groupe de permutations.
$\diamondsuit$

Ainsi, en théorie, on peut ramener l'étude des groupes à l'études des groupes de permutations.
Cependant, l'étude de tels groupes est très difficile si le cardinal de G est grand ou infini.

4.1.3 Fixateurs et stabilisateurs

Soit G un groupe opérant sur un ensemble E.

Définition *Soit X une partie non vide de E.*
On appelle fixateur de X, et on note $Fix_G(X)$ (ou G_X),
l'ensemble $\{g \in G \ / \ \forall x \in X \ g.x{=}x\}$.
On appelle Stabilisateur de X, et on note $Stab_G(X)$ (ou G(X)),
l'ensemble $\{g \in G \ / \ g.X{=}X\}$.

Remarque *Si x est un élément de E, on note G_x à la place de $Fix_G(\{x\}) = Stab_G(\{x\})$.*

Propriétés 4.1.5 *Soit X une partie non vide de E.*
1)$Fix_G(X)$ et $Stab_G(X)$ sont des sous-groupes de G.
2)$Fix_G(X)$ est un sous-groupe normal de $Stab_G(X)$.
3)Soit φ l'homomorphisme de G dans S_E associé à l'opération .
Ker $\varphi = Fix_G(G) = \cap_{x\in E}\ G_x$.

Démonstration *1)Montrons que $Fix_G(X)$ est un sous-groupe :*
1 appartient à $Fix_G(X)$ donc $Fix_G(X)$ n'est pas vide.
Soient g et g' appartenant à $Fix_G(X)$.
Pour tout x de X, gg'.x=g.(g'.x)=g.x=x.
Pour tout x de X, g.x=x donc $g^{-1}.x = g^{-1}.(g.x) = g^{-1}g.x = 1.x = x$.
$Fix_G(X)$ est bien un sous-groupe de G.
Montrons que $Stab_G(X)$ est un sous-groupe de G :
$Stab_G(X)$ n'est pas vide puisque 1 en est un élément.
Soient g et g' appartenant à $Stab_G(X)$ et x un élément de X.
g' appartient à $Stab_G(X)$ donc g'.x appartient à X.
Puisque g appartient à $Stab_G(X)$, g.(g'.x)=gg'.x appartient à X.
D'où, gg'.X est inclus dans X.
Puisque g appartient à $Stab_G(X)$, il existe un élément y de X tel que g.y=x.
Puisque g' appartient à $Stab_G(X)$, il existe un élément z de X tel que g'.z=y.
D'où, gg'.z=x et X est inclus dans gg'.X. gg'.X=X.
Soient g un élément de $Stab_G(X)$ et x un élément de X.
Puisque g appartient à $Stab_G(X)$, il existe un élément y de X tel que g.y=x.
D'où, $g^{-1}.x = g^{-1}.(g.y) = g^{-1}g.y = y$ et $g^{-1}.X$ est inclus dans X.
Puisque g appartient à $Stab_G(X)$, g.x=y appartient à X. D'où, $g^{-1}.y=x$ et X est inclus dans $g^{-1}.X$. $g^{-1}.X=X$.
$Stab_G(X)$ est un sous-groupe de G.
2)$Fix_G(X)$ est inclus dans $Stab_G(X)$ et est un sous-groupe de G donc $Fix_G(X)$ est un sous-groupe de $Stab_G(X)$.
Montrons que $Fix_G(X)$ est normal dans $Stab_G(X)$:
Soient g un élément de $Fix_G(X)$ et g' un élément de $Stab_G(X)$.
Pour tout x de X, $g'^{-1}.x$ appartient à X donc il existe un élément y de X tel que $g'^{-1}.x=y$ c'est à dire g.y=x.
D'où,

$$\begin{aligned} g'gg'^{-1}.x &= g'g.(g'^{-1}.x) \\ &= g'g.y \\ &= g'.(g.y) \\ &= g'.y \text{ car } g \text{ appartient } Fix_G(X) \\ &= x. \end{aligned}$$

$Fix_G(X)$ est un sous-groupe normal de $Stab_G(X)$.
3)$Ker\ \varphi = \{g \in G \ / \ \forall x \in E,\ g.x=x\} = Fix_G(G) = \cap_{x\in E}\ Fix_G(X)$. $\diamondsuit$

Proposition 4.1.6 *Soit x un élément de E. Alors G_x opère sur E-$\{x\}$.*

Démonstration *Considérons la restriction de . à $G_x \times E - \{x\}$.*
Si g appartient à G_x et si y est un élément de E distinct de x alors g.y est différent de x puisque sinon, y=g^{-1}.x=x (G_x est un sous-groupe de G donc g^{-1} appartient à G_x).
D'où, pour tout couple (g,y) de $G_x \times E - \{x\}$, g.y appartient à E-$\{x\}$.
. étant une opération, pour tout couple (g,g') d'éléments de G_x et pour tout élément y de E distinct de x, g.(g'.y)=gg'.y et 1.y=y.
On a ainsi défini une opération de G_x sur E-$\{x\}$. $\diamondsuit$

Proposition 4.1.7 *Soit X une partie non vide de E. Alors, $Stab_G(X)/Fix_G(X)$ est isomorphe à un sous-groupe de S_X.*

Démonstration *Soit φ l'homomorphisme de G dans S_E associé à l'opération .*
Soit ψ la correspondance de $Stab_G(X)$ dans l'ensemble des applications de X dans E définie par $\psi(g) = \varphi(g)_{|X}$.
Puisque φ est une application et un homomorphisme, ψ est une application et un homomorphisme.
Pour tout élément g de $Stab_G(X)$ et pour tout élément x de X, $\psi(g)(x)$ appartient à X donc ψ est un homomorphisme de G dans l'ensemble des applications de X dans X.
Montrons que pour tout élément g de G(X), $\psi(g)$ est bijective :
$\varphi(g)$ étant injective, $\psi(g)$ est injective.
Soit x appartenant à X. x admet $g^-1.x$ comme antécédent pour $\varphi(g)$. Il suffit donc de montrer que $g^{-1}.x$ appartient à X. Mais g appartient à $Stab_G(X)$ et $Stab_G(X)$ est un sous-groupe de G donc g^{-1} appartient à $Stab_G(X)$ et par conséquent $g^{-1}.x$ appartient à X.
D'où, pour tout élément g de G(X), ψ est bijective et ψ est donc un homomorphisme de G dans S_E.
Déterminons le noyau de ψ :

$$\begin{aligned} Ker\psi &= \{g \in Stab_G(X) \ / \ \varphi(g)_{|X} = Id_X\} \\ &= \{g \in Stab_G(X) \ / \ \forall x \in X \varphi(g)(x) = x\} \\ &= \{g \in Stab_G(X) \ / \ \forall x \in X g.x = x\} \\ &= Stab_G(X) \cap Fix_G(X). \end{aligned}$$

Puisque $Fix_G(X)$ est inclus dans $Stab_G(X)$, Ker ψ=$Fix_G(X)$.
D'où, par le Premier Théorème d'isomorphisme, $Stab_G(X)/Fix_G(X)$ est isomorphe à Im ψ.
Or, ψ étant un homomorphisme, Im ψ et un sous-groupe de S_X, donc $Stab_G(X)/Fix_G(X)$ est isomorphe à un sous-groupe de S_X. $\diamondsuit$

4.1.4 Orbites

Soit G un groupe opérant sur un ensemble E via une opération .

Proposition 4.1.8 *La relation R sur E définie par : xRy $\Leftrightarrow \exists g \in G$ / x=g.y, est une relation d'équivalence.*

Démonstration *R est réflexive puisque, pour tout élément x de E, x=1.x.*
Montrons que R est symétrique : soient x et y deux éléments de E tels que xRy.
Il existe alors un élément g de G tel que x=g.y.
D'où $y=1.y=g^{-1}g.y=g^{-1}.(g.y)=g^{-1}.x$ et donc yRx.
Montrons que R est transitive : soient x, y et z trois éléments de E tels que xRy et yRz. Il existe alors deux éléments g et g' de G tel que x=g.y et y=g'.z.
D'où, x=g.(g'.z)=gg'.z et donc xRz. $\diamondsuit$

Définition *Soit x un élément de E.*
On appelle orbite de x, et on note $\Omega(x)$, la classe d'équivalence de x pour la relation R c'est à dire l'ensemble $\{ g.x \ / \ g \in G\}$.
On appelle orbite de E, toute orbite d'un élément x de E.

Pour tout x de E, on note par G/G_x l'ensemble quotient de G par la relation ${}_{G_x}\mathrm{R}$ (cf Chapitre 3 Section *Sous-groupes normaux*).

Proposition 4.1.9 *Pour tout élément x de E, $\Omega(x)$ est en bijection avec G/G_x.*

Démonstration *Soit ψ la correspondance de G/G_x dans $\Omega(x)$ définie par $\psi(gG_x)=g.x$.*
Montrons que ψ est une application : soient g et g' deux éléments de G tels que $gG_x=g'G_x$. $g'^{-1}g$ appartient alors à G_x c'est à dire $g'^{-1}g.x=x$.
D'où, $g.x=g'.x$ et ψ est une application.
Soit θ la correspondance de $\Omega(x)$ dans G/G_x définie par $\theta(g.x)=gG_x$.
Montrons que θ est une application : soient g et g' deux éléments de G tels que $g.x=g'.x$.
On a alors $g'^{-1}g.x=x$ c'est à dire $g'^{-1}g$ appartient à G_x.
D'où, $gG_x=g'G_x$ et θ est une application.
Il est clair que $\theta \circ \psi = Id_{G/G_x}$ et que $\psi \circ \theta = Id_{\Omega(x)}$.
D'où, ψ est une bijection de G/G_x vers $\Omega(x)$. $\diamondsuit$

Corollaire 4.1.10 *Si E et G sont finis alors, pour tout élément x de E, Card $\Omega(x)=\frac{|G|}{|G_x|}$.*

Démonstration *D'après la Proposition précédente, Card $\Omega(x)$=Card G/G_x et, d'après la Formule de Lagrange, Card $G/G_x = [G : G_x] = \frac{|G|}{|G_x|}$.* $\diamondsuit$

Corollaire 4.1.11 (Formule des classes) *Si E et G sont finis alors Card $E=\sum_{(x_i)_{1\leq i\leq n}} \frac{|G|}{|G_{x_i}|}$ où $((x_i)_{1\leq i\leq n})$ est une famille de représentants des orbites de E.*

Démonstration *Les orbites $\Omega(x_i)$ étant les classes d'équivalence de E pour la relation R, elles forment une partition de E.*
D'où, Card $E=\sum_{(x_i)_{1\leq i\leq n}}$ Card $\Omega(x_i)$ et donc Card $E=\sum_{(x_i)_{1\leq i\leq n}} \frac{|G|}{|G_{x_i}|}$ d'après le Corollaire précédent. $\diamondsuit$

4.1.5 Opérations équivalentes

Définition *Soient G et G' deux groupes opérant respectivement sur les ensembles E et F. On note les deux opérations par .*
On dit que l'opération de G sur E est équivalente à l'opération de G' sur F si il existe un isomorphisme σ de G vers G' et une bijection θ de E dans F tels que pour tout g appartenant à G et pour tout x appartenant à E, $\theta(g.x)=\sigma(g).\theta(x)$.

Proposition 4.1.12 *La relation $\Re$: "l'opération de G sur E est équivalente à l'opération de G' sur F" est une relation d'équivalence sur l'ensemble des couples (G,E) formés d'un groupe G opérant sur un ensemble E.*

Démonstration *La reflexivité de $\Re$ est évidente, il suffit de prendre $\sigma = Id_G$ et $\theta = Id_E$.*
Supposons que l'opération de G sur E est équivalente à l'opération de G' sur F.
Il existe alors un isomorphisme σ de G vers G' et une bijection θ de E vers F tels que $\theta(g.x)=\sigma(g).\theta(x)$ pour tout élément g de G et pour tout élément x de E.
Soient $\phi = \sigma^{-1}$ et $\tau = \theta^{-1}$.
ϕ est un isomorphisme de G' vers G et τ est une bijection de F vers E.
Soient g' un élément de G' et y un élément de F.
Comme σ et θ sont bijectives, il existe des éléments g de G et x de E tels que $g'=\sigma(g)$ c'est à dire $g=\phi(g')$ et $y=\theta(x)$ c'est à dire $x=\tau(y)$.
D'où, $g'.y=\sigma(g).\theta(x)=\theta(g.x)$.
Par conséquent, $\tau(g'.y)=\tau(\theta(g.x))=g.x=\phi(g').\tau(y)$.
On a trouvé un isomorphisme ϕ de G' vers G et une bijection τ de F vers E tels que $\tau(g'.y)=\phi(g').\tau(y)$ pour tout élément g' de G' et pour tout élément y de F.
La relation $\Re$ est donc symétrique.
Soit G" un groupe opérant sur un ensemble L.
Supposons que l'opération de G sur E est équivalente à l'opération de G' sur F et que l'opération de G' sur F est équivalente à l'opération de G" sur L.
Il existe alors un isomorphisme σ de G vers G' et une bijection θ de E vers F tels que $\theta(g.x)=\sigma(g).\theta(x)$ pour tout élément g de G et pour tout élément x de E et il existe un isomorphisme ζ de G' vers G" et une bijection ρ de F vers L tels que $\rho(g'.y)=\zeta(g').\rho(y)$ pour tout élément g' de G' et pour tout élément y de F.
Posons $\xi = \zeta \circ \sigma$ et $\gamma = \rho \circ \theta$.
ξ est un isomorphisme de G dans G" et γ est une bijection de E vers L.
Soient g un élément de G et x un élément de E.
On a

$$\begin{aligned} \gamma(g.x) &= \rho(\theta(g.x)) \\ &= \rho(\sigma(g).\theta(x)) \\ &= \zeta(\sigma(g)).\rho(\theta(x)) \\ &= \xi(g).\gamma(x). \end{aligned}$$

On a trouvé un isomrphisme ξ de G vers G" et et une bijection γ de E vers L tels que $\gamma(g.x)=\xi(g).\gamma(x)$ pour tout élément g de G et pour tout élément x de E.
D'où, l'opération $\Re$ est transitive.
L'opération $\Re$ est donc une relation d'équivalence. $\diamondsuit$

Proposition 4.1.13 *Soit une opération d'un groupe G sur un ensemble E équivalente à une opération d'un groupe G' sur un ensemble F.*
Alors, l'une des opérations est fidèle si et seulement si l'autre est fidèle.

Démonstration *Puisque la relation $\Re$ est symétrique d'après la Proposition précédente, il suffit de montrer l'une des deux implications pour démontrer la proposition.*
Soient φ l'homomorphisme de G dans S_E et ψ l'homomorphisme de G' dans S_F, associés aux opérations.
Supposons que l'opération de G sur E est fidèle.
Soient g'_1 et g'_2 deux éléments de G' tels que $\psi(g'_1) = \psi(g'_2)$.
On a alors $g'_1.y = g'_2.y$ pour tout y de F.
Puisque σ est bijective, il existe des éléments g_1 et g_2 de G tels que $g'_1 = \sigma(g_1)$ c'est à dire $g_1 = \phi(g'_1)$ et $g'_2 = \sigma(g_2)$ c'est à dire $g_2 = \phi(g'_2)$.
Pour tout élément x de E, il existe, τ étant surjective, un élément y de F tel que $x = \tau(y)$.
On a alors

$$\begin{aligned} \varphi(g_1)(x) &= g_1.x \\ &= \phi(g'_1).\tau(y) \\ &= \tau(g'_1.y) \\ &= \tau(g'_2.y) \\ &= \phi(g'_2).\tau(y) \\ &= g_2.x \\ = \varphi(g_2)(x). & \end{aligned}$$

D'où $\varphi(g_1) = \varphi(g_2)$.
Or l'opération de G sur E est fidèle donc φ est injective.
On en déduit que $g_1 = g_2$ et donc $g'_1 = \sigma(g_1) = \sigma(g_2) = g'_2$.
ψ est injective donc l'opération de G' sur F est fidèle. $\diamondsuit$

Proposition 4.1.14 *Soit G un groupe opérant sur un ensemble E.*
Alors, pour tout élément x de E, l'opération de G sur $\Omega(x)$ et l'opération de G sur G/G_x sont équivalentes.

Démonstration *Soit x un élément de E.*
L'opération de G sur G/G_x est : $g.g'G_x = gg'G_x$ pour tout couple (g,g') d'éléments de G. On a vu (Proposition 4.1.9) qu'il existe une bijection θ entre $\Omega(x)$ et G/G_x.
On considère l'isomorphisme Id de G dans G.
Montrons que pour tout élément g de G et pour tout élément g'.x de $\Omega(x)$ (g' élément de G), $\theta(g.(g'.x)) = g.\theta(g'.x)$:

$$\begin{aligned} \theta(g.(g'.x)) &= \theta(gg'.x) \\ &= gg'G_x \; par\; définition\; de\; \theta \\ &= g.(g'G_x) \; par\; définition\; de\; l'opération\; de\; G\; sur\; G/G_x \\ &= g.\theta(g'.x). \end{aligned}$$

D'où, l'opération de G sur $\Omega(x)$ est équivalente à l'opération de G sur G/G_x. $\diamondsuit$

4.2 Conjugaison

4.2.1 Automorphismes intérieurs

Soit G un groupe.

Proposition 4.2.1 *Pour tout élément g de G, l'application α_g, définie de G dans G par $\alpha_g(x)=gxg^{-1}$, est un automorphisme de G.*

Démonstration *Si x et y appartiennent à G alors $\alpha_g(xy)=gxyg^{-1} = gxg^{-1}gyg^{-1}=\alpha_g(x)\alpha_g(y)$ donc α_g est un homomorphisme.*
Pour tout élément x de G, $(\alpha_g\circ\alpha_{g^{-1}})(x)=(\alpha_{g^{-1}}\circ\alpha_g)(x)=x$ donc α_g est un automorphisme de G d'inverse $\alpha_{g^{-1}}$. $\diamondsuit$

Définition *L'automorphisme α_g est appelé automorphisme intérieur associé à l'élément g de G.*

Proposition 4.2.2 *L'application α définie de G dans Aut(G) par $\alpha(g)=\alpha_g$ est un homomorphisme de groupes.*

Démonstration *Pour tout triplet (g,g',x) d'éléments de G, on a*

$$\begin{aligned}
\alpha(gg')(x) &= \alpha_{gg'}(x) \\
&= gg'xg'^{-1}g^{-1} \\
&= g\alpha_{g'}(x)g^{-1} \\
&= \alpha_g(\alpha_{g'}(x)) \\
&= (\alpha_g \circ \alpha_{g'})(x) \\
&= (\alpha(g) \circ \alpha(g'))(x).
\end{aligned}$$

D'où, α est un homomorphisme de groupes. $\diamondsuit$

Définition *L'image de l'homomorphisme α est noté Int(G).*

4.2.2 Centre d'un groupe

Soit G un groupe.

Définition *On appelle centre de G et on note Z(G), le noyau de l'homomorphisme de groupes α.*

Remarque *Par définition du noyau d'un homomorphisme de groupes, on a $Z(G)=\{g \in G \ / \ \alpha_g = Id_G\} = \{g \in G \ / \ \forall x \in G \ gx = xg\}$.*

Proposition 4.2.3 *G est abélien si et seulement si Z(G)=G.*

Démonstration *Le résultat découle de la Remarque précédente.* $\diamondsuit$

Propriété 4.2.4 *Z(G) est un sous-groupe normal de G.*

Démonstration *Z(G) est le noyau d'un homomorphisme de groupes partant du groupe G.* $\diamondsuit$

Proposition 4.2.5 *Si G/Z(G) est cyclique alors G est abélien.*

Démonstration *Z(G) étant un sous-groupe normal de G, le groupe quotient G/Z(G) est bien défini.*
Soit $\overline{x}$*=xZ(G) le générateur de G/Z(G) et soient g et g' deux éléments de G.*
G/Z(G) étant cyclique, il existe des entiers n et m tels que $\overline{g} = \overline{x}^n$ *et* $\overline{g}' = \overline{x}^m$.
D'où, il existe des éléments z et z' de Z(G) tels que $x^{-n}g = z$ *c'est à dire* $g=x^n z$ *et* $x^{-m}g' = z'$ *c'est à dire* $g'=x^m z'$.
On en déduit que

$$\begin{aligned} gg' &= x^n z x^m z' \\ &= x^n x^m z z' \ car\ z\ appartient\ à\ Z(G) \\ &= x^{n+m} z z' \\ &= x^{m+n} z z' \\ &= x^m x^n z z' \\ &= x^m x^n z' z \ car\ z\ appartient\ à\ Z(G) \\ &= x^m z' x^n z \ car\ z\ appartient\ à\ Z(G) \\ &= g'g. \end{aligned}$$

G est donc abélien. $\diamondsuit$

4.2.3 Opération de conjugaison

Soit G un groupe.

Proposition 4.2.6 *G opère sur lui-même via l'opération :* $g.x=gxg^{-1}$ *(g,x∈G).*

Démonstration *Soient g,g' et x des éléments de G.*
On a $g.(g'.x)=g(g'.x)g^{-1} = gg'xg'^{-1}g^{-1} = (gg')x(gg')^{-1}=gg'.x$ *et* $1.x=x$ *donc l'application* $g.x=gxg^{-1}$ *est bien une opération de G sur lui-même.* $\diamondsuit$

Définition *Cette opération est appelée opération de conjugation et on dit que G opère sur lui-même par conjugaison (ou par automorphismes intérieurs).*

Propriétés 4.2.7 *1)Le noyau de l'opération de conjugaison est Z(G).*
2)Si G n'est pas réduit à l'élément neutre, l'opération de conjugaison n'est pas transitive.

Démonstration *1)L'homomorphisme de G dans Aut(G) associé à l'opération de conjugaison est* $\varphi : g \longrightarrow \varphi(g) : x \longrightarrow g.x = gxg^{-1}$.
g appartient au noyau de φ *si et seulement si, pour tout x de G,* $gxg^{-1}=x$ *c'est à dire* $gx=xg$. *D'où le noyau de l'opération est Z(G).*
2)Supposons que l'opération soit transitive.
Alors, pour tout couple (x,y) d'éléments de G, il existe un élément g de G tel que $g.x=gxg^{-1}=y$.
Prenons x=1 et y un élément de G distinct de 1 (G non réduit à $\{1\}$*).*
Il existe alors un élément g de G tel que $g.1=1=y$. *Contradiction.* $\diamondsuit$

4.2.4 Centralisateur et normalisateur

Soient G un groupe et H un sous-groupe de G.

Définition *On appelle centralisateur de H, et on note* $C_G(H)$*, le fixateur de H pour l'opération de conjugaison c'est à dire l'ensemble*
$\{g \in G \ / \ \forall h \in H \ ghg^{-1} = h\}$.
On appelle normalisateur de H, et on note $N_G(H)$*, le stabilisateur de H pour l'opération de conjugaison c'est à dire l'ensemble*
$\{g \in G \ / \ \forall h \in H \ ghg^{-1} \in H\}$.
On dit qu'un sous-groupe K de G normalise H si K est inclus dans $N_G(H)$.

Propriétés 4.2.8 *1)*$C_G(H)$ *et* $N_G(H)$ *sont des sous-groupes de G.*
2)$C_G(H)$ *est un sous-groupe normal de* $N_G(H)$.
3)$N_G(H)/C_G(H)$ *est isomorphe à un sous-groupe de Aut(G).*

Démonstration *Résultent des propriétés des fixateurs et stabilisateurs (cf Section* Opération d'un groupe sur un ensemble*).* $\diamondsuit$

Proposition 4.2.9 *H est normal dans G si et seulement si* $N_G(H)=H$.

Démonstration *Découle de la définition de* $N_G(H)$. $\diamondsuit$

Proposition 4.2.10 $N_G(H)$ *est le plus grand (au sens de l'inclusion) sous-groupe de G dans lequel H est normal.*

Démonstration $N_G(H)$ *contient H et H est un sous-groupe de G donc H est un sous-groupe de* $N_G(H)$.

Montrons que H est normal dans $N_G(H)$: soient h appartenant à H et g appartenant à $N_G(H)$. Comme $N_G(H)$ est un sous-groupe de G, g^{-1} appartient aussi à $N_G(H)$. Par définition de $N_G(H)$, ghg^{-1} appartient à h donc H est normal dans $N_G(H)$.
Soit K un sous-groupe de G dont H est un sous-groupe normal.
Soit h un élément de H. Pour tout élément k de K, khk^{-1} appartient à H donc k appartient à $N_G(H)$. D'où, K est inclus dans $N_G(H)$. $\diamondsuit$

4.2.5 Formule des classes pour l'opération de conjugauison

Soit G un groupe.

A l'opération de conjugaison, on associe la relation d'équivalence R sur G définie par xRy $\Leftrightarrow$ $\exists g \in G$ / $gxg^{-1} = y$ (cf Section *Opération d'un groupe sur un ensemble*).
La classe d'équivalence d'un élément x de G est appelée orbite de x et est notée Ω(x).

Proposition 4.2.11 *Soit x un élément de G.*
Alors, l'orbite de x est réduite à $\{x\}$ si et seulement si x appartient à Z(G).

Démonstration *$\Omega(x)$ est de cardinal 1 si et seulement si pour tout élément g de G, $g.x=gxg^{-1}=x$ c'est à dire $gx=xg$.* $\diamondsuit$

Proposition 4.2.12 (Formule des classes) *Si G est fini alors*
$|G| = |Z(G)| + \sum \frac{|G|}{|G_{g_i}|}$ *où la somme est prise sur une famille (g_1, ... ,g_n) de représentants des orbites de G non réduites à un élément.*

Démonstration *Soient (g_1, ... ,g_n) une famille de représentants des orbites de G non réduites à un élément et soient $\Omega(z_1)$, ... , $\Omega(z_m)$ les orbites composées d'un unique élément.*
Les orbites $\Omega(g_1)$, ... , $\Omega(g_n)$ forment une partition de G donc $|G| = \sum Card\Omega(z_i) + \sum Card\Omega(g_i)$.
Or d'après la Proposition 4.1.10, $Card\Omega(g_i) = \frac{|G|}{|G_{g_i}|}$ pour tout i compris entre 1 et n.
D'où, $|G| = \sum Card\Omega(z_i) + \sum \frac{|G|}{|G_{g_i}|}$.
D'après la Proposition précédente, l'orbite d'un élément est de cardinal 1 si et seulement si cet élément appartient à Z(G) donc les z_i sont les éléments de Z(G).
D'où, $|G| = |Z(G)| + \sum \frac{|G|}{|G_{g_i}|}$. $\diamondsuit$

Remarque *Cette Formule des classes est utilisée pour démontrer qu'un corps fini est commutatif. Pour plus de détails, on pourra se référer aux ouvrages de D. Perrin : cours d'algèbre ou de I. Gozard : Théorie de Galois, les deux aux éditions Ellipses.*

Soient G un groupe et p un nombre premier.

Définition *On dit que G est un p-groupe si l'ordre de G est une puissance non nulle de p.*

Proposition 4.2.13 *Le centre d'un p-groupe n'est pas réduit à l'élément neutre.*

Démonstration *Si il n'y pas d'orbite de cardinal strictement supérieur à 1, alors $|Z(G)| = |G|$>1 donc Z(G) n'est pas réduit à l'élément neutre.*
On suppose donc qu'il existe des orbites non réduites à un élément.
D'après la Formule des classes, $|G| = |Z(G)| + \sum \frac{|G|}{|G_{g_i}|}$ où la somme est prise sur une famille (g_1, ... ,g_n) de représentants des orbites de G non réduites à un élément.
D'après la Formule de Lagrange, $|G_{g_i}|$ divise $|G|$ pour tout i compris entre 1 et n.
Soit i compris entre 1 et n.
Si $|G_{g_i}|$=1 alors Card $\Omega(g_i) = \frac{|G|}{|G_{g_i}|} = |G|$ et donc $\Omega(g_i)$=G.
D'où, l'opération de conjugaison est transitive ce qui est impossible puisque G n'est pas réduit à l'élément neutre (cf Propriétés 4.2.7).
Si $|G_{g_i}| = |G|$ alors Card $\Omega(g_i) = \frac{|G|}{|G_{g_i}|}$=1 ce qui est impossible par choix de g_i.
D'où, pour tout i compris entre 1 et n, il existe un entier a_i compris entre 1 et n-1 tel que $\frac{|G|}{|G_{g_i}|} = p^{a_i}$.
En considérant la somme $|G| = |Z(G)| + \sum \frac{|G|}{|G_{g_i}|}$ modulo p (c'est à dire en prenant les classes de ces nombres pour la relation de congruence modulo p), on obtient $\overline{|Z(G)|}$=0 c'est à dire p divise $|Z(G)|$.
D'où, Z(G) n'est pas réduit à l'élément neutre. ♢

Corollaire 4.2.14 *Tout groupe d'ordre p^2, où p est un nombre premier, est abélien.*

Démonstration *D'après la Formule de Lagrange et la Proposition précédente, l'ordre de Z(G) est soit p soit p^2.*
Si $|Z(G)| = p^2$ alors Z(G)=G et G est donc abélien (Proposition 4.2.3).
Si $|Z(G)|$=p alors $\frac{|G|}{|Z(G)|}$=p donc G/Z(G) est cyclique.
D'où, d'après la Proposition 4.2.5, G est abélien et donc $|Z(G)| = p^2$. Contradiction.
♢

4.3 Transitivité

4.3.1 Opération transitive

Soit G un groupe opérant sur un ensemble E.

Définition *On dit que l'opération est transitive (ou que G opère transitivement sur E) si E n'admet qu'une seule orbite.*

Proposition 4.3.1 *G opère transitivement sur E si et seulement si pour tout couple (x,y) d'éléments de E, il existe un élément g de G tel que g.x=y.*

Démonstration *G opère transitivement sur E si et seulement si pour tout couple (x,y) d'éléments de E, x et y sont en relation c'est à dire si et seulement si pour tout couple (x,y) d'éléments de E, il existe un élément g de G tel que g.x=y.* $\diamondsuit$

Exemples *1)L'opération de S_E sur E est transitive puisque si x et y sont deux éléments de E et f l'élément de S_E défini en posant f(x)=y, f(y)=x et f(z)=z pour tout z distinct de x et y, on a f.x=y.*
2)La translation à gauche est transitive puisque pour tout couple (g,g') d'élements de G, $(g'g^{-1}).g = g'$.
De même, la translation à droite est transitive.
3)L'opération de G sur $(G/H)_g$ est transitive puisque pour tout couple (g,g') d'éléments de G, $(g'g^{-1}).gH = g'H$.

Proposition 4.3.2 *Soit G un groupe opérant sur un ensemble E.*
Alors, pour tout élément x de E, G opère transitivement sur $\Omega(x)$.

Démonstration *G opère sur $\Omega(x)$ via l'opération g.(g'.x)=gg'.x pour tout couple (g,g') d'élements de G et pour tout élément x de E. Cette opération est transitive puisque si g et g' sont deux éléments de G, $g'g^{-1}.(g.x)=g'.x$.* $\diamondsuit$

Proposition 4.3.3 *Soit G un groupe opérant transitivement sur un ensemble E. Alors, pour tout élément x de E, Card $E=\frac{|G|}{|G_x|}$.*

Démonstration *Puisque l'opération est transitive, E=$\Omega(x)$ pour tout élément x de E. On applique alors la Proposition 4.1.10.* $\diamondsuit$

Proposition 4.3.4 *Soit une opération d'un groupe G sur un ensemble E équivalente à une opération d'un groupe G' sur un ensemble F.*
Alors, l'une des opérations est transitive si et seulement si l'autre est transitive.

Démonstration *La relation "l'opération de G sur E est équivalente à l'opération de G' sur F" est symétrique d'après la Proposition 4.1.12, il suffit de montrer l'une des deux implications pour démontrer la proposition.*
Par hypothèse, il existe un isomorphisme σ de G dans G' et une bijection θ de E vers F tels que $\theta(g.x)=\sigma(g).\theta(x)$ pour tout g de G et x de E. Soit $\phi = \sigma^{-1}$.
Supposons que l'opération de G sur E est transitive.
Soient y_1 et y_2 deux éléments de F.
Comme θ est surjective, il existe des éléments x_1 et x_2 de E tels que $y_1 = \theta(x_1)$ et $y_2 = \theta(x_2)$.
Comme l'opération de G sur E est transitive, il existe un élément g de G tel que $g.x_1 = x_2$.
Comme ϕ est bijective, il existe un élément g' de G' tel que $g=\phi(g')$ c'est à dire $g' = \sigma(g)$.
D'où,

$$\begin{aligned} g'.y_1 &= \sigma(g).\theta(x_1) \\ &= \theta(g.x_1) \\ &= \theta(x_2) \\ &= y_2 \end{aligned}$$

et donc l'opération de G' sur F est transitive. $\diamondsuit$

4.3.2 Opération simplement transitive

Soit G un groupe opérant sur un ensemble E.

Définition *On dit que l'opération . est simplement transitive (ou que G opère simplement transitivement sur E) si pour tout couple (x,y) d'éléments de E, il existe un unique élément g de G tel que g.x=y.*

Exemple *Les translations à gauche et à droite sont simplement transitives.*

Propriété 4.3.5 *Si G opère simplement transitivement sur E alors G opère fidèlement et transitivement sur E.*

Démonstration *Soit G opérant simplement transitivement sur E.*
Alors, par définition, G opère transitivement sur E.
Montrons que G opère fidèlement sur E :
Soit φ l'homomorphisme de G dans S_E associé à l'opération.
Soient g et g' deux éléments de G tels que $\varphi_g=\varphi_{g'}$.
On a alors g.x=g'.x pour tout x de E.
D'où, si on pose y=g.x, g.x=g'.x=y.
Or G opère simplement transitivement sur E donc g=g'.
φ est injective donc l'opération est fidèle. $\diamondsuit$

A t'on la réciproque ?

Proposition 4.3.6 *On suppose G abélien.*
Si G opère fidèlement et transitivement sur E alors G opère simplement transitivement sur E.

Démonstration *Soient x et y deux éléments de E.*
Comme G opère transitivement sur E, il existe un élément g de G tel que g.x=y.
Montrons que ce point g est unique :
Supposons qu'il existe un élément g' de G tel que g.x=g'.x.
Montrons qu'alors, pour tout élément z de E, g.z=g'.z :
Comme G opère transitivement sur E, il existe un élément g" de G tel que g".x=z.
Comme G est abélien et comme g.x=g'.x, g.z=g.(g".x)=g".(g.x)=g".(g'.x)=g'.(g".x)=g'.z.
D'où, si φ est l'homomorphisme de G dans S_E associé à l'opération,
$\varphi(g) = \varphi(g')$. Or l'opération est fidèle c'est à dire φ est injective donc g=g'.
Pour tout couple (x,y) d'éléments de E, il existe un unique élément g de G tel que g.x=y et par conséquent, G opère simplement transitivement sur E. $\diamondsuit$

La commutativité de G est primordiale comme le montre l'exemple suivant :

Exemple *On suppose E de cardinal supérieur ou égal à 4.*
On a vu qu'alors S_E n'est pas abélien.
On a montré que l'opération de S_E sur E est fidèle et transitive.
Montrons qu'elle n'est pas simplement transitive :
Soient x, y, z et t quatre éléments distincts de E, σ l'élément de S_E défini par : $\sigma(x)=y$, $\sigma(y)=x$ et $\sigma(k)=k$ pour tout k distinct de x et y, et ψ l'élément de S_E défini par $\psi(x)=y$, $\psi(y)=x$, $\psi(z)=t$, $\psi(t)=z$ et $\psi(k)=k$ pour tout k appartenant à E-{x, y, z, t}. Alors, σ et ψ sont différents mais $\sigma.x=\sigma(x)=y$ et $\psi.x=\psi(x)=y$.
D'où, S_E n'opère pas transitivement sur E.

4.3.3 Opération k-transitive

Soit G un groupe non réduit à l'élément neutre, opérant sur un ensemble E, de cardinal supérieur ou égal à 2.

Définition *Soit k un entier compris entre 2 et Card E si E est fini, supérieur ou égal à 2 si E est infini.*
On dit que l'opération . est k-transitive sur E (ou que G opère k fois transitivement sur E) si pour pour tout couple ($(x_1, \ldots, x_k)$,$(y_1, \ldots, y_k)$) de k-uplets d'éléments distincts de E, il existe un élément g de G tel que $g.x_i = y_i$ pour tout i compris entre 1 et k.

Propriétés 4.3.7 *1)Si l'opération est k-transitive, avec k≥3, alors elle est (k-1)-transitive.*
1)Si l'opération est k-transitive, avec k≥3, alors elle est n-transitive pour tout entier n compris entre 2 et k-1.
2)Si l'opération est k-transitive alors elle est transitive.

Démonstration *1)Soient* $(x_1, \ldots, x_{k-1})$ *et* $(y_1, \ldots, y_{k-1})$ *deux (k-1)-uplets d'éléments distincts de E.*
Comme l'opération est k-transitive, le cardinal de E (pouvant être infini) est supérieur ou égal à k (on a besoin de k-uplets d'éléments distincts), donc il existe $x \in E-\{x_1, \ldots, x_{k-1}\}$ *et* $y \in E-\{y_1, \ldots, y_{k-1}\}$.
Les k-uplets $(x_1, \ldots, x_{k-1}, x)$ *et* $(y_1, \ldots, y_{k-1}, y)$ *sont ainsi formés d'éléments distincts de E.*
D'où, comme l'opération est k-transitive, il existe un élément g de G tel que $g.x_i = y_i$ *pour tout i compris entre 1 et k-1 (et g.x=y).*
L'opération est donc (k-1)-transitive.
2)Découle directement, par une récurrence descendante, de la Propriété 1.
3)Soient x et y deux éléments de E. Si x=y alors 1.x=x=y.
Supposons x et y distincts.
Alors les couples (x,y) et (y,x) sont formés d'éléments distincts de E.
Comme l'opération est k-transitive, elle est 2-transitive d'après la Propriété 2.
Donc il existe un élément g de G tel que g.x=y (et g.y=x).
L'opération est par conséquent transitive. $\diamondsuit$

Proposition 4.3.8 *Soit k compris entre 2 et Card E si E est fini, k supérieur ou égal à 2 si E est infini.*
G opère k fois transitivement sur E si et seulement si G opère transitivement sur E et, pour tout élément x de E, G_x *opère (k-1) fois transitivement sur* $E-\{x\}$.

Démonstration *(⇒) D'après la Propriété 3 précédente, G opère transitivement sur E. Soit x un élément de E.*
On a vu que G_x *opère sur* $E-\{x\}$.
Puisque le cardinal de E est supérieur ou égal à k, on peut trouver deux (k-1)-uplets $(x_1, \ldots, x_{k-1})$ *et* $(y_1, \ldots, y_{k-1})$ *d'éléments distincts de* $E-\{x\}$.
Alors, $(x_1, \ldots, x_{k-1}, x)$ *et* $(y_1, \ldots, y_{k-1}, x)$ *sont deux k-uplets d'éléments distincts de E.*
D'où, puisque G opère k fois transitivement sur E, il existe un élément g de G tel que $g.x_i = y_i$ *pour tout i compris entre 1 et k-1, et g.x=x.*
Comme g.x=x, g appartient à G_x.
D'où, G_x *opère (k-1) fois transitivement sur* $E-\{x\}$.
(⇐) Puisque le cardinal de E est supérieur ou égal à k, on peut trouver deux k-uplets $(x_1, \ldots, x_k)$ *et* $(y_1, \ldots, y_k)$ *d'éléments distincts de E.*
Comme G opère transitivement sur E, il existe un élément g de tel que $g.x_1 = y_1$.
Soit φ *l'homomorphisme de G dans* S_E *associé à l'opération .*
Comme $\varphi(g)$ *est injective,* $g.x_i = \varphi(g)(x_i) \neq \varphi(g)(x_j) = g.x_j$ *pour tout couple (i,j) d'entiers, compris entre 1 et k, distincts.*

D'où, ($g.x_2$, ... ,$g.x_k$) et (y_2, ... ,y_k) sont deux k-uplets d'élements distincts de E-$\{y_1\}$. Comme G_{y_1} opère k-1 fois transitivement sur E-$\{y_1\}$, il existe un élément g' de G_{y_1} tel que g'.($g.x_i$)=g'$g.x_i = y_i$ pour tout i compris entre 2 et k. Comme g'$g.x_1$=g'$.y_1 = y_1$ (car g' appartient à G_{y_1}), on a g'$g.x_i$=y_i pour tout i compris entre 1 et k.
D'où, G opère k fois transitivement sur E. $\diamondsuit$

Proposition 4.3.9 *Soit une opération d'un groupe G sur un ensemble E équivalente à une opération d'un groupe G' sur un ensemble F.*
Alors, l'une des opérations est k-transitive si et seulement si l'autre est k-transitive.

Démonstration *La démonstration est analogue à celle de la Proposition 4.3.4.* $\diamondsuit$

4.4 Opérations primitives

Nous allons étudier les opérations qui agissent d'une manière particulière sur les relations d'équivalences. Le but de cette partie est de démontrer un critère de simplicité.

4.4.1 Relations d'équivalence stables par un groupe

Soit G un groupe opérant sur un ensemble E.

Proposition 4.4.1 *Soit R une relation d'équivalence sur E.*
Alors, pour tout élément g de G, la relation ${}_gR$ définie sur E par $x\,{}_gR\,y \Leftrightarrow g.xRg.y$, *est une relation d'équivalence.*

Démonstration *Soient g un élément de G et x, y et z des éléments de E.*
R est réflexive donc $g.xRg.x$. *D'où,* $x\,{}_gR\,x$ *et ${}_gR$ est réflexive.*
Puisque R est symétrique, si $g.xRg.y$ *alors* $g.yRg.x$. *D'où, si* $x\,{}_gR\,y$ *alors* $y\,{}_gR\,x$ *et ${}_gR$ est donc symétrique.*
Supposons que $x\,{}_gR\,y$ *et* $y\,{}_gR\,z$. *Alors,* $g.xRg.y$ *et* $g.yRg.z$.
D'où, puisque R est transitive, $g.xRg.z$ *et ${}_gR$ est donc transitive.* $\diamondsuit$

Proposition 4.4.2 *Soient g un élément de G et R une relation d'équivalence sur E. Alors, pour tout élément x de E, la classe d'équivalence* $cl_{{}_gR}(x)$ *de x pour la relation ${}_gR$ est égale à* $g^{-1}.cl_R(g.x)$ *où* $cl_R(x)$ *désigne la classe d'équivalence de x pour la relation R.*

Démonstration *y appartient à* $cl_{{}_gR}(x)$ *si et seulement si* $x\,{}_gR\,y$ *c'est à dire si et seulement si* $g.xRg.y$.
D'où, y appartient à $cl_{{}_gR}(x)$ *si et seulement si g.y appartient à* $cl_R(g.x)$.
On en déduit que y appartient à $cl_{{}_gR}(x)$ *si et seulement si y appartient à* $g^{-1}.cl_R(g.x)$.
$\diamondsuit$

Définition *Une relation R sur E est <u>stable</u> par G si, pour tout élément g de G,* ${}_gR=R$.

Exemples *L'égalité est stable par G.*
La relation d'équivalence grossière (x est en relation avec y quels que soient les éléments x et y de E) est stable par G.

4.4.2 Blocs

Soit G un groupe opérant sur un ensemble E.

Définition *Soit B une partie non vide de E.*
On dit que B est un bloc (pour l'opération de G) si, pour tout élément g de G, g.B=$\{g.b$ / $b \in B\}$=B ou g.B$\cap$B=$\emptyset$.

Exemples *1)E est un bloc de E.*
2)Toute partie de E de cardinal 1 est un bloc de E.

Définition *Un bloc B de E est trivial si B=E ou si Card B=1.*

Propriété 4.4.3 *1)Si B_1 et B_2 sont deux blocs de E d'intersection non vide alors $B_1 \cap B_2$ est un bloc de E.*
2)Si B est un bloc de E alors, pour tout élément g de G, g.B est un bloc de E.

Démonstration *1)Soit g un élément de G.*
Si $g.B_1 \cap B_1 = \emptyset$ ou $g.B_2 \cap B_2 = \emptyset$ alors g.($B_1 \cap B_2$)=$\emptyset$ et $B_1 \cap B_2$ est donc un bloc.
On suppose que g.B_1=B_1 et g.B_2=B_2.
Alors, g.($B_1 \cap B_2$) est inclus dans $B_1 \cap B_2$.
Soit x appartenant à $B_1 \cap B_2$.
Puisque x appartient à B_1 et à B_2, il existe des éléments x_1 de B_1 et x_2 de B_2 tels que $g.x_1$=g.x_2=x. On a alors x_1=g^{-1}.x=x_2 et donc x_1 appartient à $B_1 \cap B_2$.
Ainsi, $B_1 \cap B_2$ est inclus dans g.($B_1 \cap B_2$).
D'où, g.($B_1 \cap B_2$)=$B_1 \cap B_2$ et $B_1 \cap B_2$ est un bloc.
2)Soit g' un élément de G.
Si $g^{-1}g'$.(g.B)$\cap$B=$\emptyset$ alors g'.(g.B)$\cap$g.B=$\emptyset$ et g.B est donc un bloc.
Si $g^{-1}g'$.(g.B)=B alors g'.(g.B)=g.B et g.B est un bloc. $\diamondsuit$

Remarque *A toute partition $\{B_i\}_{i \in I}$ de E est associée une relation d'équivalence R définie par xRy $\Leftrightarrow$ x et y appartiennent à une même partie B_i (i$\in$I).*

Proposition 4.4.4 *On suppose que G opère transitivement sur E. Soit B un bloc de E. Alors, l'ensemble $\{g.B$ / $g \in G\}$ est une partition de E.*
De plus, la relation d'équivalence associée à cette partition est stable par G.

Démonstration *Soit x un élément de E. Puisque G opère transitivement sur E, si b est un élément de B alors il existe un élément g de G tel que g.b=x.*
D'où, l'ensemble $\{g.B$ / $g \in G\}$ recouvre E.
Soient g.B et g'.B deux éléments distincts de G.
Montrons par l'absurde que g.B$\cap$g'.B=$\emptyset$:
Soit g.b=g'.b' appartenant à g.B$\cap$g'.B (b, b'$\in$B).

Alors, $g'^{-1}g.b=b'$ donc $g'^{-1}g.B\cap B\neq\emptyset$. D'où, puisque B est un bloc, $g'^{-1}g.B=B$ et donc $g.B=g'.B$. Contradiction. On a $g.B\cap g'.B=\emptyset$.
D'où, $\{g.B \ / \ g\in G\}$ est une partition de E.
Soit R la relation associée à cette partition. $xRy \Leftrightarrow \exists\ g\in G \ / \ x,\ y\in g.B$.
Soit g' un élément de G. $x_{g'}Ry \Leftrightarrow \exists\ g\in G \ / \ g'.x,\ g'.y\in g.B$.
Si x et y appartiennent à g.B alors g'.x et g'.y appartiennent à g'g.B donc si xRy alors $x_{g'}Ry$. Si g'.x et g'.y appartiennent à g.B alors x et y appartiennent à $g'^{-1}g.B$ donc si $x_{g'}Ry$ alors xRy. D'où, R est stable par G. $\diamondsuit$

Proposition 4.4.5 *Si R est une relation d'équivalence sur E, stable par G, alors les classes d'équivalences pour la relation R, sont des blocs de E.*

Démonstration *Puisque R est stable par le groupe G, toute classe d'équivalence d'un élément x de E pour la relation ${}_gR$, $g\in G$, est égale à la classe d'équivalence de x pour la relation R.*
D'où, d'après la Proposition 4.4.2, on a $g^{-1}cl(g.x)=cl(x)$ c'est à dire $cl(g.x)=g.cl(x)$ pour tout élément g de G et pour tout élément x de E.
Soient x un élément de E et g un élément de G.
Puisque les classes d'équivalence distinctes sont disjointes, on a $cl(g.x)=cl(x)$ ou $cl(g.x)\cap cl(x)=\emptyset$.
D'où, $g.cl(x)=cl(x)$ ou $g.cl(x)\cap cl(x)=\emptyset$ et donc cl(x) est un bloc de E. $\diamondsuit$

On rappelle qu'on associe à l'opération de G sur E, une relation d'équivalence définie par xRy $\Leftrightarrow$ il existe g appartenant à G tel que g.x=y.
Les classes d'équivalences pour cette relation sont appelées orbites de E.

Corollaire 4.4.6 *Les orbites de E sont des blocs de E.*

Démonstration *Puisque les orbites sont les classes d'équivalence de la relation d'équivalence associée à l'opération R de G sur E, il suffit, d'après la Proposition précédente, de montrer que cette relation d'équivalence est stable par G.*
Soient x et y deux éléments de E et g un élément de G.
$xRy \Leftrightarrow \exists\ g'\in G \ / \ g'.x=y$.
Si $g'.x=y$ alors $gg'g^{-1}.(g.x)=g.y$ donc si xRy alors x_gRy.
Si $g'.(g.x)=g.y$ alors $g^{-1}g'g.x=y$ donc si x_gRy alors xRy.
D'où, la relation R est stable par G et, d'après la Proposition précédente, les orbites de E sont des blocs de E. $\diamondsuit$

Proposition 4.4.7 *Si E est fini et si G opère transitivement sur E alors le cardinal de tout bloc de E divise le cardinal de E.*

Démonstration *D'après la Proposition précédente, l'ensemble des blocs g.B, $g\in G$, forme une partition de E. Soit m le nombre de blocs g.B distincts formant cette partition. m est fini car E est fini.*
Or, pour tout élément g de G, Card g.B=Card B car si b et b' sont deux éléments distincts de B alors g.b et g.b' sont distincts.
D'où, Card E=m Card B et le cardinal de B divise celui de E. $\diamondsuit$

4.4.3 Opération primitive

Soit G un groupe opérant transitivement sur un ensemble E.

Définition *On dit que l'opération de G sur E est primitive (ou que G opère primitivement sur E) si les seules relations d'équivalences stables par G sont l'égalité et l'équivalence grossière.*

L'intérêt des blocs réside dans la proposition suivante :

Proposition 4.4.8 *G opère primitivement sur E si et seulement si E n'a que des blocs triviaux.*

Démonstration *($\Rightarrow$) Soit B un bloc de E. D'après la Proposition 4.4.4, l'ensemble des g.B, g$\in$G, forme une partition de E et la relation d'équivalence R associée à cette partition est stable par G.*
D'où, par hypothèse, R est l'égalité ou R est l'équivalence grossière.
Si R est l'égalité alors toutes les classes d'équivalences c'est à dire les g.B, g$\in$G, sont réduites à un élément. On a donc Card g.B=1 pour tout élément g de G.
Or Card g.B=card B donc Card B=1 et B est un bloc trivial.
Si R est l'équivalence grossière alors il n'y a qu'une seule classe d'équivalence : l'ensemble E. En particulier, 1.B=B=E et B est un bloc trivial de E.
Tous les blocs de E sont triviaux.
($\Leftarrow$) Soit R une relation d'équivalence sur E. D'après la Proposition 4.4.5, les classes d'équivalence de R sont des blocs de E.
D'où, par hypothèse, ces classes d'équivalences sont soit réduites à un point et dans ce cas R est l'égalité, soit toute égales à E et dans ce cas, R est l'équivalence grossière.
Ainsi R est stable par G. G opère primitivement sur E. $\diamondsuit$

Cette caractérisation donne un bon moyen pour savoir si une opération est primitive :

Corollaire 4.4.9 *Si G opère n fois transitivement sur E , avec n$\geq$2, alors G opère primitivement sur E.*

Démonstration *Si l'opération est n-transitive avec n$\geq$2 alors elle est 2-transitive donc il suffit de montrer la proposition pour n=2.*
G opère 2 fois transitivement sur E donc E a au moins 2 éléments.
Soit B un bloc de E non réduit à un élément.
Si Card E=2 alors B=E et B est un bloc trivial.
On suppose que Card E>2. Montrons par l'absurde que B=E :
Si B est différent de E alors il existe un élément x de E n'appartenant pas à E.
Soient a et b deux éléments distincts de B (B est de cardinal supérieur ou égal à 2).

Puisque c n'appartient pas à B, (a,b) et (a,c) sont deux couples d'éléments distincts de E. D'où, G opèrant 2 fois transitivement sur E, il existe un élément g de G tel que g.a=b et g.b=c. Puisque g.a=b, on a g.B∩B≠ ∅ donc, B étant un bloc, g.B=B.
D'où, c=g.b appartient à g.B=B. Contradiction.
Card B=1 ou B=E donc B est un bloc trivial de E.
D'après la Proposition précédente, G opère primitivement sur E. ♢

Proposition 4.4.10 *Pour tout élément x de E, l'ensemble des blocs de E contenant x est en bijection avec l'ensemble des sous-groupes de G contenant G_x.*
De plus, cette bijection envoie les blocs triviaux $\{x\}$ et E respectivement sur G_x et G.

Démonstration *Soit x un élément de E.*
a)Soient B un bloc de E contenant x et S le stablisateur de B c'est à dire l'ensemble des éléments g de G tels que g.B est inclus dans B.
Puisque B est un bloc, S est l'ensemble des éléments de G tels que g.B=B.
S étant un stabilisateur, S est un sous-groupe de G (cf cours Opération*).*
Montrons que G_x est inclus dans S : soit g appartenant à G_x.
Alors, il existe un élément g de G tel que g.x=x. On a donc g.B∩B≠ ∅ et par conséquent, B étant un bloc, g.B=B. Ainsi g appartient à S et G_x est inclus dans S.
b)Soit H un sous-groupe de G contenant G_x. On pose C=$\{h.x$ / h∈H$\}$.
Montrons que C est un bloc de E : soit g un élément de G.
Supposons que g.C∩C≠ ∅. Soient alors h et k deux éléments de H tels que g.hx=kx.
On a donc $k^{-1}gh.x=x$ et $k^{-1}gh$ appartient ainsi à G_x.
G_x étant inclus dans H, $k^{-1}gh$ appartient à H et g appartient donc à $kHh^{-1}=H$.
D'où, puisque l'application (h⟶gh) est une permutation de H (c'est à dire une bijection de H dans H), g.C=C.
c)On a donc trouvé une application ϕ de l'ensemble des blocs de E contenant x dans l'ensemble des sous-groupes de G contenant G_x et une application ψ de l'ensemble des sous-groupes de G contenant G_x et l'ensemble des blocs de E contenant x.
Il reste à montrer que ϕ et ψ sont inverses l'une de l'autre : soient B un bloc de E contenant x, S=ϕ(B) et C=$\psi(\phi(B))$.
On a C=$\{s.x$ / s∈S$\}$ = $\{s.x$ / s.B=B$\}$.
Si c.x appartient à C alors, comme x appartient à B, c.x appartient à c.B=B.
D'où, C est inclus dans B.
Soit b appartenant à B. Puisque G opère transitivement sur E, il existe un élément g de G tel que g.x=b.
Puisque x appartient à B, g.B∩B≠ ∅ et donc, B étant un bloc, g.B=B. D'où, g appartient à ϕ(B) et b=g.x appartient à C.
On a donc B=$\psi(\phi(B))$.
Soient H un sous-groupe de G contenant G_x, B=ψ(H) et K=$\phi(\psi(H))$.
On a K=$\{g$∈G / g.ψ(H)=ψ(H)$\}$ = $\{g$∈G / g.(H.x)=H.x$\}$.
L'application (h⟶gh) étant une permutation de H pour tout élément g de H, H est inclus dans K.
Soit k un élément de K. Il existe alors un élément h de H tel que k.x=h.x. D'où, $h^{-1}k.x=x$ et $h^{-1}k$ appartient à G_x.
G_x étant inclus dans H, $h^{-1}k$ apprtient à H et k appartient donc à hH=H.
K est inclus dans H.

On a donc $H=\phi(\psi(H))$.
D'où, l'application ϕ est une bijection de l'ensemble des blocs de E contenant x vers l'ensemble des sous-groupes de G contenant G_x, d'inverse ψ.
d)$\phi(\{x\})=\{g\in G \ / \ g.x=x\} = G_x$.
$\phi(E)=\{g\in G \ / \ g.E=E\}=G$ car l'application $(y\rightarrow g.y)$ est une permutation de E (associée à l'opération de G sur E). $\diamondsuit$

La Proposition précédente donne une autre caractérisation des opérations primitives :

Corollaire 4.4.11 *G opère primitivement sur E si et seulement si, pour tout élément x de E, G_x est un sous-groupe maximal de G.*

Démonstration *D'après la Proposition 4.4.8, G opère primitivement sur E si et seulement si E n'a que des blocs triviaux. D'où, d'après la Proposition précédente, G opère primitivement sur E si et seulement si, pour tout élément x de E, G ne possède pas de sous-groupe H contenant G_x et différent de G_x et de G c'est à dire si et seulement si G_x est un sous-groupe maximal de G pour tout élément x de G.* $\diamondsuit$

4.4.4 Critère de simplicité d'Iwasawa

Soit G un groupe non réduit à l'élément neutre opérant sur un ensemble E.

Proposition 4.4.12 *On note φ, l'homomorphisme de G dans S_E associée à l'opération de G sur E. Soit N un sous-groupe normal de G.*
Alors, si G opère primitivement sur E, N est inclus dans Ker φ ou N opère transitivempent sur E.

Démonstration *Supposons que N n'est pas inclus dans Ker φ.*
Montrons, par l'absurde, que N n'est inclus dans aucun G_x, x_inE :
Supposons N inclus dans G_x c'est à dire, pour tout élément n de N, n.x=x.
Soit y un élément de E. Puisque G opère transitivement sur E (G opère primitivement sur E), il existe un élément g de G tel que g.x=y. D'où, pour tout élément n de N, ng.x=n.y.
Mais N est normal dans G donc il existe un élément n' de N tel que ng=gn' ($g^{-1}ng$ appartient à N). D'où, n.y=g.(n'.x)=g.x=y
Ainsi, pour tout élément n de N et pour tout élément y de E, n.y=y et N est donc inclus dans φ. Contradiction.
N n'est inclus dans aucun G_x, x∈E.
Montrons que N opère transitivement sur E : soit x un élément de E.
On pose $X_x = \{n.x \ / \ n\in N\}$. Montrons que X_x=E :
D'après le Corollaire 4.4.11, G_x est un sous-groupe maximal de G.
D'où, NG_x étant un sous-groupe de G contenant G_x, $NG_x = G_x$ ou NG_x=G. Mais NG_x est différent de G_x, car N n'est pas inclus dans G_x, donc NG_x=G.

Soit y un élément de E. Puisque G opère transitivement sur E, il existe un élément g de G tel que g.x=y.
Comme NG_x=G, il existe un élément n de N et un élément g' de G_x tel que g=ng'. D'où, y=ng'.x=n.x et y appartient à X_x.
X_x=E pour tout élément x de E donc, pour tout couple (x,y) d'éléments de E, il existe un élément n de N tel que n.x=y.
N opère transitivement sur E. $\diamondsuit$

Théorème 4.4.13 (Critère de simplicité d'Iwasawa) *Si G vérifie :*
i)G opère fidèlement sur E
ii)G opère primitivement sur E
iii)G=D(G)
iv)Pour tout élément x de E, il existe un sous-groupe normal abélien H_x de G_x tel que G est engendré par l'ensemble $\{gH_xg^{-1} / g\in G\}$.
Alors, G est un groupe simple non abélien.

Démonstration *G n'est pas réduit à $\{1\}$ et G=D(G) donc G n'est pas abélien (sinon G=D(G)=$\{1\}$).*
Soit N un sous-groupe normal de G différent de $\{1\}$. Montrons que N=G :
Puisque G opère fidèlement sur E, Ker $\varphi = \{1\}$ où φ désigne l'homomorphisme de G dans S_E asssocié à l'opération.
D'où, d'après la Proposition précédente, N opère transitivement sur E.
Soit x un élément de E. En reprenant la démonstration de la Proposition précédente, on montre que NG_x=G.
D'où, tout élément g de G s'écrit sous la forme ng' où n appartient à N et g' appartient à G_x. On en déduit que gH_xg^{-1}=ng'$H_xg'^{-1}n^{-1}$=nH_xn^{-1} car H_x est normal dans G_x.
Par conséquent, G est engendré par l'ensemble $\{nH_xn^{-1} / n\in N\}$.
Mais nhn^{-1} appartient à NH_x pour tout élément n de N et pour tout élément h de H_x car nhn^{-1}=$nhn^{-1}h^{-1}h \in NH_x$, N étant normal dans G.
D'où, G=NH_x et G/N=NH_x/N.
D'après le Deuxième Théorème d'isomorphisme, NH_x/N est isomorphe à $H_x/H_x\cap N$.
H_x étant abélien, $H_x/H_x\cap N$ est abélien et G/N est donc abélien.
D'où, D(G) est inclus dans N (cf cours Groupe dérivé, groupes résolubles*).*
Puisque D(G)=G, on a N=G.
G est un groupe simple non abélien. $\diamondsuit$

Remarque *Ce Critère est utilisé par exemple pour montrer la simplicité des groupes $PSL_n(\mathbb{F}_q)$ pour (n,q) différent de (2,2) et (2,3).*

4.5 Sous-groupes de Sylow

D'après le Théorème de Lagrange, l'ordre d'un groupe est divisible par l'ordre de n'importe lequel de ses sous-groupes.
Etant donné un diviseur d de l'ordre d'un groupe G, G possède t'il un sous-groupe d'ordre d ?

4.5.1 p-groupes, p-sous-groupes de Sylow

Définition *Soit p un nombre premier.*
On appelle p-groupe, tout groupe d'ordre une puissance non nulle de p.

Exemple $\mathbb{Z}/8\mathbb{Z}$ *est un 2-groupe.*

Proposition 4.5.1 *Le centre d'un p-groupe n'est pas réduit à l'élément neutre.*

Démonstration *On considère l'opération de conjugaison de G sur lui-même.*
On note par cl(g), la classe de conjugaison de g, élément de G.
Si il n'y pas de classe de conjugaison de cardinal strictement supérieur à 1 alors tous les éléments de G sont dans le centre de G (cf cours Conjugaison*).*
D'où, $|Z(G)| = |G| > 1$ *et donc Z(G) n'est pas réduit à l'élément neutre.*
On suppose donc qu'il existe des classes de conjugaison non réduites à un élément.
D'après la Formule des classes, $|G| = |Z(G)| + \sum \frac{|G|}{|G_{g_i}|}$ *où la somme est prise sur une famille* $\{g_1, \ldots, g_n\}$ *de représentants des classes de G non réduites à un élément.*
D'après la Formule de Lagrange, $|G_{g_i}|$ *divise* $|G|$ *pour tout i compris entre 1 et n.*
Soit i compris entre 1 et n.
Si $|G_{g_i}| = 1$ *alors Card* $cl(g_i) = \frac{|G|}{|G_{g_i}|} = |G|$ *et donc* $cl(g_i) = G$.
D'où, l'opération de conjugaison est transitive ce qui est impossible puisque G n'est pas réduit à l'élément neutre (cf cours Conjugaison*).*
Si $|G_{g_i}| = |G|$ *alors Card* $cl(g_i) = \frac{|G|}{|G_{g_i}|} = 1$ *ce qui est impossible par choix de* g_i.
D'où, pour tout i compris entre 1 et n, il existe un entier a_i *compris entre 1 et n-1 tel que* $\frac{|G|}{|G_{g_i}|} = p^{a_i}$.
En considérant la somme $|G| = |Z(G)| + \sum \frac{|G|}{|G_{g_i}|}$ *modulo p (c'est à dire en prenant les classes de ces nombres pour la relation de congruence modulo p), on obtient* $0 = cl(|Z(G)|) + 0$ *donc* $cl(|Z(G)|) = 0$ *c'est à dire p divise* $|Z(G)|$.
D'où, Z(G) n'est pas réduit à l'élément neutre. $\diamondsuit$

Corollaire 4.5.2 *Tout groupe d'ordre* p^2*, où p est un nombre premier, est abélien.*

Démonstration *D'après le Théorème de Lagrange et la Proposition précédente, l'ordre de Z(G) est soit p soit* p^2.

Si $|Z(G)| = p^2$ alors Z(G)=G donc G est abélien (cf cours Conjugaison*).*
Si $|Z(G)|$=p alors $\frac{|G|}{|Z(G)|}$=p donc G/Z(G) est cyclique.
D'où, G est abélien (cf cours Conjugaison*).* $\diamondsuit$

Définition *Soit G un groupe d'ordre $p^n s$ où n est un entier strictement positif et s un entier naturel non divisible par p.*
On appelle p-sous-groupe de Sylow de G, tout sous-groupe de G d'ordre p^n.

Exemple *<3>=$\{0, 3, 6, 9\}$ est un 2-groupe de Sylow de $\mathbb{Z}/12\mathbb{Z}$.*

Remarque *Un p-sous-groupe de Sylow est un p-groupe.*

La première question que l'on est amené à se poser est l'existence de p-sous-groupes de Sylow pour un groupe G donné.

4.5.2 Premier Théorème de Sylow

Soit G un groupe d'ordre sp^n où n est un entier strictement positif et s un entier naturel non divisible par p.

Lemme *$C_{sp^n}^{p^r} = \lambda p^{n-r}$ où λ est un entier naturel non divisible par p.*

Démonstration *Puisque pour tout couple (a,b) d'entiers strictement positifs, $C_a^b = \frac{a(a-1)...(a-b+1)}{b!}$, on a $C_{sp^n}^{p^r} = \frac{sp^n}{p^r}\frac{sp^n-1}{1}...\frac{sp^n-(p^r-1)}{p^r-1} = sp^{n-r}\frac{sp^n-1}{1}...\frac{sp^n-(p^r-1)}{p^r-1}$.*
Tout entier k compris entre 1 et p^r-1 peut s'écrire sous la forme qp^a avec $0 \leq a < r$ et q entier non divisible par p. D'où, $\frac{sp^n-k}{k} = \frac{sp^{n-a}-q}{q}$.
p ne divise pas q donc p ne divise pas $sp^{n-a} - q$.
On en déduit, p étant premier, que p ne divise pas $\lambda = \frac{sp^n-1}{1}...\frac{sp^n-(p^r-1)}{p^r-1}$.
$C_{sp^n}^{p^r} = \lambda p^{n-r}$ avec λ entier naturel non divisible par p. $\diamondsuit$

Théorème 4.5.3 [Premier Théorème de Sylow]
Pour tout entier m compris entre 1 et n, G contient un sous-groupe d'ordre p^m.

Démonstration *On considère l'ensemble F des parties de G à p^r éléments.*
F est de cardinal $C_{sp^n}^{p^r}$ c'est à dire, d'après le Lemme précédent, λp^{n-r} où λ est un entier naturel non divisible par p.
Si A appartient à F et si g appartient à G alors gA=$\{ga$ / $a \in A\}$ appartient à F (si a et b sont deux éléments distincts de A alors ga est différent de gb) donc G opère sur F par translation à gauche.

Soit $\{A_i,\ 1 \leq i \leq k\}$ une famille de représentants des orbites de F pour cette opération. Par la Formule des classes, on a $\sum_{i=1}^{n} \frac{|G|}{|G_{A_i}|} = Card\ F = \lambda p^{n-r}$.
Si p^{n-r+1} divise $\frac{|G|}{|G_{A_i}|}$ pour tout i compris entre 1 et n alors p^{n-r+1} divise $\sum_{i=1}^{n} \frac{|G|}{|G_{A_i}|}$ c'est à dire λp^{n-r}. On a alors p qui divise λ ce qui est exclu.
Il existe donc au moins un entier i compris entre 1 et k tel que p^{n-r+1} ne divise pas $\frac{|G|}{|G_{A_i}|}$. Posons $P = G_{A_i}$. Nous allons montrer que P est d'ordre p^r.
On a $sp^n = |G| = |P|\frac{|G|}{|G_{A_i}|}$ et p^{n-r+1} ne divise pas $\frac{|G|}{|G_{A_i}|}$ donc $\frac{|G|}{|G_{A_i}|} = s'p^a$ avec $0 \leq a \leq n\text{-}r$ et s' premier avec p.
s' divisant sp^n et s' étant premier avec p, s' divise s par le Lemme de Gauss.
On pose $s'' = \frac{s}{s'}$. On a alors $|P| = s''p^{n-a}$.
Puisque $0 \leq a \leq n\text{-}r$, on a $r \leq n\text{-}a \leq n$ et par conséquent, p^r divise $|P|$. D'où, $|P| \geq p^r$.
Soit a un élément de A_i. La correspondance de P dans A_i définie par $(g \rightarrow ga)$ est une application injective, on en déduit que $|P| \leq Card\ A_i = p^r$.
D'où, P est un sous-groupe d'ordre p^r de G. $\diamondsuit$

En prenant m=n, on obtient :

Corollaire 4.5.4 *Un groupe fini d'ordre divisible par un nombre premier p possède un p-sous-groupe de Sylow.*

4.5.3 Second Théorème de Sylow

Soit G un groupe d'ordre sp^n où n est un entier strictement positif et s un entier naturel non divisible par p.

D'après le Premier Théorème de Sylow, on sait que G possède des p-sous-groupes de Sylow. Nous allons maintenant voir comment sont liés les p-sous-groupes de Sylow entre eux et donner des indications sur leur nombre.

Définition *On note $S_p(G)$ l'ensemble des p-sous-groupes de Sylow de G.*

Théorème 4.5.5 [Second Théorème de Sylow]
1)Tout p-sous-groupe de G est inclus dans un p-sous-groupe de Sylow.
2)G opère transitivement par conjugaison sur $S_p(G)$.
3)Si on note $n_p(G)$ le cardinal de $S_p(G)$ alors $n_p(G)$ divise l'ordre de G et est congru à 1 modulo p.

Démonstration *1)Soient H un p-sous-groupe de G et P un p-sous-groupe de Sylow de G. H opère sur l'ensemble quotient $(G/P)_g$ de G par la relation ${}_PR$ (cf cours* Sous-groupes normaux*) par translations à gauche.*
On peut donc décomposer $(G/P)_g$ en orbites pour cette opération.
Le cardinal de chacune des orbites divise l'ordre de H (cf cours Opération*) donc les orbites sont soit de cardinal 1 soit de cardinal une puissance non nulle de p.*
Montrons qu'il existe au moins une orbite de cardinal 1 :
Si toutes les orbites sont de cardinal une puissance non nulle de p alors p divise $\sum_{g_iP\in R}$ Card Ω_i (où R est une famille de représentants des orbites et Ω_i est l'orbite de représentant g_iP) c'est à dire p divise Card $((G/P)_g)$ (puisque les orbites forment une partition de $(G/P)_g$).
Or Card $((G/P)_g)$=$[G:P]$=$|G|/|P|$=s (cf cours Sous-groupes normaux*) n'est pas divisible par p donc il existe au moins une orbite W de cardinal 1.*
Soit gP un représentant de cette orbite ($W\subset(G/P)_g$).
Puisque W est de cardinal 1, on a, pour tout élément h de H, h.gP=hgP=gP.
On en déduit que $g^{-1}hgP$=P ce qui entraîne que g-1hg appartient à P pour tout élément h de H. D'où, pour tout élément h de H, h appartient à gPg^{-1}.
H est donc inclus dans gPg^{-1}. Il est clair que ($x\rightarrow gPg^{-1}$) est une bijection de P dans gPg^{-1} donc $|gPg^{-1}| = |P| = p^n$.
Par conséquent, gPg^{-1} est un p-sous-groupe de Sylow de G.
H est ainsi inclus dans un p-sous-groupe de Sylow de G.
On a montré une propriété plus générale : (P) Etant donné un p-sous-groupe H de G, il existe, pour tout p-sous-groupe de Sylow P de G, un élément g de G tel que H est inclus dans le p-sous-groupe de Sylow gPg^{-1}.
2)Si P est un p-sous-groupe de Sylow de G alors, pour tout élément g de G,
$|gPg^{-1}| = |P| = p^n$ donc gPg^{-1} est aussi un p-sous-groupe de Sylow de G.
G opère donc par conjugaison sur $S_p(G)$.
Montrons que deux p-sous-groupes de Sylow P et Q de G sont toujours conjugués :
Q étant un p-sous-groupe de G, il existe, d'après la Propriété (P), un élément g de G tel que Q est inclus dans gPg^{-1}. Or, $|Q| = |gPg^{-1}| = p^n$ donc Q=gPg^{-1}.
P et Q sont par conséquent conjugués.
G opère transitivement par conjugaison sur $S_p(G)$.
Pour démontrer le troisième résultat, on a besoin d'un lemme intermédiaire :

Lemme *Si P est un p-sous-groupe de Sylow de Sylow de G alors P est l'unique p-sous-groupe de Sylow de $N_G(P)$.*

Démonstration *Puisque $N_G(P)$ est un sous-groupe de G, l'ordre de $N_G(P)$ est de la forme s'p^a avec 0≤aleqn, p ne divisant pas s' et s' divisant s.*
Mais P est un sous-groupe de $N_G(P)$ donc $|P| = p^n$ divise $|N_G(P)|$.
On en déduit que a=n. Ainsi, $|N_G(P)|$=s'p^n avec p ne divisant pas s'.
Puisque $|P| = p^n$, P est un p-sous-groupe de Sylow de $N_G(P)$.
Soit Q un p-sous-groupe de Sylow de $N_G(P)$.
Alors, d'après la partie 2, P et Q sont conjugués dans $N_G(P)$.
Il existe donc un élément x de $N_G(P)$ tel que xPx^{-1}=Q.
x appartenant à $N_G(P)$, on a xPx^{-1}=P et par conséquent P=Q. $\diamondsuit$

3)D'après la partie 2, G opère transitivement par conjugaison sur $S_p(G)$.
On a donc une seule orbite pour cette opération : $S_p(G)$.
D'où, $n_p(G)$=Card $S_p(G)$ divise $|G|$ (cf cours Opération*).*
Soit P un p-sous-groupe de Sylow de G.
Puisque G opère par conjugaison sur $S_p(G)$, P opère aussi par conjugaison sur $S_p(G)$.
$S_p(G)$ se décompose donc en orbites pour cette opération.
Le cardinal de ces orbites divise l'ordre de P donc chacune de ces orbites est soit de cardinal 1 soit de cardinal une puissance non nulle de p.
$\{P\}$ est une orbite de cardinal 1. Montrons que c'est la seule :
Soit Q un p-sous-groupe de Sylowde G tel que l'orbite de Q est $\{Q\}$.
Alors, pour tout élément x de P, $x.Q=xQx^{-1}=Q$.
On en déduit que P est inclus dans le normalisateur de Q dans G.
On a vu dans la démonstration du lemme que $|N_G(Q)|$ est de la forme $s'p^n$ où p ne divise pas s. On en déduit que P et Q sont des p-sous-groupes de Sylow de $N_G(Q)$.
D'où, d'après le lemme, P=Q.
On a donc une orbite de cardinal 1 et toutes les autres de cardinal divisible par p.
Puisque les orbites forment une partition de $S_p(G)$, on a
$n_p(G)$=Card $S_p(G)=1+\sum_{Q\in R}$ Card Ω_Q (où R est une famille de représentants des orbites différentes de $\{P\}$ et Ω_Q est l'orbite de représentant Q).
D'où, $n_p(G)$ est congru à 1 modulo p. $\diamondsuit$

Corollaire 4.5.6 *$n_p(G)$ divise s.*

Démonstration *n_p divise $|G|$ donc n_p est de la forme $s'p^a$ avec $0\leq a\leq n$, p ne divisant pas s' et s' divisant s.*
Si a est différent de 0 alors n_p est congru à 0 modulo p.
Contradiction avec la Propriété 3 du Second Théorème de Sylow.
D'où, a=0 et n_p=s' divise s. $\diamondsuit$

4.5.4 Applications

Théorème 4.5.7 (Théorème de Cauchy) *G possède un élément d'ordre p.*

Démonstration *D'après le Premier Théorème de Sylow, G possède un groupe P d'ordre p. p étant premier, P est un groupe cyclique (cf cours Sous-groupes normaux). Tout générateur de P est d'ordre p.* $\diamondsuit$

Remarque *Le Théorème de Cauchy ($\simeq$1825) est antérieur au Premier Théorème de Sylow (1872). En exercice est proposé une preuve directe du Théorème de Cauchy.*

D'après le Théorème de lagrange, les éléments d'un p-groupe sont d'ordre une puissance de p. La réciproque est aussi vraie :

Corollaire 4.5.8 *Si G est un groupe non réduit à* $\{1\}$ *dont tous les éléments différents de 1 sont d'ordre une puissance non nulle d'un nombre premier p alors G est un p-groupe.*

Démonstration *Soit q un diviseur premier de l'ordre de G.*
D'après le Théorème de Cauchy, G possède un élément d'ordre q.
Or tous les éléments de G, différents de 1, sont d'ordre une puissance non nulle de p donc q=p. Le seul diviseur premier de l'ordre de G est p donc G est un p-groupe. $\diamondsuit$

Regardons comment un p-sous-groupe de Sylow passe au sous-groupe et au quotient :

Proposition 4.5.9 *Soient G un groupe fini d'ordre divisible par un nombre premier p, N un sous-groupe normal de G d'ordre divisible par p et P un p-sous-groupe de Sylow de G. Alors,*
1)$P \cap N$ *est un p-sous-groupe de Sylow de N.*
2)PN/N *est un p-sous-groupe de Sylow de* G/N.

Démonstration *Posons* $|G| = sp^n$ *et* $|N| = s'p^m$ *où n et m sont des entiers strictement positifs,* $n \geq m$, *p ne divise pas s et s' divise s.*
1)Soit Q un p-sous-groupe de Sylow de N.
Q est un p-sous-groupe de N donc un p-sous-groupe de G.
D'où, d'après le Second Théorème de Sylow, il existe un p-sous-groupe de Sylow P' de G tel que Q est inclus dans P'.
Mais toujours d'après le Second Théorème de Sylow, il existe un élément g de G tel que $gP'g^{-1} = P$. *Donc,* gQg^{-1} *est inclus dans P.*
N étant normal dans G et Q étant inclus dans N, gQg^{-1} *est inclus dans N.*
D'où, gQg^{-1} *est inclus dans* $P \cap N$.
L'ordre de $P \cap N$ *divise les ordres de P et de N par le Théorème de Lagrange.*
D'où, P étant un p-sous-groupe de G, l'ordre de $P \cap N$ *est de la forme* p^a *avec* $0 \leq a \leq m$.
Puisque $P \cap N$ *contient le p-sous-groupe de Sylow* gQg^{-1}, $|P \cap N| \geq p^n$.
Ainsi, $|P \cap N| = p^n$ *et* $P \cap N$ *est donc un p-sous-groupe de Sylow de N.*
2)Par le Deuxième Théorème d'isomorphisme, PN/N *est isomorphe à* $P/P \cap N$.
D'où, $|PN/N| = |P/P \cap N| = p^{n-m}$ *car* $P \cap N$ *est un p-sous-groupe de Sylow de N.*
Comme $|G/N| = \frac{s}{s'}p^{n-m}$, PN/N *est un p-sous-groupe de Sylow de* G/N. $\diamondsuit$

Enonçons un des résultats les plus utiles découlant du Second Théorème de Sylow :

Proposition 4.5.10 *Soit G un groupe fini d'ordre divisible par un nombre premier p. Soit P un p-sous-groupe de Sylow de G.*
Alors, P est l'unique p-sous-groupe de Sylow de G si et seulement si P est normal dans G.

Démonstration *D'après le Second Théorème de Sylow, G opère transitivement par conjugaison sur $S_p(G)$.*
($\Rightarrow$) Pour tout élément g de G, gPg^{-1} est un p-sous-groupe de Sylow de G donc, par unicité, $gPg^{-1}=P$. P est normal dans G.
($\Leftarrow$) Soit Q un p-sous-groupe de Sylow de G. Il existe un élément g de G tel que $Q=gPg^{-1}$. Or $gPg^{-1}=P$ donc $Q=P$. P est l'unique p-sous-groupe de Sylow de G. $\diamondsuit$

Remarque *En particulier, si G est un groupe abélien fini d'ordre divisible par un nombre premier p alors G ne possède qu'un seul p-sous-groupe de Sylow.*

Cette Proposition est souvent utilisée pour démontrer la simplicité de certains groupes. Par exemple :

Corollaire 4.5.11 *Tout groupe fini d'ordre pq, où p et q sont deux nombres premiers distincts, n'est pas simple.*

Démonstration *Supposons $q<p$ et montrons que $n_p(G)=1$: par le Second Théorème de Sylow et le Corollaire 4.5.6, $n_p(G)$ divise q et est congru à 1 modulo p.*
Mais $1<q<p$ donc q ne peut être congru à 1 modulo p. D'où, $n_p(G)=1$.
G possède un unique p-sous-groupe de Sylow P donc, d'après la Proposition précédente, P est normal dans G.
P étant différent de $\{1\}$ et de G (car $1<p=|P|<pq=|G|$), G n'est pas simple. $\diamondsuit$

Avec des conditions supplémentaires, on a un meilleur résultat :

Proposition 4.5.12 *Soit G un groupe fini d'ordre pq où p et q sont deux nombres premiers distincts. Si p est non congru à 1 modulo q et q non congru à 1 modulo p alors G est cyclique, abélien et isomorphe à $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$.*

Démonstration *D'après le Second Théorème de Sylow et le Corollaire 4.5.6, $n_p(G)$ divise q et est congru à 1 modulo p.*
Comme q n'est pas congru à 1 modulo p, $n_p(G)=1$. De même, $n_q(G)=1$.
D'où, G possède un unique p-sous-groupe de Sylow P et un unique q-sous-groupe de Sylow Q. D'après la Proposition 4.5.10, P et Q sont normaux dans G.
P étant d'ordre p premier, P est cyclique engendré par un élément x (cf cours Sous-groupes normaux*). De même, Q est cyclique engendré par un élément y.*
Montrons que x et y commutent : d'après le Théorème de Lagrange, $|P\cap Q|$ divise $|P|=p$ et $|Q|=q$. Or p et q sont premiers entre eux donc $|P\cap Q|=1$ et $P\cap Q=\{1\}$.
Puisque P et Q sont normaux dans G, $xyx^{-1}y^{-1}$ appartient à $P\cap Q=\{1\}$.
D'où, $xy=yx$ et x et y commutent.
Montrons que xy engendre G : puisque x et y commutent $xy^{pq}=x^{pq}y^{pq}=1$ car x est d'ordre p et y est d'ordre q.

Soit m un entier strictement positif tel que $xy^m=1$.
On a alors $x^m y^m=1$ c'est à dire $x^m=y^{-m}$ et $y^{-m}=x^m$.
D'où, x^m et y^m appartiennent à $P\cap Q=\{1\}$.
On a donc $x^m=1$ ce qui entraîne que p divise m et $y^m=1$ qui implique que q divise m.
Ainsi, ppcm(p,q)=pq divise m.
D'où, xy est d'ordre $pq=|G|$. G est cyclique engendré par xy.
Puisque $|P\cap Q|=1$, on a $|PQ| = |P||Q|=pq=|G|$ (cf cours Produit semi-direct*) donc $G=PQ$.*
D'où, P et Q étant normaux dans G et $P\cap Q$ étant réduit à $\{1\}$, $G=PQ$ est isomorphe à $P\times Q$ (cf cours Produit semi-direct*).*
P étant cyclique d'ordre p, P est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (cf cours Groupes cycliques*).*
De même, Q est isomorphe à $\mathbb{Z}/q\mathbb{Z}$.
D'où, G est isomorphe à $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$. $\diamondsuit$

Remarques *1)Pour montrer que G est isomorphe à $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$, on pouvait aussi utiliser le Théorème chinois (cf Exercice 10 des cours* Congruence, groupes cycliques*) : G étant un groupe cyclique d'ordre pq, G est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$ groupe isomorphe à $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$.*
2)D'après cette Proposition, il n'y a qu'un seul groupe, à isomorphisme près, d'ordre pq où p et q sont deux nombres premiers distincts, p non congru à 1 modulo q et q non congru à 1 modulo p.
Par exemple, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ est le seul groupe, à isomorphisme près, d'ordre 15.

Considérons un cas plus général :

Proposition 4.5.13 *Soit G un groupe fini d'ordre $p_1^{n_1}...p_k^{n_k}$ où p_1, ... , p_k sont des nombres premiers distincts et n_1, ... , n_k des entiers strictement positifs.*
Si, pour tout i compris entre 1 et k, G ne possède qu'un seul p_i-sous-groupe de Sylow P_i alors $G=P_1...P_k$, G est isomorphe au produit direct $P_1\times...\times P_k$.

Démonstration *D'après la Proposition 4.5.10, P_i est normal dans G pour tout i compris entre 1 et k. D'où, l'ensemble $H=P_1...P_k$ est un sous-groupe normal de G (cf cours* Produit semi-direct*).*
Montrons que H est isomorphe à $P_1\times...\times P_k$: il suffit de montrer que $P_i\cap P_{i+1}...P_k$ est réduit à $\{1\}$ quel que soit l'entier i compris entre 1 et k-1 (cf cours Produit semi-direct*). Soit i compris entre 1 et k-1.*
D'après le Théorème de Lagrange, $|P_i\cap P_{i+1}...P_k|$ divise $|P_i|$ et $|P_{i+1}...P_k|$.
Si i=n-1 alors $|P_{i+1}...P_k| = |P_k|$.
Sinon, $|P_{i+1}...P_k| = \frac{|P_{i+1}||P_{i+2}...P_k|}{|P_{i+1}\cap(P_{i+2}...P_k)|}$ (cf cours Produit semi-direct*).*
D'où, quel que soit i compris entre 1 et k-1, $|P_{i+1}...P_k|$ divise $|P_{i+1}|$.
Par conséquent, $|P_i\cap P_{i+1}...P_k|$ divise $|P_i|$ et $|P_{i+1}|$.
Mais p_i et p_{i+1} sont premiers entre eux donc $|P_i\cap P_{i+1}...P_k|=1$ et $P_i\cap P_{i+1}...P_k=\{1\}$.
Ainsi, H est isomorphe à $P_1\times...\times P_k$.
On en déduit que $|H| = |P_1|...|P_k| = {p_1}^{n_1}...{p_k}^{n_k} = |G|$ et donc $G=H=P_1\times...\times P_k$. $\diamondsuit$

Corollaire 4.5.14 *Soit G un groupe abélien fini d'ordre $p_1^{n_1}...p_k^{n_k}$ où p_1, ... , p_k sont des nombres premiers distincts et n_1, ... , n_k des entiers strictement positifs.*
Alors, G est isomorphe au produit direct de ses p_i-sous-groupes de Sylow.

Démonstration *Puisque G est abélien, il ne possède, pour chaque i compris entre 1 et n, qu'un seul p_i-sous-groupe de Sylow. On applique alors la Proposition précédente.*
$\diamondsuit$

4.6 Exercices du Chapitre 4

Exercice 1 : Formule de Burnside : Soit G un groupe fini opérant sur un ensemble fini E. Montrer que le nombre d'orbites de E est égal à $\frac{1}{|G|}\sum_{g\in G}$ Card $\{x \in E \ / \ \text{g.x=x}\}$.

Exercice 2 : Soit G un groupe fini non réduit à l'élément neutre.
Soit p le plus petit nombre premier divisant |G|.
Montrer que tout sous-groupe H de G d'indice p (c'est à dire tel que [G :H]=p) est normal dans G.
Indication : Considérer l'opération par translations à gauche de H sur l'ensemble quotient $(G/H)_g$ de G par la relation ${}_HR$.

Exercice 3 : Soit H un groupe fini non réduit à l'élément neutre.
1)Montrer que le centre de H est stable par automorphisme de H.
2)Montrer qu'il existe un élément h de H d'ordre un nombre premier.
Soit G un groupe opérant fidèlement sur H tel que, pour tout élément g de G, la permutation (h→g.h) est un automorphisme de H.
3)On suppose que G opère transitivement sur H\{1}.
a)Montrer que tous les éléments de H, différents de 1, sont d'ordre une puissance non nulle d'un nombre premier p.
b)Montrer que H est abélien.
4)Montrer que si G opère 2-transitivement sur H\{1} alors soit tous les éléments de H sont d'ordre 2 soit H est d'ordre 3.
5)Montrer que si G opère 3-transitivement sur H\{1} alors H est d'ordre 4.
6)Montrer que si k≥4 alors G ne peut opérer k-fois transitivement sur H\{1}.

Exercice 4 : Soient G un groupe non réduit à l'élément neutre opérant sur un ensemble E et N un sous-groupe normal de G non réduit à l'élément neutre.
On suppose que N opère transitivement sur E et qu'il existe un élément x de E tel que $N_x = \{1\}$.
1)Montrer que l'opération de G_x sur E\{x} est équivalente à l'opération de conjugaison de G_x sur N\{1}.
2)On suppose que G opère m-fois transitivement sur E et que l'ensemble E est fini.
a)Montrer que si m=2 alors Card E=|N|=p^k où p est un nombre premier et k$\in \mathbb{N}^*$.
b)Montrer que si m=3 alors Card E=3 où Card E=2^k où k$\in \mathbb{N}^*$.
c)Montrer que si m=4 alors Card E=4.
d)Montrer qu'on ne peut pas avoir m≥5.
Indication : Utiliser l'Exercice précédent.

Exercice 5 : Un critère de simplicité : Soit G un groupe opérant fidèlement et primitivement sur un ensemble E de cardinal supérieur ou égal à 2.
On suppose que pour tout sous-groupe normal non réduit à {1} et pour tout élément x de E, N_x est différent de {1}.
Soit x un élément de E tel que G_x est simple.
Soit N un sous-groupe normal de G différent de {1}.
1)Montrer que N contient G_x.
2)Montrer que N=G.
3)En déduire que G est un groupe simple.

Exercice 6 : Théorème de Cauchy : Soit G un groupe fini d'ordre divisible par un nombre premier p. On pose X=$\{(x_1, \ldots ,x_p) \in G^p \ / \ x_1 \ldots x_p = 1\}$.
1)Montrer que Card X=$|G|^{p-1}$.
On identifie $\mathbb{Z}/p\mathbb{Z}$ avec l'ensemble {0, ... , p-1} muni de la loi de congruence modulo p (cf Chapitre 2 Section *Congruence*).
On définit une application de $\mathbb{Z}/p\mathbb{Z} \times X$ dans X par
$(k,(x_1, \ldots ,x_n)) \to k.(x_1, \ldots ,x_n)=(x_{1+k}, \ldots ,x_{p+k})$ où on identifie les indices avec leurs représentants modulo p compris entre 0 et p-1.
2)Montrer que l'on définit ainsi une application de $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble X.
3)Vérifier que l'orbite de e=(1, ... ,1) est réduite à $\{e\}$.
4)Soit x=$(x_1, \ldots ,x_n)$ un élément de X, différent de e, dont l'orbite est réduite à {x}.
Montrer que x_1 est un élément d'ordre p de G.
Dans la suite, on suppose que e est le seul élément de X dont l'orbite est réduite à un élément.
5)Soit x un élément de X. Montrer que le cardinal de l'orbite de x est p.
6)En déduire que le cardinal de X est de la forme 1+mp où m est un entier strictement positf.
7)Conclure.

Exercice 7 : Soient G un groupe, p un nombre premier divisant l'ordre de G et H un sous-groupe de G.
Montrer que si P est un p-sous-groupe de Sylow de G tel que $N_G(P) \subset H$ alors $N_G(P)=H$.

Exercice 8 : Soient G un groupe, N un sous-groupe normal de G et p un nombre premier divisant l'ordre de N.
Montrer que si P est un p-sous-groupe de Sylow de N alors $G=N.N_G(P)$.

Exercice 9 : Montrer qu'un groupe d'ordre pqr avec p, q et r premiers distincts n'est pas simple.

Exercice 10 : Montrer qu'un groupe G d'ordre 300 n'est pas simple.
Indication : On pourra considérer le noyau de l'opération de G sur $S_6(G)$.

Chapitre 5

Groupes symétriques et alternés

Groupe symétrique

Groupe alterné

5.1 Groupe symétrique

5.1.1 Groupe S_n

Soit n un entier naturel non nul.

Définition *On note S_n l'ensemble des permutations de l'ensemble $\{1, \ldots, n\}$ c'est à dire l'ensemble des bijections de $\{1, \ldots, n\}$ vers $\{1, \ldots, n\}$.*

Proposition 5.1.1 *$(S_n, \circ)$ est un groupe.*

Démonstration *L'identité est une permutation de $\{1, \ldots, n\}$ donc S_n n'est pas vide.*
La composée de deux bijections est une bijection donc on a une loi interne.
La composition est clairement associative.
L'identité est l'élément neutre pour la composition.
Enfin, tout élément de S_n est inversible d'inverse sa fonction réciproque. $\diamondsuit$

Définition *Le groupe S_n est appelé groupe symétrique de degré n.*

Propriété 5.1.2 *S_n est d'ordre n !.*

Démonstration *Soit σ appartenant à S_n.*
$\sigma(1)$ peut être n'importe quel des $1 \leq i \leq n$. On a donc n valeurs possibles.
$\sigma(2)$ peut être n'importe quel des $1 \leq i \leq n$ hormis la valeur $\sigma(1)$ puisque σ est injective.
On a donc n-1 valeurs possibles, ...
On arrive ainsi à $n \times n\text{-}1 \times \ldots \times 1 = n!$ bijections possibles. $\diamondsuit$

Propriété 5.1.3 *1)S_1 et S_2 sont abéliens.*
2)Pour $n \geq 3$, S_n n'est pas abélien.

Démonstration *1)$S_1 = \{Id\}$ donc S_1 est abélien. S_2 est composé de l'identité et de la permutation échangeant 1 et 2 donc S_2 est abélien donc S_2 est abélien.*
2)Soient i, j et k trois éléments distincts de $\{1, \ldots, n\}$.
Soit σ une application bijective qui à i associe j, à j associe i et qui fixe k. Soit ψ une application bijective qui à i associe k, à k associe i et qui fixe j.
Alors, $(\sigma \circ \psi)(i) = k$ et $(\psi \circ \sigma)(i) = j$ et donc $\sigma \circ \psi \neq \psi \circ \sigma$ et par conséquent S_n n'est pas abélien. $\diamondsuit$

Notations *1)Pour alléger les écritures, on notera, pour tout couple (σ, ψ) d'éléments de S_n, $\sigma\psi$ à la place de $\sigma \circ \psi$.*
On parlera de produit de deux permutations plutôt que de composition de deux permutations.

2)On peut écrire une permutation σ sous la forme suivante : $\begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$. *Ainsi, l'identité s'écrit* $\begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}$ *et* $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *est la permutation de* $\{1, 2, 3\}$ *qui envoie 1 sur 2, 2 sur 3 et 3 sur 1.*

Définition *Soit σ un élément de S_n.*
On appelle support de σ et on note Supp σ, l'ensemble des éléments i de $\{1, ... , n\}$ *tels que $\sigma(i) \neq i$.*

Exemple *Le support de l'identité est l'ensemble vide.*

Propriété 5.1.4 *Si deux éléments de S_n ont leurs supports disjoints alors ils commutent.*

Démonstration *Soient σ et ψ les deux éléments de S_n. Soit i compris entre 1 et n.*
Si i appartient au support de σ alors $\sigma(i)$ appartient au support de σ car si $\sigma(\sigma(i))=\sigma(i)$ alors $\sigma(i)=i$.
D'où, puisque les supports de σ et ψ sont disjoints, $\sigma(i)$ n'appartient pas au support de ψ et par conséquent $\sigma\psi(i)=\sigma(i)=\psi\sigma(i)$.
On a de même $\sigma\psi(i)=\psi(i)=\psi\sigma(i)$ si i appartient au support de ψ.
Si i n'appartient ni au support de σ ni au support de ψ alors $\sigma\psi(i)=i=\psi\sigma(i)$. $\diamondsuit$

Remarque *La réciproque est fausse.*
Par exemple, les permutations $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *et* $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ *commutent et elles ont le même support : l'ensemble* $\{1, 2, 3\}$.

5.1.2 Cycles

Soit n un entier naturel supérieur ou égal à 3.

Définition *Soient σ un élément de S_n et i compris entre 1 et n.*
On appelle σ-orbite de i et on note $\Omega_\sigma(i)$, l'ensemble $\{\sigma^k(i) \ / \ k \in \mathbb{N}\}$.

Remarque *S_n étant un groupe fini, tout élément de S_n est d'ordre fini (par le Théorème de Lagrange). L'ensemble $\Omega_\sigma(i)$ est donc fini.*

Définition *Soit k compris entre 1 et n. Un élément σ de S_n est un k-cycle, ou un cycle de longueur k, si il n'existe qu'une seule σ-orbite non réduite à un élément, celle-ci étant de cardinal k.*
Un 2-cycle est appelé une transposition.

Remarque *S_n ne possède qu'un seul 1-cycle : l'identité.*

Propriété 5.1.5 *Un k-cycle est d'ordre k.*

Démonstration *Soit $\Omega_\sigma(i)=\{i, \sigma(i), \ldots, \sigma^{k-1}(i)\}$ la seule σ-orbite non réduite à un élément. Puisque $\Omega_\sigma(i)$ est de cardinal k, $\sigma^k(i)$ appartient à $\Omega_\sigma(i)$.*
Les sigma^j(i) étant distincts pour tout j compris entre 1 et k-1, $\sigma^k(i)=i$.
Soit s, compris entre 1 et n, n'appartenant pas à $\Omega_\sigma(i)$.
Puisque $\Omega_\sigma(i)$ est la seule σ-orbite non réduite à un élément, $\Omega_\sigma(s)=\{s\}$.
D'où, $\sigma(s)=s$ et donc $\sigma^k(s)=s$.
On en déduit que $\sigma^k=Id$ et donc l'ordre de σ est inférieur ou égal à k.
Mais $\sigma^{k-1}(i)$ est différent de i (car $\Omega_\sigma(i)$ est de cardinal k) donc σ^{k-1} est différent de l'identité. D'où, l'ordre de σ est supérieur à k-1.
On en déduit que σ est d'ordre k. $\diamondsuit$

Remarque *La réciproque est fausse en général.*
Par exemple, la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ *est d'ordre 2 mais ce n'est pas une transposition puisqu'il y a deux orbites non réduites à un élément : {1, 2} et {3, 4}.*

Proposition 5.1.6 *Soient σ un élément de S_n et k compris entre 2 et n.*
σ est un k-cycle si et seulement si il existe $i_1, i_2, \ldots, i_k$, k éléments distincts de $\{1, \ldots, n\}$, tels que $\sigma(i_j)=i_{j+1}$ pour tout j compris entre 1 et k-1, $\sigma(i_k)=i_1$ et $\sigma(s)=s$ pour tout élément s de $\{1, \ldots, n\} \backslash \{i_1, \ldots, i_k\}$.

Démonstration *($\Rightarrow$) Soit $\Omega_\sigma(i)=\{i, \sigma(i), \ldots, \sigma^{k-1}(i)\}$ la seule σ-orbite non réduite à un élément. On pose, pour tout j compris entre 1 et k, $i_j = \sigma^{j-1}(i)$ (où $\sigma^0=Id$).*
La première condition est alors clairement vérifiée.

En reprenant la démonstration de la Propriété précédente, on constate que les deux dernières conditions sont également satisfaites.
($\Leftarrow$) D'après les deux premières conditions, $\Omega_\sigma(i_1)=\{i_1, \ldots, i_k\}$ est une σ-orbite de cardinal k et d'après la troisième condition, $\Omega_\sigma(i_1)$ est la seule σ-orbite non réduite à un élément donc σ est un k-cycle. $\diamondsuit$

Notation *Pour noter le k-cycle défini par $i_1, i_2, \ldots, i_k$, on utilise la notation suivante : $(i_1\ i_2\ \ldots\ i_k)$ qui se lit : i_1 donne i_2, ... , i_{k-1} donne i_k et i_k donne i_1.*
Il est d'usage de ne pas noter les éléments fixés par un cycle.
Par exemple, le 3-cycle (1 2 3) est la permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *dans S_3 et la permutation* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ *dans S_4.*
! Puisque la loi est la composition, les cycles sont lus de droite à gauche !
Par exemple, la permutation (1 2 3)(1 3 4) envoie 1 sur 1, 2 sur 3, 3 sur 4 et 4 sur 2.

Les cycles jouent un rôle très important dans l'étude des permutations puisque :

Théorème 5.1.7 *Toute permutation, différente de l'identité, se décompose en un produit de cycles de longueur supérieure ou égale à 2 et de supports deux à deux disjoints. De plus, cette décomposition est unique à l'ordre près d'écriture des cycles.*

Démonstration *Soit σ un élément de S_n.*
Existence : Montrons que les σ-orbites distinctes forment une partition de $\{1, \ldots, n\}$: Soit i compris entre 1 et n.
Puisque σ est surjective, il existe j compris entre 1 et n tel que $i=\sigma(j)\in \Omega_\sigma(j)$. D'où, la réunion des σ-orbites est $\{1, \ldots, n\}$.
Soient $\Omega_\sigma(i)$ et $\Omega_\sigma(j)$ deux σ-orbites distinctes.
Supposons qu'il existe un élément appartenant à $\Omega_\sigma(i)$ et $\Omega_\sigma(j)$.
Il existe alors des entiers naturels k et m tels que $\sigma^k(i)=\sigma^m(j)$.
Supposons $k\geq m$. On a alors $\sigma^{k-m}(i)=j$.
D'où, j appartient à $\Omega_\sigma(i)$ et par conséquent, $\Omega_\sigma(i)=\Omega_\sigma(j)$. Contradiction.
D'où, les ensembles $\Omega_\sigma(i)$ et $\Omega_\sigma(j)$ sont disjoints.
Les σ-orbites distinctes forment une partition de $\{1, \ldots, n\}$.
Considérons les σ-orbites distinctes $\Omega_1, \ldots, \Omega_r$ non réduites à un élément et les restrictions $\sigma_1, \ldots, \sigma_r$ de σ à ces σ-orbites.
Pour tout i compris entre 1 et r, σ_i est un cycle puisqu'il n'y a qu'une seule orbite non ponctuelle : Ω_i. De plus, ce cycle est de longueur supérieure ou égale à 2.
Puisque les σ-orbites sont disjointes, les cycles $\sigma_1, \ldots, \sigma_r$ ont leurs supports disjoints.
Il reste à montrer que $\sigma=\sigma_1 \ldots \sigma_r$. Soit i compris entre 1 et n.
Si $\sigma(i)=i$ alors $\Omega_\sigma(i)=\{i\}$ donc i n'apparaît dans aucun support de $\sigma_1, \ldots, \sigma_r$ et par conséquent, $i=\sigma_1 \ldots \sigma_r(i)$.

Supposons que $\sigma(i)\neq i$. Il existe alors un entier j compris entre 1 et r tel que i appartient à $\Omega_\sigma(j)$. D'où, $\sigma_j(i)=\sigma(i)$ (par définition des σ-orbites) et, puisque les σ-orbites sont disjointes, $\sigma_k(i)=i$ pour tout entier k compris entre 1 et r, différent de j.
On en déduit que $\sigma_1 \ldots \sigma_r(i)=\sigma(i)$.
D'où, $\sigma_1 \ldots \sigma_r$.
Unicité : Soit $\sigma_1 \ldots \sigma_r$ une décomposition de σ en un produit de cycles de longueur supérieure ou égale à 2 et de supports disjoints.
Puisque les supports des cycles sont deux à deux disjoints, les cycles commutent d'après la Propriété 5.1.4. C'est pourquoi, l'ordre d'écriture ne joue aucun rôle dans la décomposition.
Soit $\psi_1, \ldots, \psi_k$ une autre décomposition de σ en un produit de cycles de longueur supérieure ou égale à 2 et de supports disjoints.
Soient $\Theta_1, \ldots, \Theta_k$ les orbites associées aux cycles $\psi_1, \ldots, \psi_k$.
Puisque les supports sont deux à deux disjoints, on a $\psi_i(j)=\sigma(j)$ pour tout entier i compris entre 1 et k et pour tout entier j compris entre 1 et n.
D'où, les $\Theta_1, \ldots, \Theta_k$ sont des σ-orbites non ponctuelles.
Puisque $\sigma=\psi_1 \ldots \psi_k$, les $\Theta_1, \ldots, \Theta_k$ sont les σ-orbites non ponctuelles.
D'où, $k=r$ et à l'ordre d'écriture près $\psi_i = \sigma_i$. $\diamondsuit$

Remarques *1)L'unicité de la décomposition à l'ordre d'écriture près s'entend également à multiplication par l'identité près.*
Par exemple dans S_5, les décompositions (1 2 3)(4 5) et (1 2 3)(1 2)(4 5)(1 2) sont les mêmes puisque (1 2)(1 2)=Id ((1 2) et (4 5) commutent car leurs supports sont deux à deux disjoints (Propriété 5.1.4)).
2)En raison du Théorème précédent, on utilisera la notation par cycles pour décrire les éléments de S_n.

Corollaire 5.1.8 *1)S_n est engendré par l'ensemble des transpositions.*
2)S_n est engendré par l'ensemble des translations (i i+1), $1\leq i\leq n-1$.
3)S_n est engendré par l'ensemble des translations (1 i), $2\leq i\leq n$.

Démonstration *1)D'après le Théorème précédent, il suffit de montrer que tout k-cycle $(i_1\ i_2 \ldots i_k)$ se décompose en un produit de transpositions.*
On a $(i_1\ i_2 \ldots i_k)=(i_1\ i_2)(i_2\ i_3) \ldots (i_{k-1}\ i_k)$ d'où le résultat.
2)Soit (s t) une transposition avec $s\leq t$ (on a (s t)=(t s)).
On a (s t)=(s s+1) ... (t-1 t)(t-1 t-2) ... (s+1 s) donc, d'après le 1, S_n est engendré par l'ensemble des translations (i i+1), $1\leq i\leq n-1$.
3)Soit i compris entre 1 et n. On a (i i+1)=(1 i)(1 i+1)(1 i) d'où, d'après le 2, S_n est engendré par l'ensemble des translations (1 i), $2\leq i\leq n$. $\diamondsuit$

Définition *Soient $k_1 \leq \ldots \leq k_r$ des entiers compris entre 2 et n tels que $k_1+ \ldots +k_r \leq n$. On appelle $k_1\times\ldots\times k_r$-cycle, la permutation obtenue comme produit d'un k_1-cycle, ... , d'un k_r-cycle, de supports deux à deux disjoints.*

Remarque *Le Théorème précédent indique que tout élément de S_n est un $k_1\times \ldots \times k_r$-cycle.*

Par exemple, l'élément de S_7 défini par $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 1 & 5 & 4 & 7 & 2 \end{pmatrix}$ *est le $2\times2\times3$-cycle (1 3)(4 5)(2 6 7).*

La mise sous forme d'un $k_1\times...\times k_r$-cycle permet de trouver facilement l'ordre d'un élément de S_n :

Propriété 5.1.9 *L'ordre d'un $k_1\times...\times k_r$-cycle est égal au ppcm des ordres des cycles composant ce $k_1\times...\times k_r$-cycle.*

Démonstration *Notons σ_i, $1\leq i\leq r$, les cycles composant le $k_1\times...\times k_r$-cycle σ.*
Soit p le ppcm des ordres des cycles σ_i, $1\leq i\leq r$.
On a alors $\sigma_i^p=Id$ pour tout i compris entre 1 et r.
Puisque les supports des cycles sont deux à deux disjoints, les cycles commutent deux à deux d'après la Propriété 5.1.4.
D'où, $\sigma^p=\sigma_1^p$ ... $\sigma_r^p=Id$ et par conséquent, l'ordre de σ divise p.
Soit m un entier strictement positif tel que $\sigma^m=Id$.
On a alors σ_1^m ... $\sigma_r^m=Id$ et donc $\sigma_1^m=\sigma_r^{-m}$ ... σ_2^{-m}.
Si $\sigma_1^m\neq Id$ alors il existe s, compris entre 1 et n, appartenant au support de σ_1^m.
D'où, s appartient au support de σ_1^m et de σ_r^{-m} ... σ_2^{-m} ce qui est impossible puisque $Supp(\sigma_i^{-m})=Supp(\sigma_i^m)\subset Supp(\sigma_i)$ pour i compris entre 2 et r et les supports de σ_1, ... σ_r sont deux à deux disjoints.
D'où, $\sigma_1^m=Id$ et l'ordre de σ_1 divise donc m.
On montre de même, pour tout i compris entre 2 et r, que $\sigma_i^m=Id$ et que l'ordre de σ_i divise donc m. D'où, p divise m et par conséquent, p=m.
L'ordre de σ est le ppcm des ordres des σ_i, $1\leq i\leq r$. $\diamondsuit$

Exemple *La permutation définie dans la remarque précédente est d'ordre 6.*

5.1.3 Classes de conjugaison

Soit n un entier naturel supérieur ou égal à 3.

Proposition 5.1.10 *Soit $(i_1$ ... $i_k)$ un k-cycle.*
Alors, pour tout élément α de S_n, $\alpha(i_1$ ... $i_k)\alpha^{-1}=(\alpha(i_1)$ ... $\alpha(i_k))$

Démonstration *Posons $\sigma=(i_1$ ... $i_k)$, $\varphi=(\alpha(i_1)$ ... $\alpha(i_k))$ et $\psi=\alpha\sigma\alpha^{-1}$.*
Soit i compris entre 1 et n. Montrons que $\psi(i)=\varphi(i)$:
Si $\alpha^{-1}(i)$ appartient au support de σ alors il existe j compris entre 1 et k tel que $\alpha^{-1}(i)=i_j$. D'où, $\psi(i)=\alpha(i_{j+1})$ (où pour j=k, on pose $i_{k+1}=i_1$).
On a $i=\alpha(\alpha^{-1}(i))=\alpha(i_j)$ donc $\varphi(i)=\alpha(i_{j+1})=\psi(i)$.
Si $\alpha^{-1}(i)$ n'appartient pas au support de σ alors $\psi(i)=\alpha(\alpha^{-1}(i))=i$.
Si i appartient au support de φ alors il existe j compris entre 1 et k tel que $i=\alpha(i_j)$.

On a alors $\alpha^{-1}(i)=i_j$ qui appartient au support de σ. Contradiction.
D'où, i n'appartient pas au support de φ et $\varphi(i)=i=\psi(i)$.
Pour tout i compris entre 1 et n, $\psi(i)=\varphi(i)$ donc $\psi=\varphi$ c'est à dire
$\alpha(i_1 \dots i_k)\alpha^{-1}=(\alpha(i_1) \dots \alpha(i_k))$. $\diamondsuit$

Exemple *Pour n=6, σ=(1 3 4) et α=(1 2)(3 5 6), on a $\alpha\sigma\alpha^{-1}$=(2 5 4).*

Corollaire 5.1.11 *La classe de conjugaison d'un $k_1\times\dots\times k_r$-cycle est l'ensemble des $k_1\times\dots\times k_r$-cycle.*

Démonstration *Soit $\sigma=\sigma \dots \sigma_r$ un $k_1\times\dots\times k_r$-cycle.*
Pour tout élément α de S_n, $\alpha\sigma\sigma^{-1}=\alpha\sigma_1\sigma^{-1} \dots \alpha\sigma_r\sigma^{-1}$ donc, d'après la Proposition précédente, $\alpha\sigma\sigma^{-1}$ est un $k_1\times\dots\times k_r$-cycle.
Soit φ un $k_1\times\dots\times k_r$-cycle.
Posons $\sigma=(i_1^1 \dots i_{k_1}^1) \dots (i_1^r \dots i_{k_r}^r)$ et $\varphi=(j_1^1 \dots j_{k_1}^1) \dots (j_1^r \dots j_{k_r}^r)$.
Définissons α par $\alpha(i_s^t)=j_s^t$, pour tout t compris entre 1 et r et pour tout s compris entre 1 et k_t, et α bijective de $\{1, \dots, n\}\backslash\{i_1^1, \dots, i_{k_r}^r\}$ vers $\{1, \dots, n\}\backslash\{j_1^1, \dots, j_{k_r}^r\}$ (ce qui est possible car ces deux derniers ensembles ont le même cardinal).
Puisque les supports des cycles sont deux à deux disjoints, α est une application injective. De plus, α est surjective par construction donc α appartient à S_n.
D'après la Proposition précédente, $\alpha\sigma\alpha^{-1}=\varphi$ donc φ et σ sont conjugués.
D'où, la classe de conjugaison du $k_1\times\dots\times k_r$-cycle σ est l'ensemble des $k_1\times\dots\times k_r$-cycles. $\diamondsuit$

5.1.4 Signature

Soit n un entier naturel supérieur ou égal à 3.

Définition *Soit σ appartenant à S_n. On appelle <u>signature</u> de σ et on note sgn(σ), l'entier $(-1)^{n-n_\sigma}$ où n_σ est le nombre de σ-orbites.*
Si sgn(σ)=1 (respectivement sgn(σ)=-1) alors on dit que σ est une permutation <u>paire</u> (respectivement <u>impaire</u>).

Proposition 5.1.12 *Un k-cycle est une permutation impaire si k est pair et une permutation paire si k est impaire.*

Démonstration *Un k-cycle σ a une seule orbite non ponctuelle et celle-ci est de cardinal k. On a donc 1+(n-k) orbites et par conséquent sgn(σ)=$(-1)^{k-1}$.* $\diamondsuit$

Propriété 5.1.13 *Soient σ une permutation et τ une transposition.*
Alors, sgn($\sigma\tau$)=-sgn(σ).

Démonstration *Posons τ=(i j). Si i et j n'appartiennent pas au support de σ alors $\{i, j\}$ et Supp σ sont des $\sigma\tau$-orbites. Les autres éléments de $\{1, \ldots, n\}$ ont leurs σ-orbite et $\sigma\tau$-orbite réduites à eux-mêmes. Puisque les σ-orbites $\{i\}$ et $\{j\}$ sont devenues une $\sigma\tau$-orbite $\{i, j\}$, on a $n_{\sigma\tau} = n_\sigma - 1$ et donc sgn($\sigma\tau$)=-(-1)$^{n-n_\sigma}$=-sgn(σ).*
Si i appartient au support de σ et j n'appartient pas au support de σ alors $\sigma\tau$ envoie σ^{-1}(i) sur i (σ^{-1}(i)$\neq$i, j), i sur j et j sur σ(i) alors que σ envoie σ^{-1}(i) sur i, i sur σ(i) et j sur j. D'où, les σ-orbites Ω_σ(i) et Ω_σ(j)=$\{j\}$ deviennent la $\sigma\tau$-orbite $\Omega_{\sigma\tau}$(i). Les autres éléments de $\{1, \ldots, n\}$ ont leurs σ-orbite et $\sigma\tau$-orbite réduites à eux-mêmes donc $n_{\sigma\tau} = n_\sigma - 1$ et par conséquent, sgn($\sigma\tau$)=-sgn(σ).
Si i et j appartiennent au support de σ alors deux cas se présentent selon que i et j sont dans le support d'un même cycle composant σ.
Si i et j apparaissent dans des supports différents alors $\sigma\tau$ envoie i sur σ(j), σ(j) sur σ^2(j), ..., σ^{k-1}(j) sur j, j sur σ(i), σ(i) sur σ^2(i), ..., σ^{m-1}(i) sur i où k (respectivement m) désigne la longueur du cycle dont j (respectivement i) est un élément du support. D'où, les σ-orbites Ω_σ(i) et Ω_σ(j) deviennent la $\sigma\tau$-orbite $\Omega_{\sigma\tau}$(i).
Les autres orbites restant inchangées, on a $n_{\sigma\tau} = n_\sigma - 1$ et donc sgn($\sigma\tau$)=-sgn(σ).
Il reste le cas où i et j sont des éléments du support d'un cycle composant σ.
Supposons d'abord que σ(j)=i.
Si σ(i)=j alors le cycle auquel appartiennent i et j est (i j) donc $\sigma\tau$ est la permutation composée des cycles, différent de τ, composant σ.
Dans ce cas, il y a n_σ-1 orbites ce qui entraîne que sgn($\sigma\tau$)=-sgn(σ).
Si σ(i) est différent de j alors $\sigma\tau$ envoie i sur i et j sur σ(i), σ(i) sur σ^2(i), ..., σ^{k-2}(i) sur σ^{k-1}(i)=σ^{-1}(i)=j où k désigne la longueur du cycle dont i et j sont des éléments du support.
D'où, la σ-orbite Ω_σ(i) devient les $\sigma\tau$-orbites $\Omega_{\sigma\tau}$(i)=$\{i\}$ et $\Omega_{\sigma\tau}$(j). Puisque les autres orbites restent inchangées, on a $n_{\sigma\tau} = n_\sigma + 1$ et donc
sgn($\sigma\tau$)=$(-1)^{-1}(-1)^{n-n_\sigma}$=-sgn($\sigma$).
On a les mêmes résultats si on suppose que σ(i)=j.
Supposons pour finir que σ(j) est différent de i et que σ(i) est diférent de j.
Alors $\sigma\tau$ envoie i sur σ(j), σ(j) sur σ^2(j), ..., σ^{-2}(i) sur σ^{-1}(i) et σ^{-1}(i) sur i.
De plus, $\sigma\tau$ envoie j sur σ(i), σ(i) sur σ^2(i), ..., σ^{-2}(j) sur σ^{-1}(j) et σ^{-1}(j) sur j.
D'où, la σ-orbite Ω_σ(i)=Ω_σ(j) devient les $\sigma\tau$-orbites $\Omega_{\sigma\tau}$(i) et $\Omega_{\sigma\tau}$(j).
Les autres orbites restant inchangées, on a $n_{\sigma\tau} = n_\sigma + 1$ et donc sgn($\sigma\tau$)=-sgn(σ). $\diamondsuit$

Corollaire 5.1.14 *La signature est un homomorphisme surjectif de S_n vers $\{\pm 1, \times\}$.*

Démonstration *Soient σ et ψ deux éléments de S_n.*
D'après la première propriété du Corollaire 5.1.8, ψ se décompose en un produit τ_1 ... τ_k de translations.
D'où, d'après la Propriété précédente, sgn($\sigma\psi$)=-sgn($\sigma\tau_1$ ... τ_{k-1})= ... =(-1)^{k}sgn(σ).
D'après la Propriété précédente et la Proposition 5.1.12, sgn(ψ)=-sgn(τ_1 ... τ_{k-1})= ... =(-1)$^{k-1}$sgn(τ_1)=(-1)^k donc sgn($\sigma\psi$)=sgn(σ)sgn(ψ).
sgn est un homomorphisme de S_n vers $\{\pm 1, \times\}$.
D'après la Proposition 5.1.12, la signature de l'identité est 1 et la signature d'une transposition est -1 donc sgn est un homomorphisme surjectif. $\diamondsuit$

5.2 Groupe alterné

Dans cette section, on va étudier le noyau de l'homomorphisme sgn.
Soit n un entier naturel supérieur ou égal à 3.

5.2.1 Groupe A_n

Définition *On appelle groupe alterné de degré n et on note A_n, le noyau de l'homomorphisme sgn de S_n dans $\{\pm 1\}$.*

Proposition 5.2.1 *A_n est un sous-groupe normal propre de S_n, d'ordre $\frac{n!}{2}$.*

Démonstration *Puisque A_n est le noyau d'un homomorphisme partant de S_n, A_n est un sous-groupe normal de S_n. Puisque la signature d'une transposition est -1 et la signature d'un 3-cycle est 1, A_n est un sous-groupe normal propre de S_n.*
D'après le Premier Théorème d'isomorphisme, S_n/A_n est isomorphe à Im sgn.
Mais sgn est un homomorphisme surjectif d'après le Corollaire 5.1.14 donc Im sgn=$\{\pm 1\}$.
D'où, $|S_n/A_n| = \frac{|S_n|}{|A_n|}$=2 et donc $|A_n| = \frac{n!}{2}$. $\diamondsuit$

Proposition 5.2.2 *1)A_3 est abélien.*
2)Pour n>3, A_n n'est pas abélien.

Démonstration *1)A_3 étant d'ordre 3, A_3 est isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et est donc abélien.*
2)On a (1 2 3)(1 2 4)=(1 3)(2 4) et (1 2 4)(1 2 3)=(1 4)(2 3) donc A_n n'est pas abélien. $\diamondsuit$

Proposition 5.2.3 *A_n est engendré par les 3-cycles.*

Démonstration *D'après la Proposition 5.1.12, les 3-cycles sont des éléments de A_n.*
Soit σ un élément de A_n. D'après le Corollaire 5.1.8, σ se décompose en un produit τ_1 ... τ_k de transpositions de la forme (1 i).
Puisque σ appartient à A_n, sgn(σ)=1 donc, d'après le Corollaire 5.1.14 et la Proposition 5.1.12, $(-1)^k$=1.
D'où, k est pair et on peut regrouper les transpositions composant σ, deux par deux.
Si i est différent de j alors (1 i)(1 j)=(1 j i) donc σ se décompose en un produit de 3-cycles. A_n est engendré par les 3-cycles. $\diamondsuit$

5.2.2 Classes de conjugaison

La Proposition 5.1.10 reste valable dans A_n. Cependant le Corollaire 5.1.11 tombe en défaut car les permutations construites pour rendre conjugués deux $k_1\times$ ... k_r-cycles, n'appartiennent pas forcément à A_n. Par exemple, la classe de conjugaison de (1 2 3) dans A_4 est {(1 2 3), (1 3 4), (1 4 2), (2 4 3)} qui n'est pas l'ensemble des 3-cycles. Les 3-cycles manquants forment la classe de conjugaison de (1 3 2).
Toutefois, on a le résultat suivant qui nous sera utile dans la section suivante :

Proposition 5.2.4 *Si n≥5 alors la classe de conjugaison d'un 3-cycle est l'ensemble des 3-cycles.*

Démonstration *Soit σ=(i_1 i_2 i_3) un 3-cycle.*
D'après la Proposition 5.1.10, les conjugués de σ sont des trois cycles.
Soit φ=(j_1 j_2 et j_3) un autre 3-cycle.
On définit α par $\alpha(i_s)=j_s$ pour tout i compris entre 1 et 3 et α bijective de $\{1, \dots, n\}\backslash\{i_1, i_2, i_3\}$ vers $\{1, \dots, n\}\backslash\{j_1, j_2, j_3\}$ (ce qui est possible car ces deux derniers ensembles ont le même cardinal.
On vérifie comme dans la démonstration du Corollaire 5.1.11, que α appartient à S_n et $\alpha\sigma\alpha^{-1}=\varphi$.
Si α appartient à A_n alors σ et φ sont conjugués dans A_n.
Sinon, soit s et t deux éléments distincts de $\{1, \dots, n\}\backslash\{j_1, j_2, j_3\}$ (possible car n≥5). Posons τ=(s t). D'après le Corollaire 5.1.14 et la Proposition 5.1.12, $\tau\alpha$ appartient à A_n. Puisque φ et τ ont leurs supports disjoints, φ et τ commutent (Propriété 5.1.4) donc $\tau\varphi\tau^{-1}=\varphi$. D'où, $\varphi=(\tau\alpha)\sigma(\tau\alpha)^{-1}$ et σ et φ sont conjugués dans A_n.
La classe de conjugaison de σ dans A_n est l'ensemble des 3-cycles. $\diamondsuit$

5.2.3 Simplicité

Sous-groupe normaux de A_n et S_n

Proposition 5.2.5 *A_3 est un groupe simple.*

Démonstration *A_3 est d'ordre 3 donc A_3 est isomorphe au groupe simple $\mathbb{Z}/3\mathbb{Z}$.* $\diamondsuit$

Corollaire 5.2.6 *Les sous-groupes normaux de S_3 sont $\{Id\}$, A_3 et S_3.*

Démonstration *Soit N un sous-groupe normal de S_3.*
D'après le Théorème de Lagrange, N est d'ordre 1, 3 ou 6.
Si N est d'ordre 1 alors N=$\{Id\}$ et si N est d'ordre 6 alors N=S_3.
Supposons N d'ordre 3.
Si N contient une transposition alors N contient toutes les transpositions d'après le Corollaire 5.1.11.
D'où, N=S_3 d'après le Corollaire 5.1.8. Contradiction.
D'où, N est constitué par l'identité et les 3-cycles c'est à dire N=A_3. $\diamondsuit$

Proposition 5.2.7 *L'ensemble formé de l'identité et des 2×2-cycles est un sous-groupe normal abélien de A_4, d'ordre 4.*

Démonstration *Pour la structure de sous-groupe abélien, la vérification est immédiate à partir des éléments (1 2)(3 4), (1 3)(2 4) et (1 4)(2 3).*
La normalité du sous-groupe découle de la Proposition 5.1.10. ♢

Définition *Le groupe défini dans la Proposition précédente est noté V_2.*

Proposition 5.2.8 *Les sous-groupes normaux de $\{Id\}$, V_2 et A_4.*

Démonstration *Soit N un sous-groupe normal de A_4 non réduit à $\{Id\}$.*
On vérifie facilement qu'il y a 8 3-cycles dans A_4.
D'où, puisque l'ordre de N doit diviser l'ordre de A_4=12 d'après le Théorème de lagrange, N contient au moins un 2×2-cycle.
D'après la Proposition 5.1.10, les conjugués (dans A_n) de (1 2)(3 4) sont des 2×2-cycles. Comme (1 2 3)(1 2)(3 4)(1 3 2)=(1 4)(2 3) et
(2 3 4)(1 2)(3 4)(2 4 3)=(1 3)(2 4), la classe de conjugaison d'un 2×2-cycle est l'ensemble des 2×2-cycles.
D'où, N contient l'ensemble des 2×2-cycles.
Si N n'a pas d'autre élément que les 2×2-cycles et l'identité alors N=V_2.
Sinon, N contient un 3-cycle (i j k). Soit s l'entier compris entre 1 et 4, différent de i,j et k.
On a (i j s)(i j k)(i s j)=(j s k) et (i s j)(i j k)(i j s)=(i k s) donc N contient au moins 3 3-cycles. D'où, puisque N possède 3 2×2-cycles et l'identité, N a un ordre au moins égal à 7. La seule possibilité est |N|=24 c'est à dire N=A_4. ♢

Corollaire 5.2.9 *Les sous-groupes normaux de S_4 sont $\{Id\}$, V_2, A_4 et S_4.*

Démonstration *Soit N un sous-groupe normal de S_4 non réduit à $\{Id\}$.*
Si N contient une transposition alors N=S_4 (Corollaire 5.1.11 et Corollaire 5.1.8).
Si N contient un 3-cycle alors A_n est inclus dans S_n (Corollaire 5.1.11 et Proposition 5.2.3). Mais |N| divise |G| par le Théorème de Lagrange donc $|N| \leq \frac{|S_n|}{2} = |A_n|$.
D'où, N=A_n.
Supposons que N ne contient aucune transposition et aucun 3-cycle.
Si N contient un 2×2-cycle alors N contient tous les 2×2-cycles d'après le Corollaire 5.1.11 et V_2 est donc inclus dans N.
Si N contient un 4-cycle alors N contient tous les 4-cycles d'après le Corollaire 5.1.11. Dans S_4, il y a 6 4-cycles donc si N n'est constitué que de l'identité et des 4-cycles, N est d'ordre 7 ce qui contredit le Théorème de Lagrange.
D'où, N contient un 2×2-cycle et donc N contient V_2.
On a alors N d'ordre 10 ce qui contredit encore le Théorème de Lagrange.
D'où, les sous-groupes normaux de S_4 sont $\{Id\}$, V_2, A_4 et S_4. ♢

Le résultat le plus important de ce paragraphe est le suivant :

Théorème 5.2.10 *Pour n≥5, le groupe A_n est simple.*

Démonstration *Soit N un sous-groupe normal de A_n, différent de $\{Id\}$.*
On va montrer que H=A_n.
D'après la Proposition 5.2.3, il suffit de montrer que N contient l'ensemble des 3-cycles de S_n.
Puisque N est normal dans A_n et les 3-cycles sont conjugués dans A_n (Proposition 5.2.4), il suffit de montrer que N contient un 3-cycle.
Soit σ un élément de N, différent de Id.
Soient i appartenant au support de σ, j=σ(i), k$\in$ $\{1, \ldots, n\}\backslash\{i, j, \sigma^{-1}(i)\}$ (possible car n≥4) et m=σ(k). On pose α=(i j k).
Puisque N est un sous-groupe normal de A_n, $\theta = \alpha^{-1}\sigma\alpha\sigma^{-1}$ appartient à N.
De plus, d'après la Proposition 5.1.10, θ=(i k j)(j σ(j) m).
D'où, θ est un 3-cycle ou un 2×2-cycle ou un 5-cycle selon les valeurs de σ(j) et m.
Cas où θ est un 2×2-cycle (a b)(c d) :
Soit e un élément de $\{1, \ldots, n\}\backslash\{a, b, c, d\}$ (possible car n≥5).
Puisque N est un sous-groupe normal de A_n, (a b e)$^{-1}\theta$(a b e)θ^{-1} appartient à N.
Puisque (a b e)$^{-1}$(a b)(c d)(a b e)((a b)(c d))$^{-1}$=
(a e b)((a b)(c d)(a b e)((a b)(c d))$^{-1}$)=(a e b)(b a e)=(a b e), N contient un 3-cycle.
Cas où θ est un 5-cycle (a b c d e) :
Puisque N est un sous-groupe normal de A_n, (a b c)$^{-1}\theta$(a b c)θ^{-1} appartient à N.
Puisque (a b c)$^{-1}\theta$(a b c)θ^{-1}=(a c b)θ(a b c)θ^{-1}=(a c b)(b c d)=(a c d), N contient un 3-cycle.
N contient toujours un 3-cycle donc N=A_n $\diamondsuit$

Corollaire 5.2.11 *Pour n≥5, les seuls sous-groupes normaux de S_n sont $\{Id\}$, A_n et S_n.*

Démonstration *Soit N un sous-groupe normal propre de S_n.*
Puisque N est un sous-groupe normal de S_n, N$\cap A_n$ est un sous-groupe normal de A_n.
D'où, d'après le Théorème précédent, $N\cap A_n = \{Id\}$ ou $N\cap A_n = A_n$.
Si $N\cap A_n = A_n$ alors A_n est inclus dans N.
Mais, d'après le Théorème de Lagrange, |N| divise $|S_n|$ donc, puisque H est différent de S_n, $|N| \leq \frac{|S_n|}{2} = |A_n|$. D'où, N=$A_n$.
Etudions le cas où $N\cap A_n = \{Id\}$:
Puisque N et A_n sont normaux dans S_n et puisque $N\cap A_n = \{Id\}$, NA_n est isomorphe à N×A_n. D'où, $|NA_n| = |N||A_n|$.
Si |N|>2 alors $|NA_n|>2|A_n|>|S_n|$. Mais NA_n est inclus dans S_n donc $|NA_n| \leq |S_n|$. Contradiction.
Puisque N est différent de $\{Id\}$, il reste le cas où |N|=2.
Si N=$\{Id, (i\ j)\}$ alors, comme N est normal dans S_n, N contient l'ensemble des transpositions d'après le Corollaire 5.1.11. D'où, |N|>2. Contradiction. $\diamondsuit$

On résume les résultats de cette section dans le tableau suivant :

n	$sous-groupes\ normaux\ de\ A_n$	$sous-groupes\ normaux\ de\ S_n$
3	$\{Id\}$, A_3	$\{Id\}$, A_3, S_3
4	$\{Id\}$, V_2, A_4	$\{Id\}$, V_2, A_4, S_4
≥ 5	$\{Id\}$, A_n	$\{Id\}$, A_n, S_n

Nous allons maintenant appliquer ces résultats pour déterminer les centres et les groupes dérivés de S_n et A_n.

Proposition 5.2.12 *1)$Z(A_3)=A_3$ et $Z(S_3)=\{Id\}$.*
2)$Z(A_4)=\{Id\}$ et $Z(S_4)=\{Id\}$.
3)Pour $n\geq 5$, $Z(A_n)=\{Id\}$ et $Z(S_n)=\{Id\}$.

Démonstration *$Z(A_n)$ est un sous-groupe normal de A_n et $Z(S_n)$ est un sous-groupe normal de S_n.*
1)A_3 est abélien donc $Z(A_3)=S_3$.
D'après la Proposition 5.2.6, $Z(S_3)=\{Id\}$, A_3 ou S_3.
S_3 n'est pas abélien donc $Z(S_3)\neq \{S_3\}$.
On a (1 2)(1 2 3)(1 2)=(1 3 2) donc (1 2 3) n'appartient pas à $Z(S_3)$ et par conséquent, A_3 n'est pas inclus dans $Z(S_3)$. D'où, $Z(S_3)=\{Id\}$.
2)D'après la Proposition 5.2.8 et le Corollaire 5.2.9, $Z(A_4)=\{Id\}$, V_2 ou A_4 et $Z(S_4)=\{Id\}$, V_2, A_4 ou S_4.
A_4 et S_4 n'étant pas abéliens, $Z(A_4)\neq A_4$ et $Z(S_4)\neq S_4$.
On a (1 2 3)(1 2)(3 4)(1 3 2)=(2 3)(1 4) donc (1 2)(3 4) n'appartient ni à A_4 ni à S_4. D'où, V_2 n'est inclus ni dans $Z(A_4)$ ni dans $Z(S_4)$.
Par conséquent, $Z(A_4)=\{Id\}$ et $Z(S_4)=\{Id\}$.
3)D'après la Proposition 5.2.10 et le Corollaire 5.2.11, $Z(A_n)=\{Id\}$ ou A_4 et $Z(S_n)=\{Id\}$, A_n ou S_n.
A_n n'est pas abélien donc $Z(A_n)\neq A_n$ et par conséquent, $Z(A_n)=\{Id\}$.
S_n n'est pas abélien donc $Z(S_n)\neq S_n$.
On a (1 2 4)(1 2 3)(1 4 2)=(2 4 3) donc (1 2 3) n'appartient pas à $Z(S_n)$.
D'où, A_n n'est pas inclus dans $Z(S_n)$ et donc $Z(S_n)=\{Id\}$. $\diamondsuit$

Etudions les groupes dérivés des groupes S_n et A_n :

Proposition 5.2.13 *1)$D(A_3)=\{Id\}$ et $D(S_3)=A_3$.*
2)$D(A_4)=V_2$ et $D(S_4)=A_4$.
3)Pour $n\geq 5$, $D(A_n)=A_n$ et $D(S_n)=A_n$.

Démonstration *1)D'après la Proposition 5.2.2, A_3 est abélien donc $D(A_3)=\{Id\}$.*
$D(S_3)$ est un sous-groupe normal de S_3 donc, d'après la Proposition 5.2.6, $D(S_3)=\{Id\}$, A_3 ou S_3. D'après la Propriété 5.1.3, S_3 n'est pas abélien donc $D(S_3)=A_3$ ou S_3.
S_3/A_3 étant d'ordre 2, S_3/A_3 est abélien.
D'où, $D(S_3)$ est inclus dans A_3 et donc $D(S_3)=A_3$.

2)$D(A_4)$ est un sous-groupes normal de A_4 donc, d'après la Proposition 5.2.8, $D(A_4)=\{Id\}$, V_2 ou A_4. D'après la Proposition 5.2.2, A_4 n'est pas abélien donc $D(A_4)$ n'est pas réduit à $\{Id\}$. A_4/V_2 étant d'ordre 3, A_4/V_2 est isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et est donc abélien. D'où, $D(A_4)$ est inclus dans V_2.
On a (1 2)(3 4)=[(1 2 3),(1 2 4)], (1 3)(2 4)=[(1 2 3),(1 4 3)] et
(1 4)(2 3)=[(1 2 3),(2 3 4)] donc V_2 est inclus dans $D(A_4)$. D'où, $D(A_4)=V_2$.
S_4/V_4 étant d'ordre 2, S_4/V_4 est abélien.
D'où, $D(S_4)$ est inclus dans A_4 et $D(S_4)$ est donc un sous-groupe normal de A_4.
$D(A_4)$ étant inclus dans $D(S_4)$, on a $D(S_4)=V_2$ ou $D(S_4)=A_4$.
On a [(1 2),(1 2 3)]=(1 2 3) donc $D(S_4)$ n'est pas inclus dans V_2. D'où, $D(S_4)=A_4$.
3)$D(A_n)$ est un sous-groupe normal de A_n donc, d'après le Théorème 5.2.10, $D(A_n)=\{Id\}$ ou $D(A_n)=A_n$.
D'après la Proposition 5.2.2, A_n n'est pas abélien donc $D(A_n)$ n'est pas réduit à $\{Id\}$.
D'où, $D(A_n)=A_n$.
S_n/A_n étant d'ordre 2, S_n/A_n est abélien.
D'où, $D(S_n)$ est inclus dans A_n et $D(S_n)$ est donc un sous-groupe normal de A_n.
On en déduit que $D(S_n)=\{Id\}$ ou A_n.
Comme $A_n=D(A_n)$ est inclus dans $D(S_n)$, on a $D(S_n)=A_n$. $\diamondsuit$

Corollaire 5.2.14 *1)Le groupe S_3 est résoluble.*
2)Le groupe S_4 est résoluble.
3)Pour $n\geq 5$, le groupe S_n n'est pas résoluble.

Démonstration *1)D'après la Proposition précédente, on a*
$D^2(S_3)=D(D(S_3))=D(A_3)=\{Id\}$ donc S_3 est résoluble.
2)D'après la Proposition 5.2.7, V_2 est abélien donc $D(V_2)=\{Id\}$.
D'où, d'après la Proposition précédente, on a
$D^3(S_4)=D^2(D(S_4))=D(D(A_4))=D(V_2)=\{Id\}$ et S_4 est donc résoluble.
D'après la Proposition précédente, on a pour tout entier $k\geq 1$,
$D^k(S_n)=A_n \neq \{Id\}$ donc S_n n'est pas résoluble. $\diamondsuit$

Remarque *Le fait que que S_n n'est pas résoluble pour $n\geq 5$ entraîne l'impossibilité de la résolution par radicaux d'équations de degré supérieur ou égal à 5.*
Pour plus de détails, on pourra se reporter à l'ouvrage
d'Ivan Gozard, Théorie de Galois, *aux éditions Ellipses.*

5.3 Exercices du Chapitre 5

Exercice 1 : Déterminer et calculer le nombre des différents $k_1\times$ ... k_r-cycles de S_4 puis de S_5.

Exercice 2 : 1)Montrer que S_n est engendré par l'ensemble {(1 2), (1 ... n)}.
2)Montrer que si p≥3 est premier alors tout sous-groupe de S_p contenant une transposition et un p-cycle est égal à S_p.

Exercice 3 : On donne dans cet exercice deux autres définitions de la signature.
Soit un entier n≥3.
A)Le produit de quotients
Soit σ un élément de S_n.
On pose $\epsilon(\sigma)=\prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$.
1)Montrer que si τ est une transposition alors $\epsilon(\tau)$=-1.
2)Montrer que $\epsilon(\sigma\psi)=\epsilon(\sigma)\epsilon(\psi)$ pour tout couple (σ,ψ) d'éléments de S_n.
3)Montrer que ϵ=sgn.
B)Les inversions
Soit σ un élément de S_n. On appelle inversion pour σ, tout couple (i,j) d'éléments de {1, ... , n} tel que i<j et σ(i)>σ(j).
On pose $\eta(\sigma)$ l'entier $(-1)^{\iota_\sigma}$ où ι_σ est le nombre d'inversions pour σ.
1)Déterminer le nombre d'inversions pour le 2×3-cycle (1 3)(2 6 4) de S_6.
2)Déterminer le nombre d'inversions pour une transposition et en déduire la valeur de $\epsilon(\tau)$ lorsque τ est une transposition.
3)Montrer que $\eta=\epsilon$.

Exercice 4 : Autre démonstration de la simplicité de A_5
1)Déterminer les classes de conjugaison de A_5.
2)En déduire, en raisonnant sur l'ordre des sous-groupes normaux, que A_5 est simple.

Exercice 5 : Autre démonstration de la simplicité de A_n, n≥5.
On utilisera dans cet exercice, les résultats de l'Exercice précédent et des Exercices 4 et 5 du Chapitre 4 (*Opération*).
1)Montrer que A_n est (n-2)-transitif sur {1, ... , n}.
A_n est t'il (n-1)-transitif sur {1, ... , n} ?
2)En déduire que A_n ne possède aucun sous-groupe H tel que Stab_H(i)={Id} pour un élément i de {1, ... , n} où Stab_H(i) désigne le stabilisateur de i pour l'opération de H sur {1, ... , n} déduite de l'opération de A_n.
3)Montrer que le fixateur Fix_{A_n}(n) de n dans A_n est isomorphe à A_{n-1}.
4)En déduire, en utilisant un raisonnement par récurrence, que A_n est simple pour n≥5.

Exercice 6 : 1)Déterminer les sous-groupes de Sylow de A_3 et S_3.
2)Déterminer les sous-groupes de Sylow de A_4 et S_4.
3)Déterminer les sous-groupes de Sylow de A_5.
Indication : On pourra étudier le sous-groupe engendré par (a b)(c d) et (a c)(b d), a, b, c et d éléments distincts de {1, 2, 3, 4, 5}.
4)Déterminer les sous-groupes de Sylow de S_5.
Indication : On admettra qu'un groupe engendré par deux éléments x et y vérifiant : x d'ordre 2, y d'ordre 4 et xyxy=1, est d'ordre 8.

Pour les trois exercices qui suivent, on rappelle les résultats suivants :
Soit G un groupe. On appelle automorphisme intérieur de G, tout automorphisme de la forme α_g : x $\rightarrow$ gxg^{-1} où g est un élément de G.
L'ensemble Int(G) des automorphismes intérieurs de G est un sous-groupe de Aut(G). De plus, Int(G) est isomorphe au groupe quotient G/Z(G).

Exercice 7 : Automorphismes de S_n, n$\neq$6
1)Pour tout i compris entre 2 et n, on pose τ_i=(1 i).
Soit f un automorphisme de S_n qui transforme toute transposition en une transposition. Pour tout i compris entre 2 et n, on pose f(τ_i)=(a_i b_i).
a)Montrer que si i$\neq$j alors $\{a_i, b_i\} \cap \{a_j, b_j\} \neq \emptyset$.
b)On suppose, quitte à échanger a_3 et b_3, que a_2=a_3.
Montrer que a_2 appartient au support de f(τ_i) pour tout i compris entre 3 et n.
Indication : On raisonnera par l'absurde, sur un élément i compris entre 4 et n, en étudiant f(τ_2)f(τ_3)f(τ_i).
c)En déduire que f est un automorphisme intérieur.
2)Soit τ=(a b) une transposition.
Montrer qu'il existe un homomorphisme surjectif de $C_{S_n}(\tau)$ (centralisateur de τ dans S_n) dans S_{n-2}, de noyau {Id, τ}.
Soit σ un élément de S_n d'ordre 2.
3)Montrer que σ se décompose en un produit de transpositions de supports deux à deux disjoints.
Soit k le nombre de ces permutations.
4)En déduire que $C_{S_n}(\sigma)$ possède un sous-groupe normal d'ordre 2^k.
5)Soit f$\in$Aut(S_n). Montrer que pour tout élément ϕ de S_n, $C_{S_n}(\phi)$ est isomorphe à C_{S_n}(f(ϕ)).
6)Montrer que pour n$\in \mathbb{N}\backslash\{0, 1, 2, 4\}$, S_n ne possède pas de sous-groupe normal d'ordre 2^m, m$\in \mathbb{N}^*$.
7)Montrer que pour n$\neq$6, Aut(S_n)=Int(S_n).
8)En déduire que pour n$\neq$6, Aut(S_n) est isomorphe à S_n.

Exercice 8 : 1)Vérifier que S_n opère sur {1, ... , n}.
Pour tout élément i de {1, ... , n}, on note S(i) le stabilisateur de i pour cette opération.
2)Montrer que pour tout élément i de {1, ... , n}, S(i) est isomorphe à S_{n-1}.
3)Montrer que pour tout couple (i,j) d'éléments de {1, ... , n}, les ensembles S(i) et S(j) sont conjugués (c'est à dire il existe $\sigma \in S_n$ tel que S(i)=σS(j)σ^{-1}).
On suppose n$\neq$4.
Soit H un sous-groupe d'indice n de S_n.
S_n opère sur l'ensemble quotient (à gauche) S_n/H par l'opération : $\sigma.\psi$H=$\sigma\psi$H. Il existe donc un homomorphisme f de S_n vers $S_{S_n/H}$.
4)Montrer que f est un isomorphisme.
Indication : On rappelle que le noyau de l'opération de S_n sur S_n/H est $\cap_{\sigma\in S_n}\sigma$H$\sigma^-$.
5)Vérifier que Im f opère sur S_n/H.
6)Montrer que f(H) est le stabilisateur de H pour cette opération.
7)Vérifier qu'il existe une bijection s de S_n/H vers {1, ... , n} telle que s(H)=1.
8)En déduire un isomorphisme g de $S_{S_n/H}$ vers S_n.
9)Montrer que g(f(H))=S(1).
10)Montrer que si Aut(S_n)=Int(S_n) alors H et S(1) sont conjugués.
11)En déduire que si Aut(S_n)=Int(S_n) alors les sous-groupes d'indice n de S_n sont les sous-groupes S(i), i$\in$ {1, ... , n}.

Exercice 9 : Automorphismes de S_6
On utilise les notations et les résultats de l'Exercice précédent.
Soit P un 5-sous-groupe de Sylow de S_5 et H le normalisateur de P dans S_5.
1)Montrer que H est d'ordre 20.
Indication : On pourra montrer que S_5 possède 6 5-sous-groupes de Sylow.
2)Montrer que l'opération de S_5 sur l'ensemble quotient (à gauche) S_5/H est fidèle et transitive.
En déduire un homomorphisme injectif f de S_5 vers S_6.
3)Montrer que Im f est un sous-groupe de S_6 d'indice 6.
4)Montrer que Im f opère transitivement sur {1, ... , 6}.
5)En déduire que Im f n'est conjugué à aucun S(i), i$\in$ {1, ... , 6}.
6)Conclure que Aut(S_6)$\neq$Int(S_6).

Exercice 10 : Groupe des isométries du cube
1)Vérifier que le groupe des isométries et le groupe des isométries directes de $\mathbb{R}^3$ conservant un cube s'identifient à un sous-groupe de S_8.
Dans la suite, on identifie le groupe G des isométries directes d'un cube C avec le sous-groupe de S_8 lui correspondant.
On note 1, 2, 3 et 4 les sommets de la face avant du cube, avec 1 au coin supérieur gauche et 2 au coin supérieur droit, et 5, 6, 7 et 8 les sommets de la face arrière du cube de sorte que les arêtes de C sont [1 5], [2 6], [3 7] et [4 8].
2)Vérifier que σ=(1 2 3 4)(5 6 7 8) et ψ=(1 2 6 5)(3 7 8 4) appartiennent à G.
3)Vérifier que G opère sur l'ensemble {1, ... , 8}.
4)Déterminer l'orbite de 1 pour cette opération.
5)En déduire que G opère transitivement sur {1, ... , 8}.

6)Déterminer le stabilisateur de 1.
7)En déduire que G est d'ordre 24.
8)Montrer que G est isomorphe à un sous-groupe de S_4.
9)En déduire que G est isomorphe à S_4.
10)Décrire le groupe des isométries du cube C.

Chapitre 6

Groupes diédraux

6.1 Groupe diédral

Dans cette partie, nous allons étudier un type particulier de groupes : les groupes diédraux.

6.1.1 Définition

Soit n un entier supérieur ou égal à 3.

On se place dans le plan complexe et on considère le polygone régulier à n côtés P_n formé par les racines n^{ièmes} de l'unité $e^{\frac{2ik\pi}{n}}$, k=0, ... , n-1.

Proposition 6.1.1 *L'ensemble des isométries affines de* $\mathbb{C} \cong \mathbb{R}^2$ *opère sur* $\mathbb{C}^n$ *via l'opération f.*$(x_1, \ldots, x_n)$=$(f(x_1), \ldots, f(x_n))$.

Démonstration *Immédiate.* $\diamondsuit$

Définition *On appelle groupe diédral de degré n et on note* D_n*, le stabilisateur de* $\{e^{\frac{2ik\pi}{n}}$*, k=0, ... , n-1*$\}$ *pour l'opération définie dans la Proposition précédente.*

Le groupe diédral de degré n n'est autre que l'ensemble des isométries affines telles que l'image de P_n est P_n.

Toute isométrie conservant P_n fixe le point O par conservation des distances.
Il suffit donc de considérer les isométries vectorielles autrement dit $O_2(\mathbb{R})$.

6.1.2 Caractérisation de D_n

Soit n un entier supérieur ou égal à 3.

Proposition 6.1.2 *D_n contient un sous-groupe cyclique d'ordre 2.*

Démonstration *On vérifie facilement que la réflexion s d'axe (OI) avec I d'affixe 1 appartient à D_n. s est d'ordre 2 donc $<s>$ est un sous-groupe cyclique d'ordre 2 de D_n.* $\diamondsuit$

Proposition 6.1.3 *D_n contient un sous-groupe cyclique d'ordre n.*

Démonstration *Les rotations $r(O,\frac{2ik\pi}{n})$ de centre O et de rayon $\frac{2k\pi}{n}$, k=0, ... , n-1, appartiennent à D_n.*
Ces rotations auxquelles on ajoute l'identité, forment un sous-groupe cyclique de D_n d'ordre n, engendré par la rotation $r(O,\frac{2\pi}{n})$. $\diamondsuit$

On pose s=s(OI), la réflexion d'axe (OI) avec I d'affixe 1 et r=r(O,$\frac{2\pi}{n}$), la rotation de centre O et d'angle $\frac{2\pi}{n}$.
On a montré que s et r appartiennent à D_n.

Proposition 6.1.4 *$s\circ r\circ s\circ r=Id$.*

Démonstration *Montrons que $s\circ r\circ s=r^{-1}$:*
r^{-1} est la rotation de centre O et de rayon $\frac{-2\pi}{n}$.
det $s\circ r\circ s$=det r=1 donc $s\circ r\circ s$ est une isométrie directe de $\mathbb{R}^2$ c'est à dire une rotation.
$s\circ r\circ s(O)=O$ donc $s\circ r\circ s$ est de centre O.
$s\circ r\circ s(I)=s(r(I))$ est le point d'affixe $e^{-2\pi n}$ donc $s\circ r\circ s$ est une rotation de centre O et d'angle $\frac{-2\pi}{n}$ c'est à dire $s\circ r\circ s=r^{-1}$. $\diamondsuit$

Proposition 6.1.5 *D_n est engendré par s et r.*

Démonstration *On pose A_0=I et pour k compris entre 1 et n-1, on définit A_k comme le point d'affixe $e^{\frac{2k\pi}{n}}$.*
Soit f appartenant à D_n.
f étant une isométrie de $\mathbb{R}^2$ ayant au moins un point fixe (le point O), f est soit une rotation soit une réflexion.
Si il existe k compris entre 0 et n-1 tel que $f(A_k)=A_k$ alors O et A_k sont des points fixes pour f donc f est la réflexion d'axe (OA_k).
$s\circ r^{n-2k}(A_k)=s(A_{n-k})=A_k$ donc O et A_k sont des points fixes pour $s\circ r^{n-2k}$.
D'où, $s\circ r^{n-2k}=f$ et $f\in<\{s,\ r\}>$.
Supposons que $f(A_k)\neq A_k$ pour tout k compris entre 0 et n-1.
Supposons que f est une rotation.
Soient k et m compris entre 0 et n-1 tels que $f(A_k)=A_m$.
Alors, l'angle de f est égal à $(\overrightarrow{OA_k},\overrightarrow{OA_m})=arg\ \frac{e^{\frac{2ik\pi}{n}}}{e^{\frac{2im\pi}{n}}}=\frac{2i(k-m)\pi}{n}$.
D'où, $f=r^{k-m}\in<\{s,\ r\}>$.
Supposons maintenant que f est une réflexion d'axe Δ. O appartient à Δ.

f appartenant à D_n, il existe k compris entre 0 et n-1 tel que Δ coupe $[A_k,A_{k+1}]$ en son milieu (où on pose $A_n = A_0$ si k=n).
Montrons que $f=s\circ r^{n-2k-1}$:
$det(s\circ r^{n-2k-1})=det(s)det(r^{n-2k-1})$=-1.1=-1 donc $s\circ r^{n-2k-1}$ est une réflexion.
$s\circ r^{n-2k-1}(A_k)=s(A_{n-k-1})=A_{k+1}$ donc l'axe de $s\circ r^{n-2k-1}$ passe par le milieu de $[A_k,A_{k+1}]$.
Puisque $s\circ r^{n-2k-1}$ appartient à D_n, O appartient à l'axe de $s\circ r^{n-2k-1}$.
D'où, l'axe de $s\circ r^{n-2k-1}$ est Δ et $f=s\circ r^{n-2k-1} \in <\{s, r\}>$.
Tout élément de D_n appartient à $<\{s, r\}>$ donc $D_n \subset <\{s, r\}>$.
Puisque s et r appartiennent à D_n, $<\{s, r\}> \subset D_n$ et par conséquent, $D_n=<\{s, r\}>$.
$\diamondsuit$

D_n est donc un groupe engendré par deux éléments s et r vérifiant : s est d'ordre 2, r est d'ordre n et s$\circ$r$\circ$s$\circ$r=Id.

6.1.3 Etude de D_n

Soit n un entier supérieur ou égal à 3.

D'après les résultats de la Section précédente, on a la proposition suivante :

Proposition 6.1.6 *Tout groupe engendré par deux éléments a et b tels que :*
1)a est d'ordre 2,
2)b est d'ordre n et
3)abab=1,
est isomorphe à D_n.

Pour étudier D_n, on va donc se placer dans le cadre défini par la Proposition précédente.

Eléments de D_n

Propriété 6.1.7 *D_n n'est pas abélien.*

Démonstration *Puisque abab=1, on a $abab^{-1}=b^{-2}$.*
b^{-2} est différent de 1 car b est d'ordre n>2 donc $abab^{-1}$ est différent de 1.
D'où, a étant d'ordre 2, $(ab)(ba)^{-1}=abab^{-1}$ est différent de 1 et par conséquent, ab est différent de ba.
D_n n'est ainsi pas abélien. $\diamondsuit$

La propriété suivante nous sera très utile :

Propriété 6.1.8 *Pour tout entier k compris entre 1 et n-1, $ab^ka = b^{-k}$.*

Démonstration *Nous allons procéder par récurrence sur k (compris entre 1 et n) :*
Cas k=1 : abab=1 donc aba=b^{-1}.
Supposons que la propriété est vraie pour jusqu'à l'entier k-1.
Alors,

$$\begin{aligned} ab^k a &= ab^{k-1}ba \\ &= ab^{k-1}aaba \text{ car } a \text{ est d'ordre } 2 \\ &= b^{1-k}b^{-1} \text{ par hypothse de rcurrence} \\ &= b^{-k}. \end{aligned}$$

♢

Proposition 6.1.9 *a n'est pas une puissance de b.*

Démonstration *Supposons qu'il existe un entier k compris entre 1 et n-1 tel que a=b^k. Alors, abab=$b^{2k+2} = b^{2k}b^2$.*
Or a est d'ordre 2 donc b^{2k}=1. D'où, abab=b^2.
Comme abab=1, on en déduit que b^2=1.
On en déduit que b est d'ordre au plus 2 ce qui est impossible puisque b est d'ordre n>2. ♢

Proposition 6.1.10 $D_n = \{1, a, b, \ldots, b^{n-1}, ab, \ldots, ab^{n-1}\}$.

Démonstration *Comme a n'est pas une puissance de b, D_n contient les éléments distincts : 1, a, b, ... , b^{n-1}.*
Si k et m sont deux entiers distincts compris entre 1 et n-1 alors $ab^k \neq ab^m$.
D'où, puisque b est d'ordre n et comme a n'est pas une puissance de b, D_n contient les éléments 1, a, b, ... , b^{n-1}, ab, ... , ab^{n-1}.
Soit x un élément de D_n.
Comme D_n est engendré par a et b, x s'écrit sous la forme $a^{m_1}b^{k_1} \ldots a^{m_r}b^{k_r}$ avec, pour tout i compris entre 1 et r, m_i=0 ou 1 et k_i compris entre 0 et n-1.
D'après la Propriété 6.1.8 et puisque a=a^{-1} (a d'ordre 2), $b^k a = ab^{-k}$ pour tout entier k compris entre 1 et n-1.
D'où, on peut ramener l'écriture de x à une écriture de la forme $a^k b^m$ avec k=0 ou 1 et m compris entre 0 et n-1.
Par suite, $D_n = \{1, a, b, \ldots, b^{n-1}, ab, \ldots, ab^{n-1}\}$. ♢

Corollaire 6.1.11 *D_n est d'ordre 2n.*

Sous-groupe normaux de D_n

Proposition 6.1.12 *<b> est un sous-groupe normal de D_n.*

Démonstration *L'ordre de <b> est n donc l'indice de <b> dans D_n est $[D_n : <b>] = \frac{|D_n|}{|<b>|}$=2. On en déduit, d'après la Proposition* **??**, *que <b> est normal dans D_n.* $\diamondsuit$

Proposition 6.1.13 *D_n est le produit semi-direct de <b> par <a>.*

Démonstration *On a montré dans la Proposition précédente que <b> est normal dans D_n. On a montré dans la Proposition 6.1.9 que <b>∩<a>=*{1}.
Comme l'ordre de <b><a> est $\frac{|<b><a>|}{|<b>\cap<a>|}$ d'après la Proposition 3.4.6, on a $|<b><a>| = \frac{2n}{1} = 2n = |D_n|$ et par conséquent <b><a>=D_n.
D'où, D_n est le produit semi-direct de <b> par <a> $\diamondsuit$

D'après la Propriété 6.1.8, on définit un homomorphisme α du groupe <a> dans le groupe Aut(<b>) en posant α(1)=Id et $\alpha(a)(b^k)=ab^ka^{-1}=ab^ka=b^{-k}$.

Proposition 6.1.14 *D_n est isomorphe au produit semi-direct <b>$\rtimes_\alpha$<a>.*

Démonstration *Si on pose N=<b>×*{1} *et H=<a>×*{1} *alors <b>$\rtimes_\alpha$<a> est le produit semi-direct de N par H (cf Proposition* **??**).
Montrons que le produit semi-direct de <b> par <a> dans D_n est isomorphe au produit semi-direct de N par H dans <b>$\rtimes_\alpha$<a> : à b^ka^m on associe $f(b^ka^m)=(b^k,1)(1,a^m)$, $0\leq k\leq n-1$, $m\in$ {0, 1}. f est clairement bijective.
Soient $0\leq k,r\leq n-1$, $m,s\in$ {0, 1}.
<b> étant normal dans D_n, on a $a^mb^ra^{-m}\in$<b> donc $f(b^ma^kb^ra^s)=f((b^ka^mb^ra^{-m})(a^ma^s))=(b^ka^mb^ra^{-m},1)(1,a^ma^s)$.
Puisqu'on utilise la loi du produit semi-direct (cf Proposition **??**), *on a $f(b^ka^m)f(b^ra^s)=(b^k,1)(1,a^m)(b^r,1)(1,a^s)=(b^k\alpha(1)(1),1a^m)\ (b^r\alpha(1)(1),1a^s)=(b^k,a^m)(b^r,a^s)$ $=(b^k\alpha(a^m)(b^r),a^ma^s)=\ (b^ka^mb^ra^{-m},a^ma^s)$.*
D'où, f est un isomorphisme entre les produits directs de sous-groupes <b>⋊<a> et H⋊K.
Or d'après la Proposition précédente, le produit semi-direct <b>⋊<a> est égal à D_n donc D_n est isomorphe à <b>$\rtimes_\alpha$<a>. $\diamondsuit$

Corollaire 6.1.15 *D_n est isomorphe au produit semi-direct $\mathbb{Z}/n\mathbb{Z}\rtimes_\gamma\mathbb{Z}/2\mathbb{Z}$.*

Démonstration *<b> est un groupe cyclique d'ordre n donc <b> est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. De même, <a> est un groupe cyclique d'ordre 2 donc <a> est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. D'où, le produit semi-direct <b>$\rtimes_\alpha$<a> est isomorphe au produit semi-direct $\mathbb{Z}/n\mathbb{Z}\rtimes_\gamma\mathbb{Z}/2\mathbb{Z}$ où γ est défini de $\mathbb{Z}/2\mathbb{Z}$ dans Aut($\mathbb{Z}/n\mathbb{Z}$) par $\gamma(\overline{0})$=Id et $\gamma(\overline{1})(\widetilde{m})=\text{-}\widetilde{m}$ (cf Proposition* **??**).
Puisque D_n est isomorphe au produit semi-direct <b>$\rtimes_\alpha$<a>, D_n est isomorphe au produit semi-direct $\mathbb{Z}/n\mathbb{Z}\rtimes_\gamma\mathbb{Z}/2\mathbb{Z}$. $\diamondsuit$

Propriété 6.1.16 *Quel que soit k compris entre 0 et n-1, $bab^kb^{-1}=ab^{k-2}$.*

Démonstration *Puisque abab=1 et a est d'ordre 2, on a* $ba=ab^{-1}$.
D'où, $bab^kb^{-1}=ab^{-1}b^{k-1}=ab^{k-2}$. ♢

Proposition 6.1.17 *1)Si n est impair alors les sous-groupes normaux de* D_n *sont* D_n *et les sous-groupes de* $<b>$.
2)Si n est pair alors les sous-groupes normaux de D_n *sont* D_n, *les sous-groupes de* $<b>$, *le sous-groupe engendré par* b^2 *et a et le sous-groupe engendré par* b^2 *et ab.*

Démonstration $<b>$ *étant cyclique, les sous-groupes de* $<b>$ *sont des groupes cycliques. Soit k compris entre 1 et n-1.*
Montrons que $<b^k>$ *est un sous-groupe normal de* D_n :
$<b^k>$ *est un sous-groupe normal de* $<b>$. *Soit i compris entre 0 et n-1.*
D'après la Propriété 6.1.8, $ab^ib^k(ab^i)^{-1}=ab^ka=b^{-k}\in<b^k>$.
D'où, $<b^k>$ *est un sous-groupe normal de* D_n *pour tout k compris entre 1 et n-1.*
Soit N un sous-groupe normal de D_n *non inclus dans* $<b>$.
Il existe alors, d'après la Proposition 6.1.10, un entier k compris entre 0 et n-1 tel que $ab^k\in N$. *Alors, d'après la Propriété précédente, N contient* ab^{k-2}, *élément différent de 1 d'après la Proposition 6.1.9. D'où, N contient l'élément* $ab^{k-2}ab^k=b^2$ *et par conséquent, N contient le groupe* $<b^2>$.
1)Si n est impair alors pgcd(2,n)=1 et par conséquent, $<b^2>=<b>$ *(cf Proposition* **??***) N est ainsi d'ordre au moins égal à n+1.*
Or $|N|$ *divise* $|D_n|$ *c'est à dire 2n donc* $|N|=2n$ *et par suite,* $N=D_n$.
Les seuls sous-groupes normaux de D_n, *lorsque n est impair, sont* D_n *et les sous-groupes de* $<b>$.
2)Supposons n pair.
Pour tout i compris entre 1 et $\frac{n}{2}$*-1,* $ab^kb^{2i}=ab^{k+2i}$ *et d'après la Propriété 6.1.8,*
$b^{2i}ab^k=aab^{2i}ab^k=ab^{k-2i}=ab^{k+n-2i}=ab^{k+2(\frac{n}{2}-i)}$ *donc* $<\{b^2,\ ab^k\}>$ *est constitué des éléments* b^{2i} *et* ab^{k+2i}, *i=0, ... ,* $\frac{n}{2}$*-1.*
Ainsi, $<\{b^2,\ ab^k\}>$ *est d'ordre n et donc* $<\{b^2,\ ab^k\}>$ *est d'indice 2 dans* D_n.
On en déduit que $<\{b^2,\ ab^k\}>$ *est un sous-groupe normal de* D_n *(cf Proposition* **??***).*
Comme ab^k *et* b^2 *appartiennent à N, N contient* $<\{b^2,\ ab^k\}>$.
D'où, N possède au moins n éléments.
Or $|N|$ *divise* $D_n=2n$ *donc* $|N|=n$ *c'est à dire* $<\{ab^k,\ b^2\}>$ *ou* $|N|=2n$ *c'est à dire* $N=D_n$.
Il reste à déterminer l'ensemble des groupes de la forme $<\{b^2,\ ab^k\}>$.
On a vu que $<\{b^2,\ ab^k\}>$ *est constitué des éléments* b^{2i} *et* ab^{k+2i}, *i=0, ... ,* $\frac{n}{2}$*-1 donc* $<\{b^2,\ ab^k\}>=<\{b^2,\ ab^m\}>$ *dès que m-k est pair.*
On en déduit qu'il y a deux sous-groupes de la forme $<\{b^2,\ ab^k\}>$: $<\{b^2,\ a\}>$ *et* $<\{b^2,\ ab\}>$.
Les sous-groupes normaux de D_n, *lorsque n est pair, sont* D_n, *les sous-groupes de* $<b>$, *le sous-groupe* $<\{b^2,\ a\}>$ *et le sous-groupe* $<\{b^2,\ ab\}>$. ♢

Etudions maintenant deux sous-groupes associés à un groupe donné : le centre et le groupe dérivé.

6.1.4 Centre et groupe dérivé de D_n

Proposition 6.1.18 *1)Si n est impair alors Z(D_n)=$\{Id\}$.*
2)Si n est pair alors Z(D_n)=$\{Id,\ b^{\frac{n}{2}}\}$.

Démonstration *Soit k compris entre 1 et n-1.*
D'après la Propriété 6.1.8, $ab^k(b^k a)^{-1}=ab^k ab^{-k}=b^{-2k}$
Si n est impair ou si n est pair et k est différent de $\frac{n}{2}$ alors b^{-2k} est différent de 1. On a alors $ab^k \neq b^k a$ et donc $b^k \notin Z(D_n)$.
1)Si n est impair alors, puisque Z(D_n) est un sous-groupe normal de D_n, Z(D_n) est un sous-groupe de $<b>$ d'après la Proposition 6.1.17.
Or chacun de ces sous-groupes, hormis $\{1\}$, possède une puissance non nulle de b donc il ne peut être inclus dans Z(D_n) d'après ce qui précède. D'où, Z(D_n)=$\{Id\}$.
2)Il est clair que $b^{\frac{n}{2}}$ commute avec toute puissance de b.
De plus, $(b^{\frac{n}{2}})^2=b^n=1$ donc $b^{\frac{n}{2}}=b^{-\frac{n}{2}}$.
Pour tout k compris entre 0 et n-1, $ab^k b^{\frac{n}{2}}=ab^{\frac{n}{2}+k}$ et d'après la Propriété 6.1.8, $b^{\frac{n}{2}}ab^k=aab^{\frac{n}{2}}ab^k=ab^{-\frac{n}{2}}b^k=ab^{\frac{n}{2}}b^k=ab^{\frac{n}{2}+k}$. D'où, $b^{\frac{n}{2}}$ appartient à Z(D_n).
On a vu que si k est différent de $\frac{n}{2}$ alors b^k n'appartient pas à Z(D_n).
Comme abab=1, on a $ab=b^{-1}a\neq ba$ donc a n'appartient pas à Z(D_n).
De plus, aab=b et $aba=b^{-}1\neq b$ donc ab n'appartient pas non plus à D_n.
D'où, puisque Z(D_n) est un sous-groupe normal de D_n, Z(D_n)=$\{1,\ b^{\frac{n}{2}}\}$ d'après la Proposition 6.1.17. $\diamondsuit$

Proposition 6.1.19 *1)Si n est impair alors D(D_n)=$<b>$.*
2)Si n est pair alors D(D_n)=$<b^2>$.

Démonstration *Pour tout couple (i,j) d'entiers compris entre 0 et n-1, on a, en utilisant la Propriété 6.1.8, $[b^i,b^j]=b^i b^j b^{-i}b^{-j}=1$, $[ab^i,b^j]=ab^i b^j b^{-i}ab^{-j}=ab^j ab^{-j}=b^{-2j}$, $[b^j,ab^i]=([ab^i,b^j])^{-1}=b^{2j}$ et $[ab^i,ab^j]=ab^i ab^j b^{-i}ab^{-j}a=b^{-i}b^j b^{-i}b^j=1$.*
D'où, puisque D(D_n) est engendré par les commutateurs, D(D_n) est inclus dans $<b^2>$.
Comme $[a,b^{-1}]=ab^{-1}ab=b^2$, $<b^2>$ est inclus dans D(D_n). D'où, D(D_n)=$<b^2>$.
*Lorsque n est impair, pgcd(2,n)=1 donc $<b^2>=<b>$ (cf Proposition **??**).* $\diamondsuit$

Corollaire 6.1.20 *Le groupe D_n est résoluble.*

Démonstration *$<b>$ et $<b^2>$ étant cycliques donc abéliens, on a D($<b>$)=D($<b^2>$)=$\{1\}$.*
D'où, $D^2(D_n)=D(D(D_n))=\{1\}$ et D_n est donc résoluble. $\diamondsuit$

Chapitre 7

Correction des exercices

Dans cette partie, est rédigée une correction exhaustive des exercices proposés à la fin de chaque chapitre de cet ouvrage.

7.1 Correction des exercices du Chapitre 1

Exercice 1 : 1)Soient a, b et c trois réels.
$(a*b)*c=(a+b-ab)*c$=(a+b-ab)+c-(a+b-ab)c=a+b+c-ab-ac-bc+abc et
$a*(b*c)=a*(b+c-bc)$=a+(b+c-bc)-a(b+c-bc)=a+b+c-ab-ac-bc+abc donc
$(a*b)*c=(a*b)*c)$. la loi $*$ est associative.
2)Quel que soit le réel a, a∗0=a+0-a0=a et 0∗a=0+a-0a=a donc 0 est un élément neutre de la loi $*$.
D'après la Proposition 1.1.1, 0 est l'unique élément neutre de la loi $*$
3)Montrons que 1 n'a pas d'inverse pour la loi $*$: si a est un réel inverse de 1 pour la loi $*$ alors 1∗a=1+a-1a=1+a-a=1 et 1∗a=0 ce qui est impossible.
D'où 1 n'a pas d'inverse pour la loi $*$ et par conséquent, $(\mathbb{R},*)$ n'est pas un groupe.

Exercice 2 : 1)L'union est clairement une loi associative admettant comme élément neutre, l'ensemble vide.
D'où, (P(E),∪) est un monoïde.
(P(E),∪) n'est pas un groupe car aucun élément de P(E), hormis l'ensemble vide, n'a d'inverse pour l'union.
En effet, si A est une partie non vide de E, A est incluse dans toute union de A avec une partie de E et donc cette union ne peut être l'ensemble vide.
2)L'intersection est clairement une loi associative admettant comme élément neutre, l'ensemble E.
D'où, (P(E),∩) est un monoïde.
(P(E),∩) n'est pas un groupe car aucun élément de P(E), hormis l'ensemble E, n'a d'inverse pour l'intersection.
En effet, si A est une partie de E différente de E, l'intersection de A avec une partie de E est incluse dans A et ne peut donc être l'ensemble E.
3)Montrons que la différence symétrique est associative : soient A, B et C des parties de E.

$$\begin{aligned}(A\Delta B)\Delta C &= (A\cup B/A\cap B)\Delta C\\ &= ((A\cup B)\cup C)/((A\cap B)\cap C)\\ &= (A\cup(B\cup C))/(A\cap(B\cap C))\ car \cup\ et\ \cap\ sont\ associatives,\\ &= A\Delta(B\Delta C).\end{aligned}$$

D'où, la différence symétrique est une loi associative.
Soit A une partie de E. $A\Delta\emptyset = A\cup\emptyset/A\cap\emptyset = A/\emptyset = A$ et $\emptyset\Delta A = \emptyset\cup A/\emptyset\cap A = A/\emptyset = A$ donc $\emptyset$ est l'élément 3 neutre de la différence symétrique (l'unicité résultant de la Proposition 1.1.1). $A\Delta A = A\cup A/A\cap A = A/A = \emptyset$ donc A est l'inverse de A pour la différence symétrique (l'unicité résultant de la Propostion 1.1.1).
D'où, (P(E),Δ) est un groupe.
L'union et l'intersection étant des lois commutatives, Δ est une loi commutative et (P(E),Δ) est donc un groupe abélien.

Exercice 3 : ($\Rightarrow$) On suppose que G est abélien.
Alors, pour tout couple (g,g') d'éléments de G, $(gg')^{-1} = g'^{-1}g^{-1} = g^{-1}g'^{-1}$.
($\Leftarrow$) On suppose que pour tous les éléments g et g' de G, $(gg')^{-1} = g^{-1}g'^{-1}$.
On a, pour tout couple (g,g') d'éléments de G,
$gg' = ((gg')^{-1})^{-1} = (g'^{-1}g^{-1})^{-1} = (g^{-1}g'^{-1})^{-1} = g'g$ donc G est un groupe abélien.

Exercice 4 : $\mathbb{D}$ n'est pas vide car 1 appartient à cet ensemble.
Il est clair que $\mathbb{D}$ est inclus dans $\mathbb{Q}$.
Soient $\frac{a}{10^n}$ et $\frac{b}{10^m}$, a, b$\in \mathbb{Z}$ et n, m$\mathbb{N}$, deux éléments de $\mathbb{D}$. On suppose n$\leq$m.
$\frac{a}{10^n} - \frac{b}{10^m} = \frac{10^{m-n}a-b}{10^m}$ donc $\frac{a}{10^n} - \frac{b}{10^m}$ appartient à $\mathbb{D}$.
Par conséquent, ($\mathbb{D}$,+) est un sous-groupe de $\mathbb{Q}$.
On a $\frac{1}{10} : \frac{3}{10} = \frac{1}{3}$, mais $\frac{1}{3}$ n'appartient pas à $\mathbb{D}$ puisque 3 ne divise aucune puissance entière de 10, donc $(\mathbb{D} - \{0\}, \times)$ n'est pas un sous-groupe de $(\mathbb{Q} - \{0\}, \times)$.

Exercice 5 : 1)D'après la Proposition 1.2.8, g^2=1 pour tout élément de G.
Pour tout g appartenant à G, puisque g^2=1, g=$(g^{-1}g)g = g^{-1}g^2 = g^{-1}$.
2)Soient g_1 et g_2 deux éléments de G.
D'après la question précédente, $g_1g_2 = (g_1g_2)^{-1} = g_2^{-1}g_1^{-1} = g_2g_1$.
Par conséquent, G est abélien.

Exercice 6 : Soit G un groupe d'ordre 4.
Raisonnons par l'absurde : soit g un élément de G d'ordre 3.
g est donc différent de 1 et <g>=$\{1, g, g^2\}$.
G s'écrit par conséquent sous la forme $\{1, g, g^2, g'\}$ où g' est différent de 1, g et g^2.
De plus, puisque g est d'ordre 3, g^3=1 donc $g^2 = g^{-1}$.
Puisque G est un groupe, gg'appartient à G.
gg' est différent de 1 car sinon g'=$g^{-1} = g^2$.
gg' est différent de g car sinon g'=1.
gg' est différent de g^2 car sinon g'=g.
gg' est différent de g' car sinon g=1.
D'où, gg' n'appartient pas à G. Contradiction.
Un groupe d'ordre 4 ne possède pas d'élément d'ordre 3.

Exercice 7 : Il faut d'abord remarquer que l'image de l'application ι est l'ensemble H.
($\Rightarrow$) On suppose que H est un sous-groupe de G.
On a vu qu'alors H est un groupe. Si h_1 et h_2 sont deux éléments de H, $\iota(h_1h_2) = h_1h_2 = \iota(h_1)\iota(h_2)$ donc ι est un homomorphisme de groupes.
($\Leftarrow$) H est un groupe pour une loi notée $*$.
Soient h_1 et h_2 deux éléments de H.
Alors, puisque H est un groupe, $h_1 * h_2^{-1}$ appartient à H.
ι étant un homomorphisme de groupes, on a $h_1h_2^{-1} = \iota(h_1)\iota(h_2)^{-1} = \iota(h_1 * h_2^{-1}) \in$H.
D'où, H est un sous-groupe de G.

Exercice 8 : f est un endomorphisme de G si et seulement si $f(g_1g_2) = f(g_1)f(g_2)$ pour tout couple (g_1, g_2) d'éléments de G,
si et seulement si $g_1g_2g_1g_2 = g_1g_1g_2g_2$,
si et seulement si $g_1^{-1}(g_1g_2g_1g_2)g_2^{-1} = g_1^{-1}(g_1g_1g_2g_2)g_2^{-1}$,
si et seulement si $g_2g_1 = g_1g_2$ pour tout couple (g_1, g_2) d'éléments de G,
si et seulement si G est abélien.

Exercice 9 1)La loi + est associative et commutative car l'addition usuelle $\mathbb{R}$ est associative et commutative.
On vérifie facilement que la loi + admet la matrice nulle $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ comme élément neutre et qu'une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ admet la matrice $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ comme inverse.
D'où, $(M_2(\mathbb{R}),+)$ est un groupe abélien.
2)Soient L=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, M=$\begin{pmatrix} e & f \\ g & h \end{pmatrix}$ et N=$\begin{pmatrix} i & j \\ k & l \end{pmatrix}$ trois éléments de $M_2(\mathbb{R})$.
On a (LM)N=$\begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}\begin{pmatrix} i & j \\ k & l \end{pmatrix}$
=$\begin{pmatrix} (ae+bg)i+(af+bh)k & (ae+bg)j+(af+bh)l \\ (ce+dg)i+(ce+dg)k & (ce+dg)j+(ce+dg)l \end{pmatrix}$
=$\begin{pmatrix} a(ei+fk)+b(gi+hk) & a(ej+fl)+b(gj+hl) \\ c(ei+fk)+d(gi+hk) & c(ej+fl)+d(gj+hl) \end{pmatrix}$
=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} ei+fk & ej+fl \\ gi+hk & gj+hl \end{pmatrix}$=L(MN) donc la loi . est associative.
On vérifie facilement que la loi . admet la matrice identité Id=$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ comme élément neutre donc $(M_2(\mathbb{R}),.)$ est un monoïde.
3)La loi . n'est pas commutative puisque, si on pose M=$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ et N=$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, on a MN=$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ et NM=$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$.
4)Montrons par l'absurde, que la matrice M=$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ n'a pas d'inverse pour la loi . : si N=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est une matrice inverse de M alors MN=Id c'est à dire $\begin{cases} a=1 \\ b=0 \\ 0=0 \\ 0=1 \end{cases}$.
Contradiction.
La matrice M n'admet donc pas d'inverse.
5)Soient M=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et N=$\begin{pmatrix} e & f \\ g & h \end{pmatrix}$ deux éléments de $M_2(\mathbb{R})$.
det(MN)=det($\begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$)=(ae+bg)(cf+dh)-(af+bh)(ce+dg)=aedh+bgcf-afdg-bhce=(ad-bc)(eh-fg)=det(M)det(N).
6)Soit M un élément de $M_2(\mathbb{R})$ inversible pour la loi .
Il existe alors un élément N de $M_2(\mathbb{R})$ tel que MN=Id.

On en déduit que det(MN)=det(M)det(N)=det(Id)=1.
Par conséquent, det(M) ne peut pas être nul.
7)La loi. étant associative, si un élément de $(M_2(\mathbb{R}),+)$ est inversible alors son inverse est unique. On pose M=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec det(ad-bc)neq0 et N=$\frac{1}{det(M)}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.
On a MN=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \frac{d}{det(M)} & \frac{-b}{det(M)} \\ \frac{-c}{det(M)} & \frac{a}{det(M)} \end{pmatrix} = \begin{pmatrix} \frac{ad-bc}{det(M)} & 0 \\ 0 & \frac{-cb+da}{det(M)} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$=Id et de même NM=Id donc M est inversible d'inverse N.
8)D'après les deux questions précédentes, $GL_2(\mathbb{R})$ est l'ensemble des éléments de $M_2(\mathbb{R})$ de déterminant non nul.
$GL_2(\mathbb{R})$ car Id est un élément de cet ensemble.
Montrer que $Gl_2(\mathbb{R})$ est stable pour la loi . : Si M et N appartiennent à $GL_2(\mathbb{R})$ alors, det(M)$\neq$0, det(N)$\neq$0 et d'après la question 5, det(MN)=det(M)det(N)$\neq$0.
D'où, $Gl_2(\mathbb{R})$ est stable pour la loi . (autrement dit . est une loi interne sur$Gl_2(\mathbb{R})$).
On a vu à la question 2 que la loi. est associative et admet l'identité comme élément neutre.
De plus, par définition de $Gl_2(\mathbb{R})$, tous les éléments det ensemble sont inversibles pour la loi . donc $(Gl_2(\mathbb{R}),.)$ est un groupe.
9)Soit M=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de $GL_2(\mathbb{R})$.
D'après la question 6, det(MM^{-1})=det(M)det($M^{-}1$).
Mais MM^{-1}=Id donc det (MM^{-1})=det(Id)=1. D'où, det(M^{-1})=$\frac{1}{det(M)}$.
10)<u>Première méthode :</u> $SL_2(\mathbb{R})$ n'est pas vide puisque l'identité apartient à cet ensemble.
Il est clair que $SL_2(\mathbb{R})$ est inclus dans $GL_2(\mathbb{R})$.
Soient M et N deux éléments de $SL_2(\mathbb{R})$.
D'après les questions 5 et 9, det(MN^{-1})=det(M)det(N^{-1})=$\frac{det(M)}{det(N)}$=1 donc MN^{-1} appartient à $SL_2(\mathbb{R})$.
$Sl_2(\mathbb{R})$ est par conséquent un sous-groupe de $GL_2(\mathbb{R})$.
<u>Deuxième méthode :</u> $GL_2(\mathbb{R})$ étant un groupe, la restriction de l'application det à $GL_2(\mathbb{R})$ est, d'après la question 6, un homomorphisme de groupes de $(GL_2(\mathbb{R}),.)$ dans $(\mathbb{R},\times)$.
On remarque que $SL_2(\mathbb{R})$ est le noyau de cet homomorphisme donc d'après la Proposition 1.3.3, $SL_2(\mathbb{R})$ est un sous-groupe de $GL_2(\mathbb{R})$.

<u>Exercice 10 :</u> 1)Soient φ l'isomorphisme entre G_1 et G'_1 et ψ l'isomorphisme entre G_2 et G'_2. Soit σ l'application de $G_1 \times G_2$ vers $G'_1 \times G'_2$ définie par $\sigma(g_1, g_2) = (\varphi(g_1), \psi(g_2))$.
Montrons que σ est un homomorphisme : soient (g_1, g_2) et (h_1, h_2) deux éléments de $G_1 \times G_2$. On a

$$\begin{aligned}
\sigma((g_1,g_2)(h_1,h_2)) &= \sigma(g_1h_1, g_2h_2)) \\
&= (\varphi(g_1h_1), \psi(g_2h_2)) \\
&= (\varphi(g_1)\varphi(h_1), \psi(g_2)\psi(h_2)) \textit{ car } \varphi \textit{ et } \psi \textit{ sont des homomorphismes} \\
&= (\varphi(g_1), \psi(g_2))(\varphi(h_1), \psi(h_2)) \\
&= \sigma(g_1, g_2)\sigma(h_1, h_2).
\end{aligned}$$

σ est un homomorphisme de groupes.
Déterminons le noyau de σ : Ker $\sigma = \{(g_1, g_2) \in G_1 \times G_2 \ / \ \sigma(g_1, g_2)=(1,1)\} = \{(g_1, g_2) \in G_1 \times G_2 \ / \ \varphi(g_1)=1 \text{ et } \psi(g_2)=1\} = \{(1,1)\}$ car φ et ψ sont des homomorphismes injectifs (Proposition 1.3.4).
σ est donc un homomorphisme injectif, d'près la Proposition 1.3.4. Soient (g'_1, g'_2) un élément de $G'_1 \times G'_2$.
φ et ψ étant des homomorphismes surjectifs, il existe un élément g_1 de G_1 et un élément g_2 de G_2 tels que $\varphi(g_1) = g'_1$ et $\psi(g_2) = g'_2$.
On en déduit que $\sigma(g_1, g_2) = (g'_1, g'_2)$.
D'où, σ est un homomorphisme surjecif.
On en déduit que σ est un isomorphisme entre $G_1 \times G_2$ et $G'_1 \times G'_2$.
2)Montrons le résultat par récurrence sur n :
n=1 : $\mathbb{C}$ est isomorphe à $\mathbb{R}$ par l'isomorphisme f(x+iy)=(x,y).
Supposons le résultat vrai pour n. Alors, d'après la question précédente, $\mathbb{C}^n \times \mathbb{C} = \mathbb{C}^{n+1}$ est isomorphe à $\mathbb{R}^n \times \mathbb{R} = \mathbb{R}^{n+1}$.

7.2 Correction des exercices du Chapitre 2

Exercice 1 : 1)Commençons par montrer, par récurrence, que, pour tout entier naturel n, 10^n est congru à 1 modulo 9 :
Si n=0 alors 10^n=1 est congru à 1 modulo 9.
Si n=1 alors 10^1=10 est congru à 1 modulo 9.
Supposons que 10^n est congru à 1 modulo 9.
Alors, puisque $10^{n+1} = 10.10^n$ et 10 et 10^n sont congrus à 1 modulo 9, 10^{n+1} est congru à 1 modulo 9.
Soit x un entier naturel. Soient x_0, x_1, ... , x_n les chiffres de x.
On a alors x=$x_n.10^n$+ ... +$x_1.10 + x_0$.
D'après ce que l'on vient de montrer, $x_i.10^i$ est congru à x_i modulo 9 pour tout entier i compris entre 0 et n.
D'où, x est congru à x_n+ ... +x_0 modulo 9.
2)Un entier naturel n est divisible par 9 si et seulement si il est congru à 0 modulo 9 donc si et seulement si la somme de ses chiffres est divisible par 9.
Remarque : On démontre de la même manière qu'un entier naturel est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

Exercice 2 : Puisque $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \ldots, \overline{n}\}$ et $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \ldots, \overline{n}, \ldots, \overline{m}\}$, on pourrait penser que $\mathbb{Z}/n\mathbb{Z}$ est inclus dans $\mathbb{Z}/m\mathbb{Z}$. Mais pour $\mathbb{Z}/n\mathbb{Z}$, le terme $\overline{x}$ (0≤x≤n-1) désigne l'ensemble x+n$\mathbb{Z}$ et pour $\mathbb{Z}/m\mathbb{Z}$, le terme $\overline{x}$ désigne l'ensemble x+m$\mathbb{Z}$ donc bien que l'on utilise la même notation, ces deux ensembles sont différents.
On ne peut donc pas comparer les groupes $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$.
La proposition est fausse.

Exercice 3 : 1)Le nombre d'automorphismes de $\mathbb{Z}/6\mathbb{Z}$ est égal à $\varphi(6)$ (Proposition 2.2.13). Il y a donc 2 automorphismes de $\mathbb{Z}/6\mathbb{Z}$.

2)On a vu que l'image d'un générateur de $\mathbb{Z}/6\mathbb{Z}$ par un automorphisme est encore un générateur de $\mathbb{Z}/6\mathbb{Z}$ (Proposition 2.2.4) donc l'image de $\overline{1}$ par un automorphisme de $\mathbb{Z}/6\mathbb{Z}$ est $\overline{1}$ ou $\overline{5}$.
Puisque $\mathbb{Z}/6\mathbb{Z}$ est un groupe cyclique, l'image de $\overline{1}$ par un automorphisme suffit à déterminer cet automorphisme.
D'où, les deux automorphismes de $\mathbb{Z}/6\mathbb{Z}$ sont l'identité qui à $\overline{1}$ associe $\overline{1}$ et l'automorphisme f défini par $f(\overline{1})=\overline{5}$.
Les valeurs de f sont : $f(\overline{2})=f(2.\overline{1})=2f(\overline{1})=\overline{1}0=\overline{4}$, $f(\overline{3})=\overline{3}$, $f(\overline{4})=\overline{2}$ et $f(\overline{5})=\overline{1}$.

Exercice 4 : 1)Montrons que Φ est injective : soient A et B deux parties de E telles que $\Phi(A)=\Phi(B)$.
Soit x un élément de E.
Puisque $\Phi_A=\Phi_B$, x appartient à A si et seulement si x appartient à B (par définition de Φ_A et Φ_B). D'où, A=B et Φ est injective.
Montrons que Φ est surjective : soit f une application de E dans $\mathbb{Z}/2\mathbb{Z}$.
Posons $A=\{x \in E \ / \ f(x)=\overline{1}\}$.
Alors, pour tout élément x de E, $\Phi_A(x)=f(x)$ donc $\Phi(A)=f$. Φ est surjective.
Φ est donc une bijection de P(E) dans F.
2)Montrons que la loi + est associative : soient f, g et h des éléments de F.
Pour tout élément x de E,

$$\begin{aligned}((f+g)+h)(x) &= (f+g)(x)+h(x)\\ &= (f(x)+g(x))+h(x)\\ &= f(x)+(g(x)+h(x)) \textit{ car la loi de } \mathbb{Z}/2\mathbb{Z} \textit{ est associative}\\ &= f(x)+(g+h)(x)\\ &= (f+(g+h))(x)\end{aligned}$$

donc (f+g)+h=f+(g+h). La loi + est associative.
la loi + est commutative car la loi de $\mathbb{Z}/2\mathbb{Z}$ est commutative. La loi + admet l'application nulle pour élément neutre.
Tout élément de F admet pour inverse lui-même car $\overline{1}+\overline{1}=\overline{0}$.
D'où, (F,+) est un groupe abélien)
3)$\Phi_A+\Phi_B$ appartient à F d'après la question précédente. D'où, puisuqe Φ est bijective, $\Phi_A+\Phi_B$ possède un unique antécédent par Φ.
Soit x un élément de E. $\Phi_A+\Phi_B(x)=\overline{1}$ si et seulement si x appartient à une et une seule des parties A et B car $\overline{1}+\overline{1}=\overline{0}$.
Autrement dit, $\Phi_A+\Phi_B(x)=\overline{1}$ si et seulement si x appartient à $A\Delta B=A\cup B/A\cap B$.
D'où, $\Phi_A+\Phi_B=\Phi_{A\Delta B}$.
4)La différence symétrique Δ est une loi interne sur P(E). Posons $\Theta=\Phi^{-1}$.
Θ est une bijection faisant correspondre $\Phi_A+\Phi_B$ avec $A\Delta B$ pour tout couple (A,B) d'éléments de P(E).
Montrons que la différence symétrique est associative : soient A, B et C trois parties de E. On a

$$\begin{aligned}(A\Delta B)\Delta C &= \Theta(\Phi_{A\Delta B}+\Phi_C)\\ &= \Theta((\Phi_A+\Phi_B)+\Phi_C)\\ &= \Theta(\Phi_A+(\Phi_B+\Phi_C)) \textit{ car la loi de } F \textit{ est associative}\end{aligned}$$

$$\begin{aligned} &= \Theta(\Phi_A + \Phi_{B\Delta C}) \\ &= A\Delta(B\Delta C). \end{aligned}$$

D'où, la loi Δ est associative.
L'union et l'intersection étant des lois commutatives sur P(E), la différence symétrique est une loi commutative.
Pour toute partie A de E, $\Phi_{A\Delta\emptyset} = \Phi_A + \Phi_\emptyset = \Phi_A$ donc, puisque Φ est injective, A$\Delta\emptyset$=A.
L'élément neutre de la loi Δ est l'ensemble vide.
Pour toute partie A de E, $\Phi_{A\Delta A} = \Phi_A + \Phi_A = 0 = \Phi_\emptyset$ donc, puisque Φ est injective, AΔA=$\emptyset$. D'où, l'inverse de A pour la loi Δ est A.
D'où, (P(E),Δ) est un groupe abélien.
Remarques : Φ est un isomorphisme entre les groupes (P(E),Δ) et (F,+).

Exercice 5 : Déterminons l'ensemble des solutions de l'équation complexe $z^n = 1$:
Si z est un nombre complexe alors on peut l'écrire sous la forme z=$|z|e^{i\,arg(z)}$.
D'où, $z^n = 1$ si et seulement si $|z|^n e^{i\,n.arg(z)} = 1 = 1e^{i\,0}$, si et seulement si $|z|^n$=1 et n.arg(z)=2kπ où k est un entier (pour tout réel x et pour tout entier k, $e^{ix+2k\pi} = e^{ix}$).
|z| étant un réel positif, $|z|^n$=1 si et seulement si |z|=1.
arg(z) est défini à 2π près donc si n.arg(z)=2kπ alors n.arg(z)=2(k+m)π pour tout entier m.
D'où, $e^{i\,n.arg(z)} = e^{i\,0}$ si et seulement si il existe un entier k compris entre 0 et n-1 tel que n.arg(z)=2kπ mod 2π.
On en déduit que l'ensemble des solutions de l'équation complexe $z^n = 1$ est l'ensemble U=$\{z_k = e^{i.\frac{2k\pi}{n}} \ / \ 0 \leq k \leq n-1\}$.
On remarque que $z_0 = 1$.
Pour tout entier i compris entre 0 et n-1, on a $z_k = e^{i.\frac{2k\pi}{n}} = \left(e^{i.\frac{2\pi}{n}}\right)^k = z_1^k$ donc
U=$\{z_1^k \ / 0 \leq k \leq n-1\}$.
On en déduit que U muni de la multiplication usuelle des complexes est un groupe cyclique d'ordre n (de plus, U est un sous-groupe de ($\mathbb{C}^*$,$\times$)).

Exercice 6 : Soit g un élément de G, différent de 1.
<g> est un sous-groupe de G donc, par hypothèse, <g>={1} ou <g>=G. Mais g est différent de 1 donc <g> est différent de {1}.
D'où, G=<g> et G est cyclique.
Supposons |G| non premier.
Il existe alors un entier n, 1<n<|G|, tel que n divise |G|.
Posons h=$g^{\frac{|G|}{n}}$.
Alors, h est d'ordre n (si d est l'ordre de h alors h^d=$g^{\frac{d|G|}{n}}$=1 donc |G| divise $\frac{d|G|}{n}$ ce qui entraîne que n divise d) et <h> est donc un groupe d'ordre n.
Puisque 1<n<|G|, <h> est un sous-groupe de G différent de {1} et de G.
Contradiction. L'ordre de G est un nombre premier.

Exercice 7 : Montrons la proposition par récurrence sur n :
Si n=1 alors $\varphi(p^n) = \varphi(p) = p - 1 = (p-1)p^{n-1}$.

Supposons le résultat vrai jusqu'à n.
Puisque p est un nombre premier, les diviseurs de p^{n+1} dans $\mathbb{N}$ sont les p^a où a est un entier variant de 0 à n+1.
D'où, d'après la Proposition 2.2.11, $p^{n+1} = \sum_{0\leq a\leq n+1} \varphi(p^a) = \varphi(1)+\sum_{1\leq a\leq n} \varphi(p^a)+ \varphi(p^{n+1})$.
On applique l'hypothèse de récurrence :

$$\begin{aligned} p^{n+1} &= \varphi(1) + \sum_{1\leq a\leq n} (p-1)p^{a-1} + \varphi(p^{n+1}) \\ &= 1 + (p-1)\sum_{1\leq a\leq n} \varphi(p^{a-1}) + \varphi(p^{n+1}) \\ &= 1 + (p-1)\sum_{0\leq a\leq n-1} \varphi(p^a) + \varphi(p^{n+1}) \end{aligned}$$

$\sum_{0\leq a\leq n-1} p^a$ est la somme des n premiers termes de la suite géométrique de premier terme 1 et de raison p donc $\sum_{0\leq a\leq n-1} p^a = \frac{1-p^n}{1-p}$.
On en déduit que

$$\begin{aligned} \varphi(p^{n+1}) &= p^{n+1} - 1 - (p-1)\frac{1-p^n}{1-p} \\ &= p^{n+1} - 1 + (1-p^n) \\ &= p^{n+1} - p^n \\ &= (p-1)p^n. \end{aligned}$$

Exercice 8 : 1)Notons par . la correpondance $((\overline{x},\overline{y})\rightarrow \overline{x+y})$.
On note $\overline{x}+\overline{y}$ à la place de .$(\overline{x},\overline{y})$.
Commençons par montrer que la correspondance . est une loi interne sur $\mathbb{Z}/n\mathbb{Z}$ c'est à dire une application : soient $(\overline{x},\overline{z})$ et $(\overline{y},\overline{t})$ deux couples égaux d'éléments de $\mathbb{Z}/n\mathbb{Z}$.
On a alors $\overline{x}=\overline{y}$ c'est à dire x≡y mod n et $\overline{z} = \overline{t}$ c'est à dire z≡t mod n.
D'où, d'après la seconde Propriété 2.1.2, (xz)≡(yt) mod n c'est à dire $\overline{xz} = \overline{yt}$. On a donc $\overline{xz}=\overline{y}\overline{t}$.
D'où, la correpondance . est une loi interne sur $\mathbb{Z}/n\mathbb{Z}$.
Pour tout triplet $(\overline{x}, \overline{y}, \overline{z})$ d'éléments de$\mathbb{Z}/n\mathbb{Z}$, on a

$$\begin{aligned} (\overline{xy})\overline{z} &= \overline{xyz} \\ &= \overline{(xy)z} \\ &= \overline{x(yz)} \textit{ car la multiplication de } \mathbb{Z} \textit{ est associative} \\ &= \overline{xyz} \\ &= \overline{x}(\overline{yz}) \end{aligned}$$

donc la loi . est associative.
Puisque la multiplication est commutative dans $\mathbb{Z}$, la loi. est commutative.
Pour tout élément $\overline{x}$de $\mathbb{Z}/n\mathbb{Z}$, on a $\overline{x}.\overline{1} = \overline{x1}=\overline{x}$ donc la loi . admet l'élément $\overline{1}$ comme élément neutre.

D'où, $(\mathbb{Z}/n\mathbb{Z},.)$ est un monoïde commutatif.
2)Soit $\overline{x}$ un élément non nul de $\mathbb{Z}/n\mathbb{Z}$.
$\overline{x}$ est inversible si et seulement si il existe un élément $\overline{y}$ de $\mathbb{Z}/n\mathbb{Z}$ tel que $\overline{yx}$=$\overline{yx} = \overline{1}$, si et seulement si yx est congru à 1 modulo n,
si et seulement si il existe un entier m tel que yx=1+mn,
si et seulement il existe un couple (y,k) d'entiers tels que yx+kn=1,
si et seulement si x et n sont premiers entre eux d'après le Théorème de Bezout.
3)U$(\mathbb{Z}/n\mathbb{Z})$ est inclus dans $\mathbb{Z}/n\mathbb{Z}$ et contient $\overline{1}$ donc (U$(\mathbb{Z}/n\mathbb{Z})$,.) est un monoïde commutatif. Si $\overline{x}$ appartient à U$(\mathbb{Z}/n\mathbb{Z})$ alors, par définition de U$(\mathbb{Z}/n\mathbb{Z})$, $\overline{x}$ est inversible et son inverse appartient aussi à U$(\mathbb{Z}/n\mathbb{Z})$.
D'où, (U$(\mathbb{Z}/n\mathbb{Z})$,.) est un groupe abélien.
4)Puisque $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique, un automorphisme de $\mathbb{Z}/n\mathbb{Z}$ est caractérisé par l'image de $\overline{1}$.
D'après la Proposition 2.2.12, l'image de $\overline{1}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$.
Or $\overline{x}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$si et seulement si x est premier avec n c'est à dire, d'après la Question 2, si et seulement si $\overline{x}$ appartient à U$(\mathbb{Z}/n\mathbb{Z})$.
D'où, si f est un automorphisme de $\mathbb{Z}/n\mathbb{Z}$ alors f($\overline{1}$) appartient à U$(\mathbb{Z}/n\mathbb{Z})$.
Soit ϕ l'application qui à un automorphisme f de $\mathbb{Z}/n\mathbb{Z}$ associe f($\overline{1}$).
Pour tout couple (f,g) d'automorphismes de $\mathbb{Z}/n\mathbb{Z}$, on a $\phi(fg) = fg(\overline{1}) = f(\overline{1})g(\overline{1}) = \phi(f)\phi(g)$ donc ϕ est un homomorphisme.
Montrons que ϕ est injective : soient f et g deux éléments de Aut$(\mathbb{Z}/n\mathbb{Z})$ tels que $\phi(f) = \phi(g)$.
On a alors f($\overline{1}$)=g($\overline{1}$).
D'où, pour tout élément $\overline{x}$ de $\mathbb{Z}/n\mathbb{Z}$, f($\overline{x}$)=f(x$\overline{1}$)=x f($\overline{1}$)=x g($\overline{1}$)=g(x$\overline{1}$)=g($\overline{x}$) et donc, f=g. ϕ est injective.
L'ordre de Aut$(\mathbb{Z}/n\mathbb{Z})$ est φ(n).
Or d'après la question 2, U$(\mathbb{Z}/n\mathbb{Z})$ est aussi d'ordre φ(n).
D'où, puisque ϕ est injective, ϕ est surjective.
Aut$(\mathbb{Z}/n\mathbb{Z})$ est donc isomorphe à U$(\mathbb{Z}/n\mathbb{Z})$.
5)U$(\mathbb{Z}/n\mathbb{Z})$ est abélien et Aut$(\mathbb{Z}/n\mathbb{Z})$ est abélien donc Aut$(\mathbb{Z}/n\mathbb{Z})$ est abélien d'après la Proposition 1.3.5.
Remarque : D'après la question 2, $(\mathbb{Z}/n\mathbb{Z}$-{0},.) est un groupe si et seulement si n est un nombre premier.

Exercice 9 : 1)Montrons que avm est congru à a modulo n : puisque un+vm=1, on a aun+avm=a. Comme aun est congru à 0 modulo n (car n divise aun), on obtient a congru à avm modulo n.
bun étant congru à 0 modulo n, bun+avm est congru à a modulo n.
On montre de même que bun+avm est congru à b modulo m.
D'où, x_0=bun+avm est une solution de (S).
2)x et x_0 sont congrus à a modulo n donc x-x_0 est congru à 0 modulo n.
D'où, n divise x-x_0.
De même, puisque x et x_0 sont congrus à b modulo m, x-x_0 est congru à 0 modulo n et donc m divise x-x_0.
3)D'après la question précédente, il existe deux entiers s et t tels que x-x_0=sn=tm.
D'après le Théorème de Bezout, il existe deux entiers u et v tels que 1=un+vm.

D'où, x-x_0=u(x-x_0)n+v(x-x_0)m=utmn+vsnm=(ut+vs)nm et donc nm divise x-x_0.
4)D'après la question précédente, si x est solution du système (S) alors il existe un entier k tel que x=x_0+knm.
Soit k un entier. Puisque x_0 est congru à a modulo n et knm est congru à 0 modulo n, x_0+knm est congru à a modulo n.
De même, x_0 étant congru à b modulo m et knm étant congru à 0 modulo m, x_0+knm est congru à b modulo m.
On en déduit que pour tout entier k, x_0+knm est solution du système (S).
D'où, les solutions du système (S) sont les éléments de l'ensemble $\{x_0 + knm \ / \ k \in \mathbb{Z}\}$.
5)3 et 5 étant premiers entre eux, on peut appliquer le résultat de la question précédente.
Puisque 2.3+(-1).5=1, une solution particulière du système (C) : $\left\{ \begin{array}{l} x \equiv 2 \ mod \ 3 \\ x \equiv 1 \ mod \ 5 \end{array} \right.$ est x_0=1.2.3+2.(-1).5=-4.
D'après la question précédente, l'ensemble des solutions du système (C) est {-4+15k, k$\in \mathbb{Z}$}.
Remarque : Il existe plusieurs couples d'entiers (u,v) tels que un+vm=1. Si (u,v) et (u',v') sont deux tels couples et si on pose x_0=bun+avm et x'_0=bu'n+av'm, les ensembles E=$\{x_0 + knm \ / \ k \in \mathbb{Z}\}$ et E'=$\{x'_0 + knm \ / \ k \in \mathbb{Z}\}$ sont égaux car $x_0 \in$E' et $x'_0 \in$E d'après la question 3 (nm divise $x_0 - x'_0$).

Exercice 10 : A)1)Soient $\overline{x}$=$\overline{y}$ deux éléments égaux de $\mathbb{Z}/n\mathbb{Z}$.
On a alors x congru à y modulo nm.
D'où, x-y est congru à 0 modulo nm (Seconde Propriété 2.1.2) c'est à dire nm divise x-y.
On en déduit que n divise x-y c'est à dire x-y est congru à 0 modulo n et m divise x-y c'est à dire x-y est congru à 0 modulo m.
Par conséquent, x est congru à y modulo n c'est à dire $\hat{x} = \hat{y}$ et x est congru à y modulo m c'est à dire $\check{x} = \check{y}$.
D'où, f($\overline{x}$)=f($\overline{y}$) et f est une application.
2)Soient $\overline{x}$ et $\overline{y}$ deux éléments de $\mathbb{Z}/n\mathbb{Z}$.
On a

$$\begin{array}{rcl} f(\overline{x}+\overline{y}) & = & (\hat{x}+\hat{y}, \check{x}+\check{y}) \\ & = & (\hat{x},\check{x})+(\hat{y},\check{y}) \ \textit{par dfinition de la loi d'un groupe produit} \\ & = & f(\overline{x})+f(\overline{y}) \end{array}$$

donc f est un homomorphisme.
3)Il existe deux entiers s et t tels que x=sn=tm.
D'après le Théorème de Bezout, il existe deux entiers u et v tels que 1=un+vm. D'où, x=uxn+vxm=utmn+vsnm=(ut+vs)nm et donc nm divise x.
4)Soit $\overline{x}$ un élément de $\mathbb{Z}/n\mathbb{Z}$ tel que f($\overline{x}$)=$(\hat{0}, \check{0})$.
Alors, $\hat{x} = \hat{0}$ donc n divise x et $\check{x} = \check{0}$ donc m divise x.
D'où, d'après la question précédente, nm divise x c'est à dire x est congru à 0 modulo nm.
Par conséquent, $\overline{x}$=$\overline{0}$ et f est un homomorphisme injectif.
5)Montrons que f est un homomorphisme surjectif :

Puisque n et m sont premiers entre eux, il existe deux entiers u et v tels que un+vm=1.
Puisque n divise un, $\hat{1} = \hat{un} + \hat{vm} = \hat{vm}$. Comme m divise vm, on a $\check{vm} = \check{0}$.
D'où f($\overline{vm}$)=($\hat{1}, \check{0}$).
On montre de même que f($\overline{un}$)=($\hat{0}, \check{1}$).
Soit $(\hat{x}, \check{y})$ un élément de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
Puisque x et y sont des entiers, on a

$$\begin{aligned}
(\hat{x}, \check{y}) &= (\hat{x}, \check{0}) + (\hat{0}, \check{y}) \\
&= (\hat{x.1}, \check{0}) + (\hat{0}, \check{y.1}) \\
&= x(\hat{1}, \check{0}) + y(\hat{0}, \check{y}) \\
&= xf(\overline{vm}) + yf(\overline{un}) \\
&= f(x\overline{vm} + f(y\overline{un}) \text{ } car \text{ } f \text{ } est \text{ } un \text{ } homomorphisme \\
&= f(\overline{xvm} + f(\overline{yun}) \\
&= f(\overline{xvm + yun}) \text{ } car \text{ } f \text{ } est \text{ } un \text{ } homomorphisme.
\end{aligned}$$

D'où, f est un homomorphisme surjectif.
F est donc un isomorphisme entre les groupes $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
6)$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$ est un groupe cyclique donc $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est un groupe cyclique d'après la Proposition 2.2.4.
Remarque : L'isomorphisme f permet de retrouver les solutions du système (S) de l'Exercice 9. En effet, si x est solution de x alors $\overline{x}$ est l'unique antécédent de $(\hat{a}, \check{b})$ par f.
Comme cet antécédent est $\overline{avm + bun}$, on a $\overline{x}$=$\overline{avm + bun}$ c'est à dire x=avm+bun+knm où k est un entier. B)1)Soit k=ppcm(o($\hat{x}$),o($\check{y}$)).
Puisque k est un multiple de o($\hat{x}$) et de o($\check{y}$), k($\hat{x}$,$\check{y}$)=($k\hat{x}$,$k\check{y}$)=(0,0).
L'ordre de ($\hat{x}$,$\check{y}$) divise donc k, d'après la Proposition 1.2.9.
Soit s un entier tel que s($\hat{x}$,$\check{y}$)=($s\hat{x}$,$s\check{y}$)=(0,0).
Alors, o($\hat{x}$) et o($\check{y}$) divisent s donc s est un multiple de o($\hat{x}$) et o($\check{y}$).
D'où, k divise s. On en déduit, d'après la Proposition 1.2.8, que l'ordre de ($\hat{x}$,$\check{y}$) est ($\hat{x}$,$\check{y}$)).
2)Par hypothèse, pgcd(n,m)>1.
Pour montrer que $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ n'est pas cyclique, on va montrer que l'ordre de tout élément de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est strictement inférieur à l'ordre de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ c'est à dire nm.
Soit ($\hat{x}$,$\check{y}$) un élément de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. On note a (respectivement b, k) l'ordre de $\hat{x}$ (respectivement $\check{y}$, ($\hat{x}$,$\check{y}$).
Supposons que k=nm.
D'après la question précédente, k est égal au ppcm de a et b.
Or le ppcm de a et b est compris entre 1 et ab et ab est inférieur à nm (car a est compris entre 1 et n et b est compris entre 1 et m) donc ab=nm=k.
Puisque a est compris entre 1 et n et b est compris entre 1 et m, cette égalité entraîne a=n et b=m.
D'où, k=ppcm(a,b)=ppcm(n,m).
Or pgcd(n,m)>1 et pgcd(n,m)k=pgcd(n,m)ppcm(n,m)=nm donc k<nm.
Contradiction.
L'ordre de tout élément de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est strictement inférieur à nm.
Par conséquent, $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ n'est pas cyclique puisqu'il ne possède pas de générateur.

7.3 Correction des exercices du Chapitre 3

Exercice 1 : 1)Soit α un automorphisme de G.
Pour tout couple (g,g') d'éléments de G,
$\alpha[g,g'] = \alpha(gg'g^{-1}g'^{-1}) = \alpha(g)\alpha(g')\alpha(g)^{-1}\alpha(g')^{-1} = [\alpha(g),\alpha(g')]$.
D'où, puisque D(G) est engendré par les commutateurs $[g,g']$, α(D(G)) est inclus dans D(G).
Cette propriété étant vraie pour tout automorphisme α, elle est vraie pour tout α^{-1}, $\alpha \in$Aut(G).
D'où, α^{-1}(D(G)) est inclus dans D(G) c'est à dire D(G) est inclus dans α(D(G)).
α(D(G))=D(G) pour tout automorphisme α de G donc D(G) est un sous-groupe caractéristique de G.
2)Par hypothèse, α(H)=H pour tout automorphisme α de G.
Quel que soit l'élément g de G, l'application α_g : x $\rightarrow$ gxg^{-1}, est un automorphisme de G (d'inverse $\alpha_{g^{-1}}$).
D'où, pour tout élément g de G, gHg^{-1} = α_g(H)=H et H est donc un sous-groupe normal de G.
3)Soit α un automorphisme de G.
Puisque H est caractéristique dans G, α(h) et α^{-1}(h) appartiennent à H pour tout élément h de H.
D'où, la restriction α_H de α à H est un automorphisme de H.
Puisque K est caractéristique dans H, α_H(K)=α(K) est inclus dans K.
Cette propriété étant vraie pour tout automorphisme α, elle est vraie pour tout α^{-1}, $\alpha \in$Aut(G).
D'où, α^{-1}(K) est inclus dans K c'est à dire K est inclus dans α(K).
K est donc un sous-groupe caractéristique de G.
4)Soit g un élément de G.
Puisque N est normal dans G, l'application α_g définie par α_g(n)=gng^{-1} pour tout élément n de N, est un endomorphisme de N.
L'application α_g est un automorphisme de N (d'inverse $\alpha_{g^{-1}}$).
D'où, puisque H est caractéristique dans N, gHg^{-1} = α_g(H)=H.
H est donc un sous-groupe normal de G.

Exercice 2 : 1)N_A n'est pas vide car A, non vide, est inclus dans N_A (en prenant n=1 et g_1=1). Soient x=$(g_1a_1g_1^{-1})$ ... $(g_na_ng_n^{-1})$ et y=$(g'_1b_1g'^{-1}_1)$ ... $(g'_mb_mg'^{-1}_m)$ deux éléments de N_A (n,m$\in \mathbb{N}$, $\forall 1 \leq i \leq n$ $g_i \in$G et ($a_i \in$A ou $a_i^{-1} \in$A), $\forall 1 \leq i \leq m$ $g'_i \in$G et ($b_i \in$A ou $b_i^{-1} \in$A)).
Pour tout entier i compris entre 1 et m, b_i^{-1} appartient à A ou $(b_i^{-1})^{-1} = b_i$ appartient à A donc xy^{-1}=$(g_1a_1g_1^{-1})\dots(g_na_ng_n^{-1})(g'_1b_1^{-1}g'^{-1}_1)\dots(g'_mb_m^{-1}g'^{-1}_m)$ appartient à N_A.
D'où, N_A est un sous-groupe de G.
Soient g un élément de G et x=$(g_1a_1g_1^{-1})$ ... $(g_na_ng_n^{-1})$ un élément de N_A (n$\in \mathbb{N}$ et $\forall 1 \leq i \leq n$, $g_i \in$G et ($a_i \in$A ou $a_i^{-1} \in$A).

$$\begin{aligned} gxg^{-1} &= g(g_1a_1g_1^{-1})\dots(g_na_ng_n^{-1})g^{-1} \\ &= (gg_1a_1g_1^{-1}g^{-1})\dots(gg_na_ng_n^{-1}g^{-1}) \\ &= (gg_1)a_1(gg_1)^{-1}\dots(gg_n)a_n(gg_n)^{-1} \end{aligned}$$

donc gxg^{-1} appartient à N_A.
N_A est un sous-groupe normal de G contenant A.
2)Soit N un sous-groupe normal de G contenant A.
Soient a un élément de A et g un élément de G.
Puisque N est normal dans G, gag^{-1} appartient à N.
Si b est un élément de G tel que b^{-1} appartient à A alors b^{-1} appartient à N et puisque N est un sous-groupe de G, b appartient à N.
D'où, puisque N est normal dans G, gbg^{-1} appartient à N pour tout élément g de G.
On en déduit, N étant un sous-groupe de G, que N contient tous les éléments de G de la forme $(g_1a_1g_1^{-1})$ ... $(g_na_ng_n^{-1})$ avec n$\in \mathbb{N}$ et $\forall 1 \leq i \leq n$, $g_i \in$G et ($a_i \in$A ou $a_i^{-1} \in$A). N_A est donc inclus dans N.
N_A est le plus petit (au sens de l'inclusion) sous-groupe normal de G contenant A.

Exercice 3 : 1)Soit p un nombre premier.
Soit H un sous-groupe de $\mathbb{Z}$ contenant p$\mathbb{Z}$.
D'après la Proposition 2.1.7, il existe un entier naturel n tel que H=n$\mathbb{Z}$.
Puisque p$\mathbb{Z}$ est inclus dans H, p appartient à H.
D'où, n divise p.
Or p est premier donc n=1 et H=$\mathbb{Z}$ ou n=p et H=p$\mathbb{Z}$.
Les sous-groupes p$\mathbb{Z}$ avec p premier, sont des sous-groupes maximaux de $\mathbb{Z}$.
Soit n$\mathbb{Z}$ un sous-groupe maximal de $\mathbb{Z}$.
Soit d un diviseur positif de n.
n appartient alors à d$\mathbb{Z}$ et n$\mathbb{Z}$ est donc inclus dans d$\mathbb{Z}$.
D'où, puisque n$\mathbb{Z}$ est un sous-groupe maximal de $\mathbb{Z}$, d$\mathbb{Z}$=n$\mathbb{Z}$ c'est à dire d=n ou d$\mathbb{Z} = \mathbb{Z}$ c'est à dire d=1.
D'où, puisque les seuls diviseurs positifs de n sont 1 et n, n est un nombre premier.
2)Nous allons montrer les deux propriétés en même temps.
Soit H un sous-groupe de G différent de G (il y en a au moins : {1}).
Si H est maximal alors on a fini.
Si H n'est pas maximal alors il existe un sous-groupe K de G, différent de H et G, contenant H.
Si K est maximal alors on a fini.
Sinon on recommence le raisonnement avec K.
Puisque G est fini, le processus s'arrête.
Il existe un sous-groupe maximal M de G contenant H.
3)Puisque N est un sous-groupe normal de G, le groupe quotient G/N est bien défini.
Soit π la surjection canonique de G vers G/N.
($\Rightarrow$) Montrons que G/N n'a pas de sous-groupes propres :
Soit K un sous-groupe de G/N.
D'après la Proposition Ss-gr qotients, K=π(H) où H est un sous-groupe de G contenant N.
Or N est un sous-groupe maximal de G donc H=N c'est à dire K={1} ou H=G c'est à dire K=G/N.

G/N n'a pas de sous-groupes propres donc (cf Exercice 6 du Chapitre 2) G/N est un groupe cyclique d'ordre un nombre premier.
($\Leftarrow$) Puisque G/N est d'ordre premier, G/N ne possède pas de sous-groupes propres.
Soit H un sous-groupe de G contenant N.
Alors, puisque π est un homomorphisme, π(H) est un sous-groupe de G/N.
D'où, π(H)=$\{1\}$ c'est à dire H=N (Ker π=N) ou π(H)=G/N c'est à dire H=G.
N est donc un sous-groupe maximal de G.

Exercice 4 : 1)Nous allons montrer les deux propriétés en même temps.
Soit H un sous-groupe normal de G différent de G (il y en a au moins : $\{1\}$).
Si H est normal maximal alors on a fini.
Si H n'est pas normal maximal alors il existe un sous-groupe normal K de G, différent de H et G, contenant H.
Si K est normal maximal alors on a fini.
Sinon on recommence le raisonnement avec K.
Puisque G est fini, le processus s'arrête.
Il existe un sous-groupe normal maximal N de G contenant H.
2)Puisque N est un sous-groupe normal de G, le groupe quotient G/N est bien défini.
Soit π la surjection canonique de G vers G/N.
($\Rightarrow$) Montrons que G/N n'a pas de sous-groupe normal non trivial : soit K un sous-groupe normal de G/N.
D'après la Proposition Ss-gr qotients, K=π(H) où H est un sous-groupe normal de G contenant N.
Or N est un sous-groupe normal maximal de G donc H=N c'est à dire K=$\{1\}$ ou H=G c'est à dire K=G/N.
G/N n'a pas de sous-groupe normal non trivial donc G/N est un groupe simple.
($\Leftarrow$) Puisque G/N est simple, G/N ne possède pas de sous-groupe normal non trivial.
Soit H un sous-groupe normal de G contenant N.
Alors, d'après la Proposition Ss-gr qotients, π(H) est un sous-groupe normal de G/N.
D'où, π(H)=$\{1\}$ c'est à dire H=N (Ker π=N) ou π(H)=G/N c'est à dire H=G.
N est donc un sous-groupe normal maximal de G.
3)Un sous-groupe normal et maximal de G est clairement normal maximal.
Si N est normal maximal dans G alors G/N est un groupe simple (d'après la question 2) c'est à dire ne possède pas de sous-groupe normal différent de $\{1\}$ et G/N.
Mais N est maximal dans G si et seulement si G/N ne possède pas de sous-groupe différent de $\{1\}$ et G/N.
Il existe des groupes simples possédant des sous-groupes propres (par exemple, le groupe alterné A_5 que nous étudierons plus en détail plus tard) donc un sous-groupe normal maximal n'est pas forcément maximal.
Si G est abélien alors tous les sous-groupes de G sont normaux dans G et donc les sous-groupes normaux maximaux et les sous-groupes maximaux sont les mêmes.

Exercice 5 : 1)D'après la Question 1 de l'Exercice 3, $\Upsilon_{\mathbb{Z}} = \{p\mathbb{Z} \text{ / p premier }\}$.
$\Phi(\mathbb{Z}) = \cap_{p\,premier} p\mathbb{Z}$.
Montrons que $\Phi(\mathbb{Z}) = \{1\}$: 1 appartient à $\Phi(\mathbb{Z})$.
Soit n un entier strictement supérieur à 1.

Il existe un nombre premier p ne divisant pas n (il suffit de prendre un nombre premier strictement supérieur à n).
D'où, n n'appartient pas à $p\mathbb{Z}$ et donc n n'appartient pas à $\Phi(\mathbb{Z})$.
D'où, $\Phi(\mathbb{Z}) = \{1\}$.
2)$\Phi(G)$ étant une intersection de sous-groupes de G, Φ(G) est un sous-groupe de G.
Soit α un automorphisme de G.
Si $\Upsilon_G = \emptyset$ alors $\Phi(G)$=G et donc, puisque α est surjective, $\alpha(\Phi(G)) = \Phi(G)$.
On suppose Υ_G non vide.
Puisque α est injective, $\alpha(\Phi(G)) = \alpha(\cap_{M\in\Upsilon_G} M) = \cap_{M\in\Upsilon_G} \alpha(M)$.
Montrons que si M est maximal alors α(M) est maximal :
Puisque α est un homomorphisme, α(M) est un sous-groupe de G.
Soit H un sous-groupe de G contenant α(M).
Alors, α^{-1}(H) est un sous-groupe de G contenant M.
D'où, puisque M est maximal, α^{-1}(H)=M c'est à dire H=α(M) ou α^{-1}(H)=G c'est à dire H=α(G).
Ainsi, α(M) est un sous-groupe maximal de G.
Puisque cette propriété est vraie pour tout automorphisme α, elle est vraie pour α^{-1}, $\alpha \in$Aut(G).
On en déduit que si M est maximal alors $\alpha^{-1}(M)$ est maximal.
D'où, $\alpha(\Phi(G)) = \cap_{M\in\Upsilon_G} \alpha(M) = \cap_{M\in\Upsilon_G} M = \Phi(G)$.
Ainsi, $\Phi(G)$ est un sous-groupe caractéristique de G.

Exercice 6 : 1)Soient h un élément de H et g un élément de G.
Puisque f est surjective, il existe un élément g' de G tel que g=f(g').
Puisque f est un homomorphisme, g^{-1}=f(g'^{-1}).
D'où, $gf(h)g^{-1}$=f(g')f(h)f(g'^{-1})=f(g'hg'$^{-1}$).
H étant normal dans G, g'hg'$^{-1}$ appartient à H et $gf(h)g^{-1}$ appartient donc à f(H).
f(H) est un sous-groupe normal de G.
2)Puisque H et f(H) sont normaux dans G, les groupes quotients G/H et G/f(H) sont bien définis.
Pour tout élément g de G, on note $\overline{g}$ la classe de g dans G/H et $\widehat{g}$ la classe de g dans G/f(H).
D'après la Proposition 3.2.8, il existe un (unique) homomorphisme de groupes $\overline{f}$ de G/H dans G/f(H) tel que $\overline{f}(\overline{g}) = \widehat{f(g)}$ pour tout élément g de G.
Montrons que $\overline{f}$ est injective : soient $\overline{g}$ et $\overline{g}'$ deux éléments égaux de G/H.
Alors, gg'$^{-1}$ appartient à H donc f(gg'$^{-1}$)=f(g)f(g')$^{-1}$ appartient à f(H).
D'où, $\widehat{f(g)} = \widehat{f(g')}$ et $\overline{f}$ est injective.
Montrons que $\overline{f}$ est surjective : soit $\widehat{g}$ un élément de G/f(H).
f étant surjective, il existe un élément g' de G tel que g=f(g').
Alors, $\overline{f}(\overline{g}') = \widehat{f(g')} = \widehat{g}$ et $\overline{f}$ est surjective.
$\overline{f}$ est un isomorphisme entre G/H et G/f(H).

Exercice 7 : 1)$H_1 \times H_2$ n'est pas vide car (1,1) appartient à $H_1 \times H_2$.
Soient (h_1, h_2) et (h'_1, h'_2) deux éléments de $H_1 \times H_2$. $(h_1, h_2)(h'_1, h'_2)^{-1} = (h_1, h_2)({h'_1}^{-1}, {h'_2}^{-1}) = (h_1{h'_1}^{-1}, h_2{h'_2}^{-1})$ appartient à $H_1 \times H_2$ car H_1 est un sous-groupe de G_1 et H_2 est un sous-groupe de G_2. D'où, $H_1 \times H_2$ est un sous-groupe de $G_1 \times G_2$.
Soient (h_1, h_2) un élément $H_1 \times H_2$ et (g_1, g_2) un élément de $G_1 \times G_2$.
$(g_1, g_2)(h_1, h_2)(g_1, g_2)^{-1} = (g_1, g_2)(h_1, h_2)({g_1}^{-1}, {g_2}^{-1}) = (g_1 h_1 {g_1}^{-1}, g_2 h_2 {g_2}^{-1})$ appartient à $H_1 \times H_2$ car H_1 est normal dans G_1 et H_2 est normal dans G_2.
D'où, $H_1 \times H_2$ est un sous-groupe normal de $G_1 \times G_2$.
2)Les groupes quotients $G_1 \times G_2 / H_1 \times H_2$, G_1/H_1 et G_2/H_2 sont bien définis.
Si g_1 est un élément de G_1, on note $\overline{g_1}$ la classe de g_1 dans G_1/H_1 et si g_2 est un élément de G_2, on note $\widehat{g_2}$ la classe de g_2 dans G_2/H_2.
Soit f l'application de $G_1 \times G_2$ dans $G_1/H_1 \times G_2/H_2$ définie par $f(g_1, g_2) = (\overline{g_1}, \widehat{g_2})$.
Montrons que f est un homomorphisme de groupes : soient (g_1, g_2) et (g'_1, g'_2) deux éléments de $G_1 \times G_2$.

$$\begin{aligned} f((g_1, g_2)(g'_1, g'_2)) &= f(g_1 g'_1, g_2 g'_2) \\ &= (\overline{g_1 g'_1}, \widehat{g_2 g'_2}) \\ &= (\overline{g_1}\,\overline{g'_1}, \widehat{g_2}\,\widehat{g'_2}) \\ &= (\overline{g_1}, \widehat{g_2})(\overline{g'_1}, \widehat{g'_2}) \\ &= f(g_1, g_2) f(g'_1, g'_2). \end{aligned}$$

D'où, f est un homomorphisme de groupes.
f est clairement surjective car l'élément $(\overline{g_1}, \widehat{g_2})$ de $G_1/H_1 \times G_2/H_2$ admet l'élément (g_1, g_2) de $G_1 \times G_2$ comme antécédent.
Déterminons le noyau de f : Ker f$= \{(g_1, g_2) \in G_1 \times G_2 \ / \ (\overline{g_1}, \widehat{g_2}) = (\overline{1}, \widehat{1})\} =$
$\{(g_1, g_2) \in G_1 \times G_2 \ / \ g_1 \in G_1 \text{ et } g_2 \in G_2\} = H_1 \times H_2$.
D'où, d'après le Premier Théorème d'isomorphisme, $G_1 \times G_2 / H_1 \times H_2 = G_1 \times G_2 /$Ker f est isomorphe à Im f$= G_1/H_1 \times G_2/H_2$.

Exercice 8 : On note ax+b à la place de (x$\rightarrow$ax+b).
1)Montrons que A est un sous-groupe de l'ensemble B des applications bijectives de $\mathbb{R}$ dans $\mathbb{R}$: l'ensemble A n'est pas vide puisque il contient l'application nulle.
Une application affine ax+b est bijective d'inverse $\frac{1}{a}$x-$\frac{b}{a}$ donc A est inclus dans B.
Soient ax+b et cx+d deux éléments de A.
On a (ax+b)$\circ$(cx+d)$^{-1}$=(ax+b)$\circ$($\frac{1}{c}$x-$\frac{d}{c}$)= $\frac{a}{c}$x-$\frac{ad+bc}{c}$ $\in$A donc A est un sous-groupe de B. A étant un sous-groupe, A est un groupe.
2)Soit α l'application de A dans $\mathbb{R}$ définie par α(ax+b)=a.
Si ax+b et cx+d sont deux éléments de A, on a
α((ax+b)$\circ$(cx+d))=α(acx+ad+b)=ac=α(ax+b)α(cx+d) donc α est un homomorphisme du groupe A vers le groupe $(\mathbb{R}^*, \times)$.
Il est clair que N=Ker f donc N est un sous-groupe normal de A.
3)D'après le Premier Théorème d'isomorphisme, A/N est isomorphe à Im α.
Or α est surjective puisque si a est un réel non nul, α(ax)=a.
D'où, Im $\alpha = \mathbb{R}^*$ et A/N est isomorphe à $\mathbb{R}^*$.

Exercice 9 : $\mathbb{U}$ est un groupe pour la multiplication complexe car 1 appartient à $\mathbb{U}$ et si z et z' appartiennent à $\mathbb{U}$, $|\frac{z}{z'}| = \frac{|z|}{|z'|}$=1.
1)Un nombre complexe de module s'écrit sous la forme z=$e^{i\theta}$ où $0 \leq \theta < 2\pi$.
On peut également écrire z sous la forme $e^{2\pi ia}$ où $0 \leq a < 1$ en posant a=$\frac{\theta}{2\pi}$.
Soit f l'application de $\mathbb{R}$ dans $\mathbb{U}$ définie par f(a)=$e^{2\pi ia}$.
Vérifions que f est un homomorphisme de groupes : soient a et b deux réels.
f(a+b)=$e^{2\pi i(a+b)} = e^{2\pi ia}e^{2\pi ib}$=f(a)f(b) donc f est un homomorphisme.
Déterminons le noyau de f :

$$\begin{aligned} Ker\, f &= \{a \in \mathbb{R} \,/\, f(a) = 1\} \\ &= \{a \in \mathbb{R} \,/\, e^{2\pi ia} = 1\} \\ &= \{a \in \mathbb{R} \,/\, a \in \mathbb{Z}\} \\ &= \mathbb{Z}. \end{aligned}$$

D'où, d'après le Premier Théorème d'isomorphisme, $\mathbb{R}/\mathbb{Z}$ est isomorphe à Im f.
Or f est clairement surjective puisque l'élément $e^{2\pi ia}$ de $\mathbb{U}$ possède le réel a comme antécédent.
D'où, Im f=$\mathbb{U}$ et $\mathbb{U}$ est isomorphe à $\mathbb{R}/\mathbb{Z}$.
2)Soit g l'application de $\mathbb{C}^*$ dans $\mathbb{R}_+^*$ définie par g(z)=$|z|$.
g est un homomorphisme de groupes puisque pour tout couple (z,z') de complexes, on a $|zz'| = |z||z'|$.
Le noyau de g est l'ensemble des nombres complexes de module 1 c'est à dire $\mathbb{U}$.
D'où, d'après le Premier Théorème d'isomorphisme, $\mathbb{C}^*/\mathbb{U}$ est isomorphe à Im g.
Or f est clairement surjective puisque le réel strictement positif x possède le complexe x comme antécédent.
D'où, Im g=$\mathbb{R}_+^*$ et $\mathbb{C}^*/\mathbb{U}$ est isomorphe à $\mathbb{R}_+^*$.

Exercice 10 : Raisonnons par récurrence sur n$\geq$2 :
Si n=2 alors le résultat est clair.
Supposons la propriété vraie pour n>2 : $H_1H_2 \dots H_n$ est donc un sous-groupe de G.
On suppose que pour tout couple d'entiers (i,j) avec 1$\leq$i<j$\leq$n+1, H_iH_j est un sous-groupe de G.
Montrons que $(H_1H_2 \dots H_n)H_{n+1} = H_{n+1}(H_1H_2 \dots H_n)$:
D'après la Proposition 3.4.1, $H_nH_{n+1} = H_{n+1}H_n$, $H_{n-1}H_{n+1} = H_{n+1}H_{n-1}$, ... , $H_1H_{n+1} = H_{n+1}H_1$ donc $(H_1H_2 \dots H_n)H_{n+1} = H_1H_2 \dots H_{n+1}H_n = \dots = H_{n+1}(H_1H_2 \dots H_n)$.
D'où, puisque $H_1H_2 \dots H_n$ et H_{n+1} sont des sous-groupes de G, $H_1H_2 \dots H_nH_{n+1}$ est un sous-groupe de G, d'après la Proposition 3.4.1.

7.4 Correction des exercices du Chapitre 4

Exercice 1 : Il est clair que {{(g,x)∈ G×E / g.x=x} / g∈G} et
{{(g,x)∈G×E / g.x=x} / x∈E} forment deux partitions de {(g,x)∈G×E / g.x=x}.
G et E étant finis, on a donc
$\sum_{g\in G}$ Card {x∈E / g.x=x} = $\sum_{x\in E}$ Card {g∈G / g.x=x}.
Or, pour tout élément x de E, {g∈G / g.x=x} = G_x donc
$\sum_{g\in G}$ Card {x∈E / g.x=x} = $\sum_{x\in E}$ $|G_x|$.
Si x est un élément de E, on note Ω_x l'orbite de x.
Pour tout élément x de E, $|G_x| = \frac{|G|}{Card\,\Omega_x}$ (Proposition 4.1.10) donc $\sum_{g\in G}$ Card {x∈E / g.x=x} = $|G|\sum_{x\in E}\frac{1}{Card\,\Omega_x}$.
En regroupant les éléments de E suivant leur orbite, on a $\sum_{g\in G}$ Card {x∈E / g.x=x} = $|G|\sum_{x\in R}\frac{Card\,\Omega_x}{Card\,\Omega_x} = |G|n$ où R est un ensemble de représentants des orbites de E et n est le nombre d'orbites de E.
Le nombre d'orbites de E est donc égal à $\frac{1}{|G|}\sum_{g\in G}$ Card {x∈E / g.x=x}.

Exercice 2 : G opère sur $(G/H)_g$ par translations à gauche : g.(g'H)=gg'H. D'où, comme H est un sous-groupe de G, H opère sur $(G/H)_g$ par translations à gauche.
Soient Ω_1, ... , Ω_n les orbites de $(G/H)_g$ pour cette opération.
Soit i compris entre 1 et n. Card $\Omega_i = \frac{|H|}{|H_{x_iH}|}$ où x_iH est un représentant de Ω_i (Proposition 4.1.10) donc le cardinal de Ω_i divise l'ordre de H.
H est un sous-groupe de G donc l'ordre de H divise l'ordre de G par le Théorème de Lagrange. Ainsi, le cardinal de Ω_i divise p.
p étant premier, le cardinal de Ω_i vaut soit 1 soit p
Comme les orbites forment une partition de $(G/H)_g$ et Card $(G/H)_g = [G : H]$ =p, on a p=$\sum_{i=1}^{n} Card\,\Omega_i$.
Si il existe un entier i compris entre 1 et n tel que Card Ω_i=p alors Ω_i est la seule orbite de $(G/H)_g$ et donc toute orbite de $(G/H)_g$ est égale à $\Omega_i = (G/H)_g$.
Mais l'orbite H=1H est réduite à $\{H\}$. Contradiction.
D'où, Card Ω_i=1 pour tout i compris entre 1 et n.
On en déduit que $|H_{x_iH}| = \frac{|H|}{Card\,\Omega_i} = |H|$ et donc H_{x_iH}=H pour tout i compris entre 1 et n. D'où, le stabilisateur de tout élément de $(G/H)_g$ est égal à H.
Soient x et y deux éléments de $(G/H)_g$ et g un élément de G.
Si g.x=y alors G_y=gG_xg^{-1}. En effet, g' appartient à G_y si et seulement si g'.y=y si et seulement si g^{-1}g'g.x=x si et seulement si g' appartient à gG_xg^{-1}.
Soit g un élément de G. Soit x un élément de $(G/H)_g$.
H est le stabilisateur de x donc gHg^{-1} est le stabilisateur de g.x.
Mais le stabilisateur de g.x est H donc gHg^{-1}=H.
gHg^{-1}=H pour tout élément g de G donc H est normal dans G.

Exercice 3 : 1)Soient z un élément de Z(H) et α un automorphisme de H.
Montrons que α(z) appartient à Z(G) : soit h un élément de H.
α étant surjective, il existe un élément k de H tel que α(k)=h.

D'où,

$$\begin{aligned} h\alpha(z) &= \alpha(k)\alpha(z) \\ &= \alpha(kz) \\ &= \alpha(zk)\, car\, z\, appartient\, à\, Z(H) \\ &= \alpha(z)\alpha(k) \\ &= \alpha(z)h. \end{aligned}$$

α(z) appartient à Z(G). Z(H) est donc stable par α.
2)Soit p un nombre premier divisant l'ordre de H.
D'après le Théorème de Cauchy, H possède un élément h d'ordre p.
3)a)Soit x un élément de H différent de 1.
Puisque G opère transitivement sur H\{1}, il existe un élément g de G tel que g.h=x (h est différent de 1 car d'ordre p>1).
Soit φ l'homomorphisme de G dans Aut(G) associé à l'opération de G sur H.
Si g appartient à G, on note φ_g à la place de φ(g).
h étant d'ordre p, $x^p = (\varphi_g(h))^p = \varphi_g(h^p) = \varphi_g(1)$=1.
Si x^m=1 alors $\varphi_g(h^m)$=1=φ_g(1) donc, φ_g étant injective, h^m=1.
D'où, p divise m (Proposition 1.2.9).
Ainsi, tout élément x de H, différent de 1, est d'ordre p. On en déduit que H est un p-groupe.
b)Montrons que H=Z(H) : H étant un p-groupe, Z(H) n'est pas réduit à {1}.
Soient x un élément de H\{1} et z un élément de Z(H)\{1}.
G opérant transitivement sur H\{1}, il existe un élément g de G tel que x=g.z=φ_g(z).
φ_g étant un automorphisme de H, φ_g(z) appartient à Z(H) d'après la question 1.
D'où, H est inclus dans Z(H). H=Z(H) et H est donc un groupe abélien.
4)Supposons qu'il existe un élément x de H\{1} d'ordre strictement supérieur à 2.
On a alors x^{-1} différent de x.
Montrons que x et x^{-1} sont les seuls éléments de H\{1} : soit y appartenant à H\{1, x}.
Puisque G opère 2-transitivement sur H\{1}, il existe un élément g de G tel que g.x=x et g.y=x^{-1}. g.x=φ_g(x)=x donc g.x^{-1} = φ_g(x^{-1})=x^{-1}.
D'où, y=x^{-1} (φ_g injective). D'où, N={1, x, x^{-1}} est d'ordre 3.
5)Soient x, y et t trois éléments distincts de H\{1}.
xy est différent de x car sinon y=1. De même, xy est différent de y.
Puisque G opère 3-transitivement sur H\{1}, il existe un élément g de G tel que g.x=x, g.y=y et g.xy=t.
φ_g étant un homomorphisme, t=φ_g(xy)=φ_g(x)φ_g(y)=(g.x)(g.y)=xy.
D'où, N={1, x, y, xy} est d'ordre 4.
6)Supposons que G opère 4-transitivement sur H\{1}.
Alors, H\{1} possède au moins 4 éléments distincts et H est donc d'ordre supérieur ou égal à 5.
Or, comme G opère 4-transitivement sur H\{1}, G opère 3-transitivement sur H\{1} donc, d'après la question 5, H est d'ordre 4. Contradiction.
G ne peut opérer 4-transitivement sur E donc G ne peut opérer k-transitivement sur H\{1} pour k≥4.

Exercice 4 : 1)Il existe, pour tout élément y de E distinct de x, un élément n de N\{1} tel que n.x=y.
Supposons qu'il existe un élément n' de N tel que n'.x=y=n.x.
On a alors $n^{-1}n'.x=x$ c'est à dire $n^{-1}n' \in N_x$.
D'où, par hypothèse, $n^{-1}n'=1$ et donc n'=n.
On pose $\theta(y)=n$.
Montrons que l'application θ ainsi définie de E\{x} dans N\{1} est une bijection : soient y et z deux éléments de E\{x} tels que $\theta(y)=\theta(z)=n$.
On a alors, par définition de n, y=n.x=z. θ est donc injective.
Soit n appartenant à N\{1}. Montrons que n.x est différent de x : si n.x=x alors n appartient à $N_x=\{1\}$. Contradiction. n.x est différent de x.
$n=\theta(n.x)$ donc θ est surjective. θ est bijective.
Comme l'identité est clairement un automorphisme de G_x, il reste à montrer que pour tout élément g de G_x et pour tout élément y de E\{x}, $\theta(g.y)=g\theta(y)g^{-1}$ (G_x opère sur N\{1} par conjugaison). Posons $n=\theta(y)$. On a alors n.x=y.
D'où, $gng^{-1}.x=gn.x=g.y$ car g^{-1} appartient au groupe G_x. Ainsi, $\theta(g.y)=gng^{-1}=g\theta(y)g^{-1}$.
L'opération de G_x sur E\{x} est donc équivalente à l'opération de conjugaison de G_x sur N\{1}.
2)Puisque G opère m-transitivement sur E, G_x opère (m-1)-transitivement sur E\{x}.
D'où, d'après la question précédente, G_x opère (m-1)-transitivement sur N\{1}.
N\{1} étant en bijection avec l'ensemble fini E\{x}, N est un groupe fini.
G_x opère sur N par conjugaison.
Notons φ l'homomorphisme de G_x dans Aut(N) associé à cette opération.
Soit g un élément de G_x. On note φ_g à la place de φ(G).
Montrons que l'application φ_g : $n \to gng^{-1}$ est un automorphisme de N :
Pour tout couple (n,n') d'éléments de N, $\varphi_g(nn')=g(nn')g^{-1}=gng^{-1}gn'g^{-1}=\varphi_g(n)\varphi_g(n')$ donc φ_g est un endomorphisme de N. φ_g étant bijective (car G_x opère sur N), φ_g est un automorphisme de N.
On peut donc appliquer les résultats de l'Exercice précédent :
a)Si m=2 alors G_x opère transitivement sur N. D'où, N est un p-groupe autrement dit, l'ordre de N est une puissance non nulle d'un nombre premier p. Puisque E et N ont le même cardinal (car N\{1} et E\{x} sont en bijection), le cardinal de N est une puissance non nulle d'un nombre premier p.
b)Si m=3 alors N est d'ordre 3 et par conséquent E est de cardinal 3, ou tous les éléments de N sont d'ordre 2 ce qui entraine que N est un 2-groupe et par conséquent E est de cardinal une puissance non nulle de 2.
c)Si m=4 alors N est d'ordre 4 et E est donc de cardinal 4.
d)Puisque G_x ne peut opérer k-transitivement sur N pour $k \geq 4$, G ne peut opérer m-transitivement sur E pour $m \geq 5$.

Exercice 5 : 1)Puisque N est un sous-groupe normal de G, N$\cap G_x$ est un sous-groupe normal de G_x. G_x étant un groupe simple, on a N$\cap G_x = \{1\}$ ou N$\cap G_x = G_x$.
Mais N$\cap G_x = N_x$ et N_x est différent de $\{1\}$ donc N$\cap G_x = G_x$.
On en déduit que G_x est inclus dans N.
2)Puisque G opère primitivement sur E, G_x est un sous-groupe maximal de G d'après la Proposition 4.4.11.
D'où, N=G_x ou N=G.
Soit φ l'homomorphisme de G dans S_E associé à l'opération de G sur E.
Puisque G opère fidèlement sur E, on a Ker $\varphi = \{1\}$.
Supposons que N=G_x.
Alors, pour tout élément g de G, $G_{g.x}$=gG_xg^{-1}=gNg^{-1}=N car N est normal dans G.
Soit y un élément de E.
Puisque G opère transitivement sur E, il existe un élément g de G tel que y=g.x.
On a alors G_y=N.
Ainsi, quels que soient les éléments n de N et y de E, n.y=y et par conséquent, N est inclus dans Ker $\varphi = \{1\}$. Contradiction.
D'où, N=G.
3)Les seuls sous-groupes normaux de G sont $\{1\}$ et G donc G est un groupe simple.

Remarque *Les Exercices 4 et 5 peuvent être utilisés pour démontrer la simplicité des groupes alternés A_n, n$\geq$5.*

Exercice 6 : 1)Soit x=$(x_1, \ldots, x_p)$ un élément de X.
Puisque $x_1 \ldots x_p$=1, x est déterminé par la valeur de $x_1, \ldots, x_{p-1}$ ($x_p = {x_{p-1}}^{-1} \ldots {x_1}^{-1}$).
D'où, le cardinal de X est égal à $|G|^{p-1}$.
2)Soient k et m deux éléments de $\mathbb{Z}/p\mathbb{Z}$ et $(x_1, \ldots, x_p)$ un élément de x.
On a k.(m.$(x_1, \ldots, x_p)$)=k.$(x_{1+m}, \ldots, x_{p+m})$=$(x_{1+m+k}, \ldots, x_{p+m+k})$=(k+m).$(x_1, \ldots, x_p)$).
Comme de plus 0.$(x_1, \ldots, x_n)$=$(x_1, \ldots, x_p)$, on a bien défini une opération de $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble X.
3)Puisque toutes les composantes de e sont égales, e est fixé par tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ et par conséquent, son orbite est réduite à lui-même.
4)Puisque l'orbite de x est réduite à $\{x\}$, on a, pour tout élément k de $\mathbb{Z}/p\mathbb{Z}$, k.x=x.
D'où, $x_{1+k} = x_1$ pour tout entier k compris entre 1 et p-1 et donc $x_1 = x_2 = \ldots = x_p$.
On en déduit que ${x_1}^p = x_1 \ldots x_p$=1 car x appartient à X.
L'ordre o(x_1) de x_1 divise le nombre premier p donc o(x_1)=1 ou o(x_1)=p.
Mais x_1 est différent de 1, car x=$(x_1, \ldots, x_p)$ est différent de e, donc o(x_1) n'est pas égal à 1. D'où, x_1 est un élément d'ordre p de G.
5)Puisque $\mathbb{Z}/p\mathbb{Z}$ opère sur X, le cardinal de l'orbite Ω_x de x divise l'ordre du groupe $\mathbb{Z}/p\mathbb{Z}$ (Proposition 4.1.10) c'est à dire p. p étant premier, le cardinal de Ω_x est soit 1 soit p. Mais Ω_x n'est pas réduite à un élément donc est de cardinal strictement supérieur à 1.
Par conséquent, le cardinal de Ω_x est égal à p.
6)Puisque les orbites de X forment une partition de X, on a Card X=$\sum_{x \in X}$ Card Ω_x.
Puisqu'il n'y a qu'une seule orbite de cardinal 1, les autres orbites étant de cardinal p, Card X=1+mp où m est le nombre de représentants des orbites non réduites à un élément.

7)L'ordre de G est divisible par p donc, d'après la question 1, le cardinal de X est congru à 0 modulo p.
Or si e est le seul élément de X dont l'orbite est réduite à un élément, le cardinal de X est congru à 1 modulo p. Contradiction.
Il existe donc un élément x de X différent de e dont l'orbite est réduite à un élément.
On en déduit, d'après la question 3, que G possède un élément d'ordre p.

Exercice 7 : Puisque H est inclus dans N_G(H), il suffit de montrer que N_G(H) est inclus dans H.
P est inclus dans N_G(P) lui-même inclus dans H donc P est un p-sous-groupe de Sylow de H.
Soit n un élément de N_G(H). Comme P est inclus dans H, nPn^{-1} est inclus dans H.
Puisque nPn^{-1} a le même ordre que P (car (p$\rightarrow$npn^{-1}) est une bijection de P vers nPn^{-1}), nPn^{-1} est un p-sous-groupe de Sylow de H.
D'où, d'après le Second Théorème de Sylow, il existe un élément h de H tel que h(nPn^{-1})h^{-1}=P. c'est à dire hn appartient à N_G(P).
Puisque N_G(P) est inclus dans H, il existe un élément h' de H tel que hn=h' c'est à dire n=h^{-1}h'. N_G(H) est donc inclus dans H et N_G(H)=H.

Exercice 8 : Puisque NN_G(P) est inclus dans G, il suffit de montrer que G est inclus dans NN_G(P). Soit g un élément de G.
Puisque P est inclus dans N et N est normal dans G, le sous-groupe gPg^{-1} est inclus dans N. Comme de plus, gPg^{-1} a le même ordre que P (car (h$\rightarrow$ghg^{-1} est une bijection de P vers gPg^{-1}), gPg^{-1} est un p-sous-groupe de Sylow de N.
D'où, d'après le Second Théorème de Sylow, il existe un élément n de N tel que n(gPg^{-1})n^{-1}=P. D'où, ng appartient à N_G(G). On en déduit que g appartient à n$^{-1}N_G$(P)$\subset$NN_G(P). G est inclus dans NN_G(P) et donc G=NN_G(P).

Exercice 9 : On suppose p>q>r. On note n_p (respectivement n_q, n_r) le nombre de p (respectivement q, r) sous-groupes de Sylow de G.
Puisque p, q et r sont premiers entre eux, l'intersection d'un p-sous-groupe de Sylow avec un q-sous-groupe de Sylow est réduite à {1} tout comme l'intersection d'un p-sous-groupe de Sylow avec un r-sous-groupe de Sylow et l'intersection d'un q-sous-groupe de Sylow avec un r-sous-groupe de Sylow.
D'où, l'ensemble des p, q, r-sous-groupes de Sylow de G contient
N=n_p(p-1)+n_q(q-1)+n_r(r-1)+1 éléments de G.
Supposons n_p>1, n_q>1 et n_r>1.
D'après le Second Théorème de Sylow, $n_p \in$ {q, r, qr} et n_p est congru à 1 modulo p.
Or p>q>r donc n_p=qr et qr est congru à 1 modulo p.
$n_q \in$ {p, r, pr} et n_q est congru à 1 modulo q. Puisque q>r, $n_q \in$ {p, pr} et n_q>p.
$n_r \in$ {p, q, pq} donc, comme p>q, n_r>q.
D'où, N>qr(p-1)+p(q-1)+q(r-1)+1=pqr+p(q-1)-(q-1)=pqr+(p-1)(q-1).
Puisque p>1 et q>1, on a (p-1)(q-1)>0 et donc N>pqr.
Or G est d'ordre pqr donc N$\leq$pqr. Contradiction.
D'où, au moins un des trois nombres n_p, n_q ou n_r est égal à 1.

Prenons, par exemple, n_p=1. G possède ainsi un unique p-sous-groupe de Sylow P. P est normal dans G d'après la Proposition 4.5.10. De plus, P est un sous-groupe propre de G car de cardinal 1<p<pqr.
G n'est donc pas simple.

Exercice 10 : $300=2.3.5^2$. D'après le Second Théorème de Sylow, G opère par conjugaison sur l'ensemble S_5(G) des 5-sous-groupes de Sylow de G.
Il existe donc un homomorphisme φ de G vers $S_{S_5(G)}$ défini par φ_g(P)=gPg^{-1} pour tout élément g de G et pour tout élément P de S_5(G).
D'après le Second Théorème de Sylow, n_5(G)$\in \{1, 6\}$.
Si n_5(G)=1 alors G contient un unique 5-sous-groupe de Sylow P.
P est normal dans G et P est un sous-groupe propre de G car de cardinal 25.
G n'est donc pas simple.
Supposons que n_5(G)=6.
S_{S_5}(G) est alors d'ordre 6 !=720 (Proposition 4.1.1).
φ étant un homomorphisme, Ker φ est un sous-groupe normal de G.
Si Ker φ est réduit à {1} alors G/Ker φ est isomorphe à G. Mais par le Premier Théorème d'isomorphisme, G/Ker φ est isomorphe à Im φ donc G est isomorphe à un sous-groupe de Im φ.
Im φ étant un sous-groupe de $S_{S_5(G)}$, son ordre divise l'ordre de $S_{S_5(G)}$ c'est à dire 720. D'où, l'ordre de G divise 720. Mais G est d'ordre 300. Contradiction.
D'où, Ker φ n'est pas réduit à {1}.
Si Ker φ=G alors, pour tout élément g de G, φ(g)=Id donc pour tout élément P de S_5(G), gPg^{-1}=P.
Soient P et Q deux 5-sous-groupes de Sylow. Il existe un élément g de G tel que Q=gPg^{-1} donc Q=P.
D'où, S_5(G) réduit à un élément et n_5(G)=1. Contradiction.
Ker φ est donc différent de G.
Ker φ est un sous-groupe normal propre de G et G n'est par conséquent pas simple.

7.5 Correction des exercices du Chapitre 5

Exercice 1 : Puisqu'un k-cycle $(i_1 \ ... \ i_k)$ est stable par permutation circulaire c'est à dire $(i_1 \ ... \ i_k)=(i_k \ i_1 \ ... \ i_{k-1})= \ ... \ =(i_2 \ ... \ i_k \ i_1)$ (par définition des cycles), k éléments distincts de {1, ... , n} déterminent $\frac{k!}{k}$=(k-1) ! k-cycles.
Commençons par S_4 : il y a l'identité, les transpositions, les 3-cycles, les 4-cycles et les 2×2-cycles.
Nombre de transpositions : $\begin{pmatrix} 4 \\ 2 \end{pmatrix}$=6 : choix de deux éléments de {1, 2, 3, 4}.
Nombre de 3-cycles : $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$ ×2 !=8 : choix de trois éléments de {1, 2, 3, 4} puis nombre de 3-cycles formés avec ces trois éléments.
Nombre de 4-cycles : 3 !=6.
Nombre de 2×2-cycles : $\begin{pmatrix} 4 \\ 2 \end{pmatrix}$/2=3 : on regroupe les paires d'éléments distincts de {1, 2, 3, 4} par 2.
On a bien les 1+6+8+6+3=24 éléments de S_4.
Pour S_5 : on a l'identité, les transpositions, les 3-cycles, les 4-cycles, les 5-cycles, les 2×2-cycles et les 2×3-cycles.
Nombre de transpositions : $\begin{pmatrix} 5 \\ 2 \end{pmatrix}$=10.
Nombre de 3-cycles : $\begin{pmatrix} 5 \\ 3 \end{pmatrix}$ ×2 !=20.
Nombre de 4-cycles : $\begin{pmatrix} 5 \\ 4 \end{pmatrix}$ ×3 !=30.
Nombre de 5-cycles : 4 !=24.
Nombre de 2×2-cycles : $\begin{pmatrix} 5 \\ 2 \end{pmatrix} \times \begin{pmatrix} 3 \\ 2 \end{pmatrix}$/2=15 : on choisit deux éléments de {1, ... , 5} pour former la première transposition puis deux autres pour former la seconde transposition. Mais $(i_1 \ i_2)(i_3 \ i_4)=(i_3 \ i_4)(i_1 \ i_2)$ donc les choix $(\{i_1, i_2\}, \{i_3, i_4\})$ et $(\{i_3, i_4\}, \{i_1, i_2\})$ sont les mêmes.
Nombre de 2×3-cycles : $\begin{pmatrix} 5 \\ 2 \end{pmatrix}$ ×2 !=20 : une fois fixés, les deux éléments formant la transposition, les trois autres éléments forment le 3-cycle. Il reste alors à placer ces trois éléments forment 2 ! 3-cycles.
On obtient ainsi les 1+10+20+30+24+15+20=120 éléments de S_5.

Exercice 2 : 1)Posons H=<{(1 2), (1 ... n)}>.
On a $(1 \ ... \ n)^i(1 \ 2)(1 \ ... \ n)^{-i}$=(i+1 i+2) pour tout i compris entre 1 et n-2.
D'où, (i i+1) appartient à H pour tout i compris entre 1 et n-1.
Or ces transpositions engendrent S_n donc H=S_n.
2)Soit H un sous-groupe de S_p contenant une transposition τ=(i j) et un p-cycle σ.
Soit φ définie par φ(i)=1, φ(j)=2 et φ bijective de vers {3, ... , p} {1, ... , p}\{i, j} (ce qui est possible car ces deux ensembles ont le même cardinal).
Alors, φ appartient à S_p et $\varphi\tau\varphi^{-1}$=(1 2).

Si $\varphi H\varphi^{-1}=S_p$ alors $H=\varphi^{-1}S_p\varphi=S_p$ donc, quitte à remplacer H par $\varphi H\varphi^{-1}$ sous-groupe de S_p, on peut supposer que H contient (1 2).
Puisque σ est un p-cycle, 1 appartient au support de σ. Posons $\sigma=(1\ i_2\ ...\ i_p)$.
σ étant un p-cycle, 2 appartient au support de σ et il existe donc k compris entre 2 et p tel que $i_k=2$. σ étant d'ordre p, $\sigma^{p(k-1)}=Id$ donc l'ordre de σ^{k-1} divise p.
p étant premier et σ^{k-1} étant différent de l'identité (puisque $\sigma^{k-1}(1)=2$), σ^{k-1} est d'ordre p.
Puisque les seuls éléments de S_p d'ordre p sont les p-cycles, σ^{k-1} est un p-cycle.
D'où, quitte à remplacer σ par le p-cycle σ^{k-1}, élément de H, on peut supposer que $\sigma(1)=2$.
Définissons ψ par $\psi(1)=1$, $\psi(2)=2$ et $\psi(i_s)=s$ pour tout s compris entre 3 et p.
Alors, ψ appartient à S_p, $\psi(1\ 2)=(1\ 2)$ et $\psi\sigma\psi^{-1}=(1\ 2\ ...\ p)$.
Par conséquent, $\psi H\psi^{-1}$, sous-groupe de S_p, contient le sous-groupe engendré par (1 2) et (1 ... n). D'où, d'après la question 1, $\psi H\psi^{-1}=S_p$ et donc $H=\psi S_p\psi^{-1}=S_p$.

Exercice 3 : A)1)Posons $\tau=(a\ b)$ avec $a<b$. Soient $1\leq i<j\leq n$.
Si $i\neq a$ et $j\neq b$ alors $\frac{\tau(i)-\tau(j)}{i-j}=\frac{i-j}{i-j}=1$.
Si $i=a$ et $j\neq b$ alors $\frac{\tau(i)-\tau(j)}{i-j}\frac{\tau(j)-\tau(b)}{j-b}=\frac{\tau(i)-\tau(j)}{i-j}\frac{\tau(b)-\tau(j)}{b-j}=\frac{b-j}{i-j}\frac{i-j}{b-j}=1$.
Si $i\neq a$ et $j=b$ alors $\frac{\tau(i)-\tau(j)}{i-j}\frac{\tau(i)-\tau(a)}{i-a}=\frac{\tau(i)-\tau(j)}{i-j}\frac{\tau(a)-\tau(i)}{a-i}=\frac{i-a}{i-j}\frac{j-i}{a-i}=1$.
Si $i=a$ et $j=b$ alors $\frac{\tau(i)-\tau(j)}{i-j}=\frac{j-i}{i-j}=-1$.
D'où, $\epsilon(\tau)=\prod_{i<j}\frac{\tau(i)-\tau(j)}{i-j}=-1$.
2)$\epsilon(\sigma\psi)=\prod_{i<j}\frac{\sigma(\psi(i))-\sigma(\psi(j))}{i-j}=\prod_{i<j}\frac{\sigma(\psi(i))-\sigma(\psi(j))}{\psi(i)-\psi(j)}\frac{\psi(i)-\psi(j)}{i-j}=(\prod_{i<j}\frac{\sigma(\psi(i))-\sigma(\psi(j))}{\psi(i)-\psi(j)})\epsilon(\psi)$.
ψ étant une bijection, $\prod_{i<j}\frac{\sigma(\psi(i))-\sigma(\psi(j))}{\psi(i)-\psi(j)}=\prod_{i<j}\frac{\sigma(i)-\sigma(j)}{i-j}=\epsilon(\sigma)$.
D'où, $\epsilon(\sigma\psi)=\epsilon(\sigma)\epsilon(\psi)$.
3)Soit σ appartenant à S_n. Puisque S_n est engendré par les transpositions, σ se décompose en un produit τ_1 ... τ_k de transpositions.
D'après les deux questions précédentes, $\epsilon(\sigma)=(-1)^k$.
sgn étant un homomorphisme et la signature d'une transposition étant -1,
$\mathrm{sgn}(\sigma)=-(-1)^k=\epsilon(\sigma)$. D'où, $\epsilon=\mathrm{sgn}$.
B)1)Le 2×3-cycle (1 3)(2 6 4) est la permutation de S_6 définie pour $\begin{pmatrix}1&2&3&4&5&6\\3&6&1&2&5&4\end{pmatrix}$.
On a donc les inversions (1,3), (1,4), (2,3), (2,4), (2,5), (2,6) et (5,6).
2)Une transposition (i j), i<j, permute la place des éléments i et j dans la ligne 1 2 ... n. On a donc les inversions (i,i+1), ... , (i,j-1), (i,j), (i+1,j), ... , (j-1,j).
On a ainsi j-i-1+j-i=2j-2i-1 inversions.
Comme 2j-2i-1 est impair quels que soient i et j, $\eta(\tau)=-1$ pour toute transposition τ.
3)Soit σ un élément de S_n. Soient $1\leq i<j\leq n$.
(i,j) est une inversion pour σ si et seulement si $\frac{\sigma(i)-\sigma(j)}{i-j}<0$ donc $\epsilon(\sigma)=1$ si et seulement si σ présente un nombre pair d'inversions.
D'où, $\epsilon(\sigma)=(-1)^{\iota_\sigma}=\eta(\sigma)$. $\eta=\epsilon$.

Exercice 4 : 1)On a vu que les conjugués d'un $k_1\times$ ... $\times k_r$-cycle sont des $k_1\times$ ... $\times k_r$-cycles.
On a vu également que la classe de conjugaison d'un 3-cycle est l'ensemble des 3-cycles.
Comme (1 2 3)(1 2)(3 4)(1 3 2)=(1 4)(2 3) et
(2 3 4)(1 2)(3 4)(2 4 3)=(1 3)(2 4), La classe de conjugaison d'un 2×2-cycle est l'ensemble des 2×2-cycles.
Il reste le cas des 5-cycles.
On sait que la classe de congugaison d'un 5-cycle dans S_5 est l'ensemble des 5-cycles et est donc de cardinal 4 !=24.
D'où, le centralisateur de (1 2 3 4 5) dans S_5 est de cardinal $\frac{120}{24}$=5 (la classe de conjugaison de (1 2 3 4 5) dans S_5 est en bijection avec l'ensemble quotient (à gauche) $S_5/C_{S_5}((1\ 2\ 3\ 4\ 5))$).
$C_{A_5}((1\ 2\ 3\ 4\ 5))$ est un sous-groupe de $C_{S_5}((1\ 2\ 3\ 4\ 5))$ non réduit à l'élément neutre car (1 2 3 4 5) appartient à $C_{A_5}((1\ 2\ 3\ 4\ 5))$.
D'où, $C_{A_5}((1\ 2\ 3\ 4\ 5))$ est de cardinal 5 d'après le Théorème de Lagrange.
On obtient ainsi que la classe de conjugaison de (1 2 3 4 5) dans A_5 est de cardinal $\frac{60}{5}$=12.
Puisqu'il y a 24 5-cycles dans A_5, la classe de conjugaison de (1 2 3 4 5) n'est pas l'ensemble des 5-cycles.
Le raisonnement fait ci-dessous étant valable quel que soit le 5-cycle, on constate qu'il y a deux classes de conjugaison composée de 5-cycles, chacune étant de cardinal 12 (les classes de conjugaison forment une partition de A_5).
Les seules partitions σ telles que $\sigma(1\ 2\ 3\ 4\ 5)\sigma^{-1}$=(1 3 5 2 4) étant des 4-cycles, éléments n'appartenant pas à A_5, on obtient la classe de conjugaison de (1 2 3 4 5) d'une part et la classe de (1 3 5 2 4)=$(1\ 2\ 3\ 4\ 5)^2$ d'autre part.
2)Soit N un sous-groupe normal de A_5 différent de {Id}.
D'après le Théorème de Lagrange, l'ordre de N divise l'ordre de A_5 c'est à dire 60.
Si N contient un 3-cycle alors N contient l'ensemble des 3-cycles d'après la question 1. D'où, puisque A_5 est engendré par les 3-cycles, N=A_5.
Supposons que A_5 ne contient aucun 3-cycle.
Si N contient un 2×2-cycle alors N contient l'ensemble des 2×2-cycles d'après la question 1. D'où, N est de cardinal supérieur ou égal à 1+15=16.
Puisque 16 ne divise pas 60, N contient au moins un 5-cycle.
D'après la question 1, N contient alors 1 ou 2 ensembles de cardinal 12 et donc l'ordre de N est soit 28 soit 40. Or ni 28 ni 40 ne divisent 60 donc on une contradiction.
Il reste le cas où N n'est composé que de l'identité et de 5-cycles.
D'après la question 1, N est d'ordre 13 ou 25. Puisque ni 13 ni 25 ne divisent 60, ce cas est impossible.
D'où, les seuls sous-groupes normaux de A_5 sont {Id} et A_5 et A_5 est donc un groupe simple.

Exercice 5 : 1)S_n et A_n opèrent sur {1, ... , n} via l'opération σ.i =σ(i).
Soient (i_1, ... ,i_{n-2}) et (j_1, ... ,j_{n-2}) deux (n-2)-uplets d'éléments distincts de {1, ... , n}.
Définissons σ par $\sigma(i_k)=j_k$ pour tout k compris entre 1 et n-2 et σ bijective de {1, ... , n}\({i_1, ... , i_{n-2}} vers {1, ... , n}\({j_1, ... , j_{n-2}} ce qui est possible car ces deux ensembles sont de cardinal 2. Alors, σ appartient à S_n.
Si σ appartient à A_n alors on a fini.
Si σ n'appartient pas à A_n alors si pose {s, t}={1, ... , n}\({j_1, ... , j_{n-2}} et τ=(s t), $\tau\sigma$ appartient à A_n et $\tau\sigma(i_k)=j_k$ pour tout k compris entre 1 et n-2.
D'où, A_n opère (n-2)-transitivement sur {1, ... , n}.
La seule permutation envoyant le (n-1)-uplet (1,2, ... ,n-1) sur le (n-1)-uplet (1,2, ... ,n-2,n) est la transposition (n-1 n) qui n'appartient pas à A_n donc A_n n'est pas (n-1)-transitif sur {1, ... , n}.
2)Puisque n$\geq$5, on a n-2$\geq$3.
Supposons que A_n possède un sous-groupe vérifiant la condition donnée.
D'après les résultats de l'Exercice 4 du Chapitre 4 :
Si n=5 alors n=3 ou est une puissance non nulle de 2. Contradiction.
Si n=6 alors n=4. Contradiction.
Si n$\geq$7, A_n ne peut opérer n-2 fois transitivement sur {1, ... , n}. Contradiction.
Dans tous les cas, on a une contradiction donc A_n ne possède pas de sous-groupe vérifiant la condition demandée.
3)Soit σ appartenant à Fix_{A_n}(n). Posons $\alpha=\sigma_{|\{1,\dots,n-1\}}$.
Puisque σ appartient à S_n et σ(n)=n, α appartient à S_{n-1}.
Puisque σ(n)=n, les α-orbites sont les σ-orbites différentes de {n}.
Le nombre m_α de α-orbites est donc égal à n_σ-1 où n_σ est le nombre de σ-orbites et par conséquent, sgn(α)=$(-1)^{n-1-m_\alpha}$=$(-1)^{n-n_\sigma}$=sgn(σ).
D'où, puisque σ appartient à A_n, α appartient à A_{n-1}.
Si α=Id alors σ=Id car σ(n)=n.
Soit ψ est un élément de A_{n-1}. En posant φ(i)=ψ(i) pour i compris entre 1 et n-1 et φ(n)=n, on définit un élément de S_n.
Les φ-orbites différentes de {n} sont les ψ-orbites donc $n_\varphi=m_\psi+1$ et sgn(φ)=$(-1)^{n-n_\varphi}$=$(-1)^{n-1-m_\psi}$=sgn(ψ).
D'où, puisque ψ appartient à A_{n-1}, φ appartient à A_n.
Considérons l'application f de Fix_{A_n}(n) dans A_{n-1} qui à σ associe sa restriction à {1, ... , n-1}. D'après ce qui précède, f est une bijection.
Il reste à montrer que f est un homomorphisme.
Soient σ et φ deux éléments de Fix_{A_n}(n). Soit i compris entre 1 et n-1.
Comme φ appartient à Fix_{A_n}(n), φ(n)=n donc, puisque φ est injective, f(φ)(i)=φ(i)$\neq$n.
D'où, f($\sigma\varphi$)(i)=σ(φ(i))=f(σ)(f(φ)(i)). f($\sigma\varphi$)=f(σ)f(φ) donc f est un homomorphisme.
f est un isomorphisme de Fix_{A_n}(n) vers A_{n-1}.
4)Procédons par récurrence sur n$\geq$5 :
A_5 est simple d'après l'Exercice précédent.
Supposons que A_n est simple.
D'après la question 3, $\mathrm{Fix}_{A_{n+1}}$(n) est alors un groupe simple (la simplicité est conservée par automorphie).
D'où, d'après l'Exercice 5 du Chapitre 4, A_{n+1} est un groupe simple.
A_n est simple pour tout entier n$\geq$5.

Exercice 6 : On notera $s_i(S_n)$ le nombre de i-sous-groupes de Sylow de S_n.
1)A_3 étant d'ordre 3, A_3 possède un unique 3-sous-groupe de Sylow : A_3.
S_3 est d'ordre 6=2×3.
D'après le Second Théorème de Sylow, $s_2(S_3)\in \{1, 3\}$ et $s_3(S_3)=1$.
Le 3-sous-groupe de Sylow est le sous-groupe <(1 2 3)>={Id, (1 2 3), (1 3 2)}.
Puisque le sous-groupe engendré par une transposition est d'ordre 2, S_3 possède 3-sous-groupes de Sylow : {Id, (1 2)}, {Id, (1 3)} et {Id, (2 3)}.
2)A_4 est d'ordre $12=2^2\times3$.
D'après le Second Théorème de Sylow, $s_2(A_4)\in \{1, 3\}$ et $s_3(A_4)\in \{1, 4\}$.
Le sous-groupe de A_4 engendré par un 3-cycle étant d'ordre 3, A_3 possède 4 3-sous-groupes de Sylow : <(1 2 3)>={Id, (1 2 3), (1 3 2)},
<(1 2 4)>={Id, (1 2 4), (1 4 2)}, <(1 3 4)>={Id, (1 3 4), (1 4 3)} et
<(2 3 4)>={Id, (2 3 4), (2 4 3)}.
L'intersection d'un 2-sous-groupe de Sylow et d'un 3-sous-groupe de Sylow étant réduite à l'élément neutre d'après le Théorème de Lagrange (3 et 4 sont premiers entre eux), les 8 éléments, différents de l'identité, composant les 3-cycles n'appartiennent pas aux 2-sous-groupes de Sylow. D'où, il reste 4 éléments pour former un seul 2-sous-groupe de Sylow. Ce 2-sous-groupe de Sylow est normal dans A_4 et est d'ordre 4 donc il s'agit de V_2.
S_4 est d'ordre $24=2^3\times3$.
D'après le Second Théorème de Sylow, $s_2(S_4)\in \{1, 3\}$ et $s_3(S_4)\in \{1, 4\}$.
Comme dans le cas de A_4, $s_3(S_4)=4$ et les 3-sous-groupes Sylow sont <(1 2 3)>,
<(1 2 4)>, <(1 3 4)> et <(2 3 4)>.
Le sous-groupe de S_4 engendré par un 4-cycle étant d'ordre 4, S_4 possède 3 2-sous-groupes de Sylow : <(1 2 3 4)>={Id, (1 2 3 4), (1 3)(2 4), (1 4 3 2)},
<(1 2 4 3)>={Id, (1 2 4 3), (1 4)(2 3), (1 3 4 2)} et
<(1 3 2 4)>={Id, (1 3 2 4), (1 2)(3 4), (1 4 2 3)}.
3)A_5 est d'ordre $60=2^2\times3\times5$.
D'après le Second Théorème de Sylow, $s_2(A_5)\in \{1, 3, 5, 15\}$, $s_3(A_5)\in \{1, 4, 10\}$ et $s_5(A_5)\in \{1, 6\}$.
Puisque A_5 est un groupe simple, $s_i(A_5)\neq1$ pour i=2, 3, 5.
D'où, $s_5(A_5)=6$. Les 5-sous-groupes de Sylow sont les sous-groupes engendrés par les 5-cycles : <(1 2 3 4 5)>, <(1 2 3 5 4)>, <(1 2 5 4 3)>, <(1 5 3 4 2)>, <(1 2 4 3 5)> et <(1 3 2 4 5)>.
Le sous-groupe engendré par un 3-cycle est d'ordre 3 dans A_5 donc A_5 possède 10 3-sous-groupes de Sylow : <(1 2 3)>, <(1 2 4)>, <(1 2 5)>, <(1 3 4)>, <(1 3 5)>, <(1 4 5)>, <(2 3 4)>, <(2 3 5)>, <(2 4 5)>, <(3 4 5)>.
Il reste à déterminer $n_2(A_5)\in \{3, 5, 15\}$.
Si a, b, c et d sont quatre éléments distincts de {1, ... , 5} alors
<{(a b)(c d), (a c)(b d)}>={Id, (a b)(c d), (a c)(b d), (a d)(b c)}.
On a donc trouvé des 2-sous-groupes de Sylow.
Déterminons le nombre de 2-sous-groupes de Sylow de cette forme : on choisit deux éléments a et b puis dans les trois éléments restants, on en choisit deux pour former (c d). Puisque (a b)(c d)=(c d)(a b), on divise le résultat par 2 soit $\begin{pmatrix} 5 \\ 2 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}/2=15$ 2-sous-groupes de Sylow de la forme <{(a b)(c d), (a c)(b d)}>.

Puisque $s_2(A_5)\leq 15$, A_5 possède 15 2-sous-groupe de Sylow, chacun de ces sous-groupes étant de la forme $<\{$(a b)(c d), (a c)(b d)$\}>$.
S_5 est d'ordre $60=2^3\times 3\times 5$.
D'après le Second Théorème de Sylow, $s_2(S_5)\in \{1, 3, 5, 15\}$, $s_3(S_4)\in \{1, 4, 10, 40\}$ et $s_5(S_5)\in \{1, 6\}$.
Si $s_5(S_5)=1$ alors S_5 possède un 5-sous-groupe de Sylow P normal dans S_5 et de cardinal 5. Or les seuls sous-groupes normaux de S_5 sont $\{Id\}$, A_5 de cardinal 60 et S_5 donc $s_5(S_5)\neq 1$ et par conséquent, $s_5(S_5)=6$.
On connait déjà 10 3-sous-groupes de Sylow : les sous-groupes de S_3 engendrés par un 3-cycle.
Réciproquement, un 3-sous-groupe de Sylow de S_5 est d'ordre 3 donc est cyclique, engendré par un élément d'ordre 3. Les seuls éléments d'ordre 3 de S_5 étant les 3-cycles, S_5 possède 10 3-sous-groupes de Sylow : les sous-groupes de S_5 engendrés par un 3-cycle.
Il reste à déterminer $s_2(S_5)$.
Si a, b, c et d sont quatre éléments distincts de $\{1, \ldots, 5\}$ alors τ=(b d) est d'ordre 2, σ=(a b c d) est d'ordre 4 et $\tau\sigma\tau\sigma$=(a d c b)(a b c d)=Id.
D'où, $<\{\tau, \sigma\}>$ est d'ordre 8 et est par conséquent un 2-sous-groupe de Sylow de S_5.
Déterminons le nombre de sous-groupes de ce type.
On a $<\{$(a b c d), (a b)$\}>=\{$Id, (a b c d), (b d), (a c)(b d), (a d c b), (a c), (a b)(c d), (a d)(b c)$\}$ donc le nombre de sous-groupes est égal à la moitié du nombre de 4-cycles soit $\begin{pmatrix} 5 \\ 4 \end{pmatrix}\times 3\,!/2=15$ sous-groupes (cf Exercice 1).
Puisque $s_2(S_5)\leq 15$, S_5 possède 15 2-sous-groupe de Sylow, chacun de ces sous-groupes étant de la forme $<\{$(a b c d), (b d)$\}>$.
Résumons les résultats de cet exercice dans le tableau suivant :

	s_2	2-Sylow	s_3	3-Sylow	s_5	5-Sylow
A_3	0		1	A_3	0	
S_3	1	$<$(1 2)$>$	1	$<$(1 2 3)$>$	0	
A_4	1	V_2	4	$<$3-cycle$>$	0	
S_4	3	$<$4-cycle$>$	4	$<$3-cycle$>$	0	
A_5	15	$<\{$(a b)(c d), (a c)(b d)$\}>$	10	$<$3-cycle$>$	6	$<$5-cycle$>$
S_5	15	$<\{$(a b c d), (b d)$\}>$	10	$<$3-cycle$>$	6	$<$5-cycle$>$

Exercice 7 : 1)a)$\tau_i\tau_j$=(1 j i)$\neq$(1 i j)=$\tau_j\tau_i$ donc, puisque f est injective, f($\tau_i\tau_j$)$\neq$f($\tau_j\tau_i$) c'est à dire, f étant un homomorphisme, f(τ_i)f(τ_j)=f(τ_j)f(τ_i).
Si $\{a_i, b_i\}\cap\{a_j, b_j\}=\emptyset$ alors f(τ_i) et f(τ_j) commutent. Contradiction.
D'où, $\{a_i, b_i\}\cap\{a_j, b_j\}\neq\emptyset$.
b)Soit i compris entre 4 et n. Supposons que $a_2\notin\{a_i, b_i\}$.
Alors, d'après la question précédente appliquée à j=2 et j=3, $\{a_i, b_i\}=\{b_2, b_3\}$.
On en déduit que f($\tau_2\tau_3\tau_i$)=f(τ_2)f(τ_3)f(τ_i)=(a_2 b_3)=f(τ_3) et donc, f étant injective, $\tau_2\tau_3\tau_i=\tau_3$. Or $\tau_2\tau_3\tau_i$=(1 i 3 2)$\neq$(1 3)=τ_3. Contradiction.
D'où, $a_2\in\{a_i, b_i\}$ pour tout i compris entre 3 et n.
c)Quitte à échanger les a_i et les b_i, on peut supposer que $a_i=a_2$ pour tout i compris entre 2 et n.
Considérons l'application σ de $\{1, \ldots, n\}$ dans $\{1, \ldots, n\}$ définie par σ(i)=b_i où on pose b_1=a_2.

Puisque f est un automorphisme, $b_i \neq b_j$ si i est différent de j donc σ appartient à S_n.
De plus, pour tout i compris entre 2 et n, f(τ_i)=(a_2 b_i)=$\sigma\tau_i\sigma^{-1}$.
Soit ψ appartenant à S_n. Les τ_i engendrant S_n, on peut écrire $\psi = \tau_{i_1}$ ... τ_{i_k}.
On a alors, f étant un homomorphisme, f(ψ)=f(τ_{i_1}) ... f(τ_{i_k}).
D'où, f(ψ)=$\sigma\tau_{i_1}\sigma^{-1}$ ... $\sigma\tau_{i_k}\sigma^{-1} = \sigma\psi\sigma^{-1}$. f est un automorphisme intérieur.
2){1, ... , n-2} et {1, ... , n}\{a, b} étant de cardinal n-2, il existe une bijection s entre ces deux ensembles.
Soit σ appartenant à $C_{S_n}(\tau)$.
On définit $\theta(\sigma)$ de {1, ... , n-2} dans {1, ... , n-2} par $\theta(\sigma)$(i)=$s^{-1}\sigma$s(i).
Puisque s et σ sont bijectives, $\theta(\sigma)$ appartient à S_{n-2}.
Montrons que l'application θ est un homomorphisme : soient σ et ψ appartenant à $C_{S_n}(\tau)$ et soit i compris entre 1 et n-2.
$\theta(\sigma\psi)$(i)=$s^{-1}\sigma\psi$s(i)=($s^{-1}\sigma$s)($s^{-1}\psi$s)(i)= $\theta(\sigma)\theta(\psi)$(i).
θ est un homomorphisme de $C_{S_n}(\tau)$ vers S_{n-2}.
Montrons que θ est surjective : soit φ appartenant à S_{n-2}.
Définissons σ de {1, ... , n} dans {1, ... , n} par σ(a)=a, σ(b)=b et σ(i)= sφs^{-1}(i) pour i$\in$ {1, ... , n}\{a, b}.
s et φ étant bijectives, σ appartient à S_n. De plus, $\sigma\tau\sigma^{-1}=\tau$ donc σ appartient à $C_{S_n}(\tau)$ et il est clair que $\theta(\sigma)=\varphi$. D'où, θ est surjective.
Déterminons le noyau de θ : soit σ appartenant à $C_{S_n}(\tau)$ tel que $\theta(\sigma)$=Id.
Alors, pour tout i compris entre 1 et n-2, $s^{-1}\sigma$s(i)=i c'est à dire σ(s(i))=s(i). D'où, puisque s est bijective, σ(i)=i pour tout i appartenant à {1, ... , n}\{a, b}.
Il reste à étudier les images de a et b par σ : puisque σ appartient à $C_{S_n}(\tau)$, (σ(a) σ(b))=$\sigma\tau\sigma^{-1}=\tau$=(a b).
Si σ(a)=a alors σ(b)=b et donc σ=Id.
Si σ(a)=b alors σ(b)=a et $\sigma=\tau$.
D'où, Ker σ={Id, τ}.
3)σ se décompose en un produit ψ_1 ... ψ_k de cycles de longueur$\geq$2, de supports deux à deux disjoints. L'ordre de σ est alors le ppcm des longueurs des cycles composant cette décomposition.
Puisque σ est d'ordre 2, les cycles sont tous de longueur 2 et σ se décompose donc en un produit de transpositions de supports deux à deux disjoints.
4)Pour tout i compris entre 1 et k, ψ_i appartient à $C_{S_n}(\sigma)$ puisque les ψ_j commutent deux à deux (supports disjoints).
D'où, N=<{ψ_1, ... , ψ_k}> est inclus dans $C_{S_n}(\sigma)$.
Puisque les ψ_i, 1$\leq$i$\leq$k, sont d'ordre 2 et commutent deux à deux, tout élément de N s'écrit sous la forme $\psi_1^{s_1}$ ... $\psi_k^{s_k}$ où $s_i \in \{0, 1\}$ pour tout i compris entre 1 et k.
D'où, l'ordre de N est égal à 2^k.
Montrons que N est normal dans $C_{S_n}(\sigma)$: soit $\varphi \in C_{S_n}(\sigma)$.
$\varphi\sigma\varphi^{-1}=\varphi\psi_1$ ... $\psi_k\varphi^{-1}$=($\varphi(a_1)$ $\varphi(a_2)$) ... ($\varphi(a_{2k-1})$ $\varphi(a_{2k})$) où on a noté ψ_i=(a_{2i-1} a_{2i}) pour tout i compris entre 1 et k.
Or $\varphi\sigma\varphi^{-1}=\sigma$ donc, par unicité de la décomposition de σ, pour tout i compris entre 1 et k, il existe j compris entre 1 et k tel que ($\varphi(a_{2i-1})$ $\varphi(a_{2i})$)=ψ_j c'est à dire $\varphi\psi_i\varphi^{-1}=\psi_j$.
Puisque tout élément de N s'écrit comme produit de ψ_i, 1$\leq$i$\leq$k, N est normal dans $C_{S_n}(\sigma)$.
5)Soit $\psi \in C_{S_n}(\phi)$. Puisque f est un homomorphisme, f(ϕ)f(ψ)(f(ϕ))$^{-1}$=f($\phi\psi\phi^{-1}$)=f(ψ).
D'où, f(ψ) appartient à C_{S_n}(f(ϕ)).

D'autre part, si f(φ) appartient à C_{S_n}(f(ϕ)) alors f($\varphi\phi\varphi^{-1}$)=f(φ)f(ϕ)(f(φ))$^{-1}$=f(ϕ) donc, f étant injective, $\varphi\phi\varphi^{-1}=\phi$ et par conséquent, φ appartient à $C_{S_n}(\phi)$.
f étant un automorphisme, l'application de $C_{S_n}(\phi)$ dans C_{S_n}(f(ϕ)) qui à ψ associe f(ψ) est un isomorphisme.
6)Si n$\geq$3, n$\neq$4, alors les seuls sous-groupes normaux de S_n sont {Id}, A_n et S_n.
3 divise l'ordre de A_n et de S_n donc S_n ne possède pas de sous-groupe normal d'ordre 2^m, m$\in \mathbb{N}^*$.
Pour n=4, la propriété n'est plus vraie car V_2 est un sous-groupe normal d'ordre 4 de S_4.
7)Int(S_n) étant inclus dans Aut(S_n), il reste à montrer que Aut(S_n) est inclus dans Int(S_n). Soit f un automorphisme de S_n.
D'après la question 1, il suffit de montrer que f transforme toute transposition en une transposition. Soit τ une transposition. On pose σ=f(τ).
Puisque f est un homomorphisme, (f(τ))^2=f(τ^2)=f(Id)=Id.
D'où, l'ordre de σ divise 2.
σ est différent de l'identité puisque f est un homomorphisme injectif.
D'où, σ est un élément d'ordre 2 de S_n.
D'après la question 4, $C_{S_n}(\sigma)$ possède un sous-groupe normal N d'ordre 2^k où k est le nombre de transpsotions de supports deux à deux disjoints composant σ (question 3). D'après la question 5, $C_{S_n}(\sigma)$ et $C_{S_n}(\tau)$ sont isomorphes par un isomorphisme g.
On vérifie facilement que H=g(N) est un sous-groupe normal de $C_{S_n}(\tau)$ d'ordre 2^k.
D'après la question 2, il existe un homomorphisme surjectif θ de $C_{S_n}(\tau)$ vers S_{n-2} de noyau {Id, τ}.
Montrons que θ(H) est un sous-groupe normal de S_{n-2} :
Soit ρ appartenant à H et η appartenant à S_{n-2}.
Puisque θ est surjective, il existe μ appartenant à $C_{S_n}(\tau)$ tel que $\eta = \theta(\mu)$.
On a alors $\eta\theta(\rho)\eta^{-1}=\theta(\mu\rho\mu^{-1})\in \theta$(H) puisque θ est un homomorphisme et H est normal dans $C_{S_n}(\tau)$. D'où, θ(H) est un sous-groupe normal de S_{n-2}.
$\theta_{|H}$ est un homorphisme de H vers θ(H) de noyau {Id} ou {Id, τ} selon que τ appartient à H on non. D'après le Premier Théorème d'isomorphisme, θ(H) est isomorphe à H/Ker $\theta_{|H}$ donc θ(H) est un sous-groupe normal d'ordre 2^k ou 2^{k-1} de S_{n-2}.
Si σ n'est pas une transposition alors k$>$1. On aboutit alors à une contradiction d'après la question 6. D'où, σ est une transposition.
f transforme toute transposition en une transposition donc, d'après la question 1, f est un automorphisme intérieur. Aut(S_n)=Int(S_n).
8)D'après le Premier Théorème d'isomorphisme, Int(S_n) est isomorphe à S_n/Z(S_n). Or Z(S_n)=Id, pour tout n$\geq$3, donc Int(S_n) est isomorphe à S_n. On en déduit d'après la question précédente, que Aut(S_n) est isomorphe à S_n lorsque n$\neq$6.

Exercice 8 : 1)S_n opère sur {1, ... , n} via l'opération σ.n=σ(n).
Cette opération est n-transitive car si (i_1, ... ,i_n) et (j_1, ... ,j_n) sont deux n-uplets d'éléments distincts de {1, ... , n} alors, en posant $\sigma(i_k)=j_k$ pour tout k compris entre 1 et n, σ appartient à S_n et envoie (i_1, ... ,i_n) sur (j_1, ... ,j_n).
Il découle de la n-transitivité que S_n opère transitivement sur {1, ... , n}.

2)On reprend le même raisonnement que pour la question 3 de l'Exercice 6, en prenant la restriction d'un élément de S(i) à l'ensemble {1, ... , n}\{i} et en utilisant le fait que le groupe des permutations de l'ensemble {1, ... , n}\{i} est isomorphe à S_{n-1}.
3)Soient σ appartenant à S_n et i compris entre 1 et n.
Si ψ appartient à S(i) alors $\sigma\psi\sigma^{-1}(\sigma(i))=\sigma(i)$ et si φ appartient à S(σ(i)) alors $\sigma^{-1}\varphi\sigma(i)=i$ donc $\sigma S(i)\sigma^{-1}=S(\sigma(i))$.
Soient i et j compris entre 1 et n. Puisque S_n opère transitivement sur {1, ... , n}, il existe un élément σ de S_n tel que $\sigma(i)=j$.
D'où, $S(j)=\sigma S(i)\sigma^{-1}$ et S(i) et S(j) sont conjugués.
4)f est définie par $f(\sigma)(\psi H)=\sigma.\psi H=\sigma\psi H$ pour tout couple (σ,ψ) d'éléments de S_n.
Montrons que f est injective : Ker $f=\cap_{\sigma\in S_n}\sigma H\sigma^{-1}$ est un sous-groupe normal de S_n inclus dans H.
Puisque $n\neq 4$, S_n est un groupe simple donc Ker f={1}, Ker f=A_n ou Ker f=$\{S_n\}$.
Mais Ker f est inclus dans H donc $|\text{Ker f}| \leq |H|=(n-1)!<\frac{n!}{2}=|A_n|$.
D'où, Ker f={1} et f est injective.
Puisque $|S_n| = |S_{S_n/H}|$, f est bijective.
f est un isomorphisme de S_n vers $S_{S_n/H}$.
5)Im f opère sur S_n/H via l'opération $f(\sigma).\psi H=f(\sigma)(\psi H)=\sigma\psi H$.
6)Pour tout élément σ appartenant à H, $f(\sigma).H=\sigma H=H$ donc f(H) est inclus dans Stab(H). Soit θ appartenant à Stab(H).
Puisque f est surjective, il existe un élément σ de S_n tel que $\theta=f(\sigma)$.
Puisque $\sigma H=f(\sigma)(H)=\theta.H=H$, σ appartient à H.
D'où, θ appartient à f(H). Stab(H)=f(H).
7)Puisque S_n/H\{H} et {2, ... , n}. ont le même cardinal, il existe une bijection entre S_n/H\{H} et {2, ... , n}.
D'où, il existe une bijection s entre S_n/H et {1, ... , n} telle que s(H)=1.
8)Soit α un élément de $S_{S_n/H}$. On définit ϕ par $\phi=s\circ\alpha\circ s^{-1}$.
s et α étant bijectives, ϕ appartient à S_n.
On peut donc définir une appplication g de $S_{S_n/H}$ dans S_n en posant $g(\alpha)=\phi$.
Pour tout couple (α,β) d'éléments de $S_{S_n/H}$,
$g(\alpha\circ\beta)=s\circ\alpha\circ\beta\circ s^{-1}=s\circ\alpha\circ s^{-1}\circ s\circ\beta\circ s^{-1}=g(\alpha)\circ g(\beta)$ donc g est un homomorphisme.
Montrons que g est injective : soit α un élément de $S_{S_n/H}$ tel que $g(\alpha)=Id$.
On a alors $s\circ\alpha\circ s^{-1}=Id$ donc $\alpha(s^{-1}(i))=s^{-1}(i)$ pour tout élément i de {1, ... , n}.
Puisque s est surjective, $\alpha(i)=i$ pour tout élément i de {1, ... , n}.
α=Id et g est donc injective.
Puisque $S_{S_n/H}$ et S_n ont le même cardinal, g est bijective.
g est un isomorphisme de $S_{S_n/H}$ vers S_n.
9)Pour tout élément σ de H, $g(f(\sigma))(1)=s\circ f(\sigma)\circ s^{-1}(1)=s(f(\sigma)(H))=s(H)=1$ donc g(f(H)) est inclus dans S(1). Soit ρ appartenant à S(1).
g et f étant surjectives, il existe un élément σ de S_n tel que $g(f(\sigma))=\rho$.
Puisque $s\circ f(\sigma)\circ s^{-1}(1)=g(f(\sigma))(1)=1$, $f(\sigma)(H)=s^{-1}(1)=H$.
D'où, $f(\sigma)$ appartient à Stab(H).
On en déduit, d'après la question 6, que σ appartient à H et par conséquent ρ appartient à g(f(H)). g(f(H))=S(1).
10)g$\circ$f est un automorphisme de S_n donc g$\circ$f est un automorphisme intérieur.
D'où, il existe un élément σ de S_n tel que $g(f(H))=\sigma H\sigma^{-1}$.
D'où, d'après la question précédente, $\sigma H\sigma^{-1}=S(1)$ et H et S(1) sont conjugués.

11)D'après la question 2, S(i) est d'ordre (n-1)! donc d'indice $\frac{n!}{(n-1)!}$=n pour tout i compris entre 1 et n.
Soit K un sous-groupe d'indice n et i compris entre 1 et n.
D'après la question précédente, il existe un élément σ de S_n tel que K=σS(i)σ^{-1}=S(σ(j)).
Les sous-groupes d'indice n de S_n sont les sous-groupes S(i), i$\in$ {1, ... , n}.

Exercice 9 : 1)D'après le Second Théorème de Sylow, S_5 possède 1 ou 6 5-sous-groupes de Sylow. Si S_6 ne possède qu'un seul 5-sous-groupe de Sylow alors celui-ci est normal dans S_5 et est de cardinal 5. Or les seuls sous-groupes normaux de S_5 sont {Id}, A_5 de cardinal 60 et S_5 donc S_5 possède 6 5-sous-groupes de Sylow.
D'après le Second Théorème de Sylow, S_5 opère transitivement (par conjugaison) sur l'ensemble des 5-sous-groupes de Sylow.
L'orbite Ω(P) de P pour cette opération est en bijection avec l'ensemble quotient (à gauche) S_5/H donc Card Ω(P)=[S_5,H]=$\frac{|S_5|}{|H|}$. Puisque l'opération est transitive, Ω(P) est l'ensemble des 5-sous-groupes de Sylow donc Card Ω(P)=6 et |H|=20.
2)L'opération de S_5 sur S_5/H est transitive puisque si σH et ψH sont des éléments de S_5/H alors $\psi\sigma^{-1}$.σH=ψH.
Montrons que l'opération est fidèle : pour cela, montrons que son noyau est réduit à l'identité :
Le noyau $\cap_{\sigma\in S_5}\sigma H\sigma^{-1}$ est un sous-groupe normal de S_5 inclus dans H (H=Id H Id^{-1}).
D'où, d'après la question précédente, $\cap_{\sigma\in S_5}\sigma H\sigma^{-1}$ est un sous-groupe normal de S_5 de cardinal inférieur ou égal à 20.
Puisque les seuls sous-groupes normaux de S_5 sont {Id}, A_5 de cardinal 60 et S_5, le noyau est {Id} et l'opération est fidèle.
S_5 opérant sur S_5/H, il existe un homomorphisme h de S_5 vers $S_{S_5/H}$, ensemble des permutations de S_5/H. L'opération étant fidèle, cet homomorphisme est injectif.
S_5/H étant de cardinal 6, $S_{S_5/H}$ est isomorphe à S_6 (Proposition 4.1.2) via l'isomorphisme α défini par $\alpha(\varphi)$(i)=j où $\varphi(\psi_i H)=\psi_j H$, $\varphi \in S_{S_5/H}$, i, j$\in$ {1, ... , 6}.
En posant f=$\alpha\circ$h, f est un homomorphisme injectif f de S_5 dans S_6.
f est définie, pour $\sigma \in S_5$, par f(σ)(i)=j où h(σ)(ψ_iH)=ψ_jH c'est à dire $\sigma.\psi_i H=\psi_j H$ par définition de h.
3)f étant un homomorphisme, Im f est un sous-groupe de S_6.
D'après le Premier Théorème d'isomorphisme, Im f est isomorphe à S_5/Ker f donc l'ordre de Im f est $\frac{120}{1}$=120. D'où, l'indice de Im f dans S_6 est $\frac{720}{120}$=6.
4)Soient ψ_1H, ... , ψ_6H les 6 éléments de S_5/H.
Im f, en tant que sous-groupe de S_6, opère sur {1, ... , n}. Soient i et j deux éléments de {1, ... , 6}.
Puisque l'opération de S_5 sur S_5/H est transitive, il exsite un élément σ de S_5 tel que $\sigma.\psi_i H=\psi_j H$. Alors, par définition de f, f(σ)(i)=j.
D'où, l'opération de Im f sur {1, ... , n} est transitive.
5)Soit i compris entre 1 et 6.
S(i), en tant que sous-groupe de S_6, opère sur {1, ... , n}.
Mais cette opération n'est pas transitive car si j est différent de i alors il n'existe pas d'élément σ de S(i) tel que σ.i=σ(i)=j puisque σ(i)=i.
Puisque le conjugué d'un S(i) est un stabilisateur S(j) d'après l'Exercice précédent et Im f opère transitivement sur {1, ... , 6}, Im f ne peut être conjugué à un S(i).

6)Si Aut(S_6)=Int(S_6) alors, d'après l'Exercice précédent, les sous-groupes de S_6 d'indice 6 sont conjugués.
D'où, toujours d'après l'Exercice précédent, les sous-groupes de S_6 d'indice 6 sont les S(i), $1 \leq i \leq 6$.
Or d'après les deux questions précédentes, Im f sous-groupe de S_6 d'indice 6, n'est conjugué à aucun S(i), $1 \leq i \leq 6$. Contradiction.
D'où, Aut(S_6)$\neq$Int(S_6).

Exercice 10 : 1)Une isométrie qui conserve un cube C, permute les 8 sommets de ce cube. Ainsi, si on note 1, ... , 8 les sommets du cube, à toute isométrie f conservant le cube, on peut associer l'élément θ(f)=$\begin{pmatrix} 1 & ... & 8 \\ f(1) & ... & f(8) \end{pmatrix}$ de S_8.
θ est clairement un homomorphisme du groupe Is(C) des isométries conservant le cube C vers S_8.
De plus, si θ(f)=Id alors f=Id car f fixe alors 4 points non coplanaires.
D'où, Ker θ={Id} et d'après le Premier Théorème d'isomorphisme Is(C) est isomorphe à Im θ sous-groupe de S_8.
Le groupe G des isométires directes conservant C est lui isomorphe à $\theta_{|G}$(G) sous-groupe de S_8.
2)Soient O le centre du cube, A le centre du carré 1234 et B le centre du carré 1265. σ est la rotation d'axe (OA) et d'angle -$\frac{\pi}{2}$ donc σ appartient à G. ψ est la rotation d'axe (OB) et d'angle $\frac{\pi}{2}$ donc ψ appartient à G.
3)G opère sur {1, ... , 8} via l'opération f.i=f(i) pour tout élément f de G et i de {1, ... , 8}.
4)On a Id(1)=1, $\sigma(1)=2$, $\sigma^2(1)=3$, $\sigma^3(1)=4$, $\psi^3(1)=5$, $\psi^2(1)=6$, $\psi\sigma^2(1)=7$ et $\psi^2\sigma^2(1)=8$ donc l'orbite de 1 est {1, ... , 8}.
5)L'orbite de 1={1, ... , 8} est la seule orbite de {1, ... , 8} pour l'opération de G donc G opère transitivement sur {1, ... , 8}.
6)Soit f appartenant au stabilisateur de 1.
Puisque f est une isométrie, O et 7 sont aussi fixés par f.
Etudions l'image de 2 par f :
Puique f est une isométrie, f(2)$\in$ {2, 4, 5}.
Si f(2)=2 alors , puisque f est une isométrie directe (donc conservant l'orientation des angles), f(3)=3 et f(4)=4. D'où, puisque f est une isométrie, f(5)=5, f(6)=6, f(7)=7 et f(8)=8 c'est à dire f=Id.
Si f(2)=4 alors, f étant une isométrie directe, f(3)=8 et f(4)=5.
D'où, f(5)=2, f(6)=3 et f(8)=6. On obtient ainsi la permutation (2 4 5)(3 8 6) qui représente la rotation d'axe (17) et d'angle -$\frac{2\pi}{3}$ puisqu'il s'agit d'un élément d'ordre 3 de S_8 et l'angle orienté $\widehat{2O4}$ est négatif.
Si f(2)=5 alors, comme f est une isométrie directe, f(3)=6 et f(4)=2.
D'où, f(5)=4, f(6)=8 et f(8)=3. On obtient ainsi la permutation (2 5 4)(3 6 8) qui représente la rotation d'axe (17) et d'angle $\frac{2\pi}{3}$ puisqu'il s'agit de la permutation inverse de la permutation précédente.
Ainsi, G_1 est d'ordre 3.
7)L'orbite de 1 est en bijection evec l'ensemble quotient (à gauche) G/G_1 donc 8=[G :G_1] = $\frac{|G|}{3}$ et |G|=24.

8)Toute isométrie et en particulier toute isométrie directe, conservant le cube permute les diagonales $D_1 = [17]$, $D_2 = [28]$, $D_3 = [35]$ et $D_4 = [46]$.
Ainsi à un élément f de Is(C), on peut associer la permutation ϕ(f)=$\begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}$ où, pour j compris entre 1 et 4, f(D_j)=D_{i_j} (par exemple, la rotation d'axe (17) et d'angle $\frac{2\pi}{3}$ s'identifie à la permutation (2 3 4)).
On vérifie que ϕ est un homomorphisme de Is(G) vers S_4.
ϕ n'est pas injective puisque si s désigne la symétrie centrale de centre O, ϕ(s)=Id.
Par contre si f est une isométrie directe et si ϕ(f)=Id alors f=Id puisque f conserve les angles. D'où, $\phi_{|G}$ est un homomorphisme injectif et d'après le Premier théorème d'isomorphisme, G est isomorphe à H=Im $\phi_{|G}$, sous-groupe de S_4.
9)H étant isomorphe à G, H est d'ordre 24.
Comme S_4 est d'ordre 24 et H est un sous-groupe de S_4, H=S_4.
G est donc isomorphe à S_4.
10)L'application déterminant de Is(C) dans $\{\pm 1, \times\}$ est un homormorphisme de groupes.
De plus, il s'agit d'un homomorphisme surjectif (det Id=1 et det s=-1 où s désigne la symétrie centrale de centre O) et Ker det=G donc, d'après le Premier Théorème d'isomorphisme, Is(C)/G est isormorphe à $\{\pm 1\}$.
On en déduit que |Is(C)|=48.
Les éléments de Is(C) sont les éléments de G et les éléments de la forme s$\circ$f où f appartient à G.

7.6 Correction des exercices du Chapitre 6

Exercice 1 : On note $A_O = I$, ... , A_{n-1}, les sommets du polygône régulier à n côtés formés à partir des racines n^{ièmes} de l'unité.
D_4 est engendré par l'ensemble constitué de la rotation r de centre O et d'angle $\frac{\pi}{2}$ et de la réflexion d'axe (OI) (droite égale à la droite (A_2A_0)).
Les éléments de D_4 sont Id, r, r^2 : symétrie centrale de centre O, r^3 : rotation de centre O et d'angle -$\frac{\pi}{2}$, s, sr : réflexion d'axe $(A_{\frac{3}{2}}A_{\frac{7}{2}})$ où $A_{\frac{3}{2}}$ (respectivement $A_{\frac{7}{2}}$) désigne le milieu de [A_1,A_2] (respectivement [A_3,A_0]), sr^2 : réflexion d'axe (A_1A_3) et sr^3 : réflexion d'axe $(A_{\frac{1}{2}}A_{\frac{5}{2}})$ où $A_{\frac{1}{2}}$ (respectivement $A_{\frac{5}{2}}$) désigne le milieu de [A_0,A_1] (respectivement [A_2,A_3]).
D_5 est engendré par l'ensemble constitué de la rotation r de centre O et d'angle $\frac{2\pi}{5}$ et de la réflexion d'axe (OI) ((droite égale à la droite $(A_{\frac{5}{2}}A_0)$ où $A_{\frac{5}{2}}$ désigne le milieu de [A_2,A_3]).
Les éléments de D_5 sont Id, r, r^2 : rotation de centre O et d'angle $\frac{4\pi}{5}$, r^3 : rotation de centre O et d'angle -$\frac{4\pi}{5}$, r^4 : rotation de centre O et d'angle -$\frac{2\pi}{5}$, s, sr : réflexion d'axe $(A_2A_{\frac{9}{2}})$ où $A_{\frac{9}{2}}$ désigne le milieu de [A_4,A_0], sr^2 : réflexion d'axe $(A_4A_{\frac{3}{2}})$ où $A_{\frac{3}{2}}$ désigne le milieu de [A_1,A_2], sr^3 : réflexion d'axe $(A_1A_{\frac{7}{2}})$ où $A_{\frac{7}{2}}$ désigne le milieu de [A_3,A_4] et sr^4 : réflexion d'axe $(A_3A_{\frac{1}{2}})$ où $A_{\frac{1}{2}}$ désigne le milieu de [A_0,A_1].

Exercice 2 : On pose D_n=<{a, b / a^2=b^n=1 et abab=1}>.
Les éléments D_n appartiennent à <b> ou sont de la forme ab^k avec k compris entre 0 et n-1.
Soit k compris entre 0 et n-1. (ab^k)^2=ab^{k}ab^k=b^{-k}b^k=1 donc l'ordre de ab^k divise 2.
Puisque ab^k est différent de l'identité (car a n'est pas une puissance de b), ab^k est d'ordre 2 pour tout k compris entre 0 et n-1.
<b> étant d'ordre n les éléments de <b> ont pour ordre un diviseur de n.
Ainsi, l'ordre d'un élément de D_n est soit 2 soit un diviseur de n.
<b> étant cyclique, il y a pour tout diviseur d de n, φ(d) éléments de <b> d'ordre d, où φ désigne l'indicateur d'Euler (cf Cours *Congruence*).
Si n est impair alors <b> ne possède pas d'élément d'ordre 2 donc D_n possède alors n éléments d'ordre 2 et pour tout diviseur d de n, φ(d) éléments d'ordre d.
Si n est pair, il y a φ(2)=1 élément d'ordre 2 dans <b> donc D_n possède n+1 éléments d'ordre 2 et pour tout diviseur d de n distinct de 2, φ(d) éléments d'ordre d.

Exercice 3 : 1)Notons A_1, ... , A_n=I, les sommets du polygône régulier à n côtés formés à partir des racines n^{ièmes} de l'unité.
Soit θ la correspondance, de D_n dans l'ensemble des applications de {1, ... , n} dans lui-même, définie par θ(f) : i$\rightarrow$j où f(A_i)=A_j.
f étant une application, pour tout f$\in D_n$, θ est une application.
f étant bijective, pour tout f$\in D_n$, θ(f) appartient à S_n pour tout élément f de D_n.
Vérifions que θ est un homomorphisme de D_n dans S_n : soient f et g deux éléments de D_n. Soit i compris entre 1 et n.
θ(fg)(i)=j où fg(A_i)=A_j.
θ(f)θ(g)(i)=θ(f)(k) où g(A_i)=A_k donc θ(f)θ(g)(i)=m où f(A_k)=A_m.

Puisque A_k=g(A_i), on a A_m=f(g(A_i))=fg(A_i)=A_j et donc m=j.
D'où, θ(fg)=θ(f)θ(g) et θ est un homomorphisme.
Montrons que θ est injective : soit f$\in D_n$ tel que θ(f)=Id.
On a alors f(A_i)=A_i pour tout i compris entre 1 et n.
f étant une isométrie, f fixe O. f fixe donc O, A_1 et A_2.
Or ces trois points déterminent une base de $\mathbb{R}^2$ ($(\overrightarrow{OA_1, OA_2}) = \frac{2\pi}{n} \neq 0 \mod \pi$) donc f=Id et θ est injective.
2)D'après le Premier Théorème d'isomorphisme, D_n/Ker θ est isomorphe à Im θ sous-groupe de S_n.
Or θ étant injective, Ker $\theta = \{\mathrm{Id}\}$ donc D_n/Ker θ est isomorphe à D_n.
Ainsi, D_n est isomorphe à un sous-groupe de S_n.
3)On utilise les notations de l'Exercice 1 pour D_4.
θ(Id)=Id, θ(r)=(1234),θ(r^2)=(13)(24),
θ(r^3)=(1432), θ(s)=(13), θ(sr)=(12)(34) et θ(sr^3)=(14)(23).
D'où, {Id, (12)(34), (13)(24), (14)(23), (1234), (1432)} =Im θ est un sous-groupe de S_4.

Exercice 4 : 1)Soit k compris entre 1 et n-1.
Pour tout m compris entre 1 et n-1, b^{m}b^{k}b^{-m}=b^k et pour tout r compris entre 0 et n-1, ab^{m}b^{k}b^{-m}a=ab^{k}a=b^{-k}.
D'où, la classe de conjugaison de b^k est {b^k, b^{-k}} si n est impair ou si n est pair et k différent de $\frac{n}{2}$ et la classe de b$^{\frac{n}{2}}$ est {b$^{\frac{n}{2}}$} lorsque n est pair.
Soit k compris entre 0 et n-1.
Pour m compris entre 1 et n-1, b^{m}ab^{k}b^{-m}=ab^{-m}b^{k}b^{-m}=ab^{k-2m} et pour r compris entre 0 et n-1, ab^{m}ab^{k}b^{-m}a=b^{-m}b^{k}b^{-m}a=b^{k-2m}a=ab^{2m-k}.
Supposons n impair.
Pour tout s compris entre 0 et n-1, s et s-n sont de parités différentes.
D'où, il existe m compris entre 0 et n-1 tel que s=k-2m ou s-n=k-2m et donc a^{k-2m}=ab^s.
La classe de conjugaison de ab^k est par conséquent l'ensemble des ab^s, s compris entre 0 et n-1.
Si n est pair et k est pair, b^{k-2m} et b^{2m-k} sont des puissances paires de b quel que soit m compris entre 1 et n-1.
De plus, pour tout s pair compris entre 0 et n-1, il existe m compris entre 0 et n-1 tel que s=k-2m ou s-n=k-2m donc ab^{k-2m}=ab^s.
Si n est pair et k est impair, b^{k-2m} et b^{2m-k} sont des puissances impaires de b quel que soit m compris entre 1 et n-1.
De plus, pour tout s impair compris entre 0 et n-1, il existe m compris entre 0 et n-1 tel que s=k-2m ou s-n=k-2m donc ab^{k-2m}=ab^s.
D'où, lorsque n est pair, on a la classe de conjugaison formée des éléments ab^k avec k pair compris entre 0 et n-1 et la classe de conjugaison formée des éléments ab^k avec k impair compris entre 1 et n-1.
Si n est impair alors D_n possède $\frac{n+3}{2}$ classes de conjugaison : {1}, {b, b^{-1}}, ... , {b$^{\frac{n-1}{2}}$, b$^{-\frac{n-1}{2}}$} et {ab^k / 0≤k≤n-1}.
Si n est pair alors D_n possède $\frac{n+6}{2}$ classes de conjugaison : {1}, {b, b^{-1}}, ... , {b$^{\frac{n-2}{2}}$, b$^{-\frac{n-2}{2}}$}, {b$^{\frac{n}{2}}$}, {ab^{2k} / 0≤k≤ $\frac{n}{2}$} et {ab^{2k+1} / 0≤k≤ $\frac{n}{2} - 1$}.
2)Si x est un élément de D_n alors la classe de conjugaison de x, cl(x), est en bijection

avec l'ensemble quotient D_n/Stab_{D_n}(x).
On a donc $|\mathrm{Stab}_{D_n}(x)|=\frac{2n}{Card\, cl(x)}$.
D'où, $|\mathrm{Stab}_{D_n}(b)|$=n, $|\mathrm{Stab}_{D_n}(a)|$=2 si n est impair et $|\mathrm{Stab}_{D_n}(a)|$=4 si n est pair.
Pour tout k compris entre 0 et n-1, $b^k b b^{-k}$=b donc $\mathrm{Stab}_{D_n}(b)$=<b>.
1 et a appartiennent à Stab_{D_n}(a) donc si n est impair, $\mathrm{Stab}_{D_n}(a)$={1, a}.
Supposons n pair.
On a $b^{\frac{n}{2}}ab^{-\frac{n}{2}}$=$aab^{\frac{n}{2}}ab^{-\frac{n}{2}}$= $ab^{-\frac{n}{2}}b^{-\frac{n}{2}}$=a et $ab^{\frac{n}{2}}a(ab^{-\frac{n}{2}})^{-1}$= $ab^{\frac{n}{2}}ab^{-\frac{n}{2}}a$=$b^{-\frac{n}{2}}b^{-\frac{n}{2}}a$=a donc $b^{\frac{n}{2}}$ et $ab^{\frac{n}{2}}$ appartiennent à Stab_{D_n}(a).
D'où, lorsque n est pair, $\mathrm{Stab}_{D_n}(a)$={1, a, $b^{\frac{n}{2}}$, $ab^{\frac{n}{2}}$}.

Exercice 5 : On pose D_n=<{a, b / o(a)=2, o(b)=n et abab=1}>.
1)D'après le Second Théorème de Sylow, $n_2(D_p)\in$ {1, p} et $n_p(D_p)$=1.
Le p-sous-groupe de Sylow de D_p est <b>.
Pour tout k compris entre 0 et n-1, $(ab^k)^2$=ab^kab^k=$b^{-k}b^k$=1 donc l'ordre de ab^k divise 2. Puisque ab^k est différent de l'identité (car a n'est pas une puissance de b), ab^k est d'ordre 2.
D'où, il y a p sous-groupes de Sylow : les sous-groupes <ab^k> pour k compris entre 0 et n-1.
2)D_4 est d'ordre 8=2^3 donc il y a un unique 2-Sylow : D_4.
3)D_6 est d'ordre 12=$2^2$3.
D'après le Second Théorème de Sylow, $n_2(D_6)\in$ {1, 3} et $n_3(D_6)\in$ {1, 4}.
b^3 est d'ordre 2 puisque b est d'ordre 6.
Soit k compris entre 1 et 3. $(ab^k)^2$=ab^kab^k=$b^{-k}b^k$=1 donc l'ordre de ab^k divise 2. Puisque ab^k est différent de l'identité (car a n'est pas une puissance de b), ab^k est d'ordre 2. De plus, b^3ab^k=aab^3ab^k=ab^3b^k=ab^kb^3.
D'où, <{b^3, ab^k}> est d'ordre 4.
On a ainsi trouvé 3 2-sous-groupes de Sylow.
L'ensemble des éléments de ces 2-sous-groupes de Sylow est de cardinal 8 (1, b^3, ab, b^3ab=ab^4, ab^2, b^3ab^2=ab^5, ab^3 et b^3ab^3=a).
Puisque 3 et 4 sont premiers entre eux, l'intersection d'un 2-sous-groupe de Sylow et d'un 3-sous-groupe de Sylow est réduite à {1}. D'où, il reste 4 éléments pour former les éléments, différents de 1, des 3-sous-groupes de Sylow.
L'intersection de deux 3-sous-groupes de Sylow distincts étant réduite à un élément (d'après le Théorème de Lagrange), il ne peut y avoir qu'un seul 3-sous-groupe de Sylow. Ce 3-sous-groupe de Sylow est <b^2>.

Exercice 6 : 1)Soit f appartenant à Aut(D_n). Soit x$\in$ D_n.
Puisque D_n est engendré par a et b, x s'écrit $a^{m_1}b^{k_1}$ ... $a^{m_s}b^{k_s}$ où pour i compris entre 1 et s, $m_i \in$ {0, 1} et 0$\leq k_i \leq$n-1.
D'où, puisque f est un homomorphisme, f(x)=$f(a)^{m_1}f(b)^{k_1}$ ... $f(a)^{m_s}f(b)^{k_s}$.
Ainsi, f est déterminée pr f(a) et f(b).
2)La vérification est immédiate.
3)Soit f un élément de F_a.
Puisque f est déterminée par f(a) et f(b) et puisque f(a)=a, il suffit de déterminer f(b).
b étant d'ordre n et f étant un homomorphisme, on a $f(b)^n$=f(b^n)=f(1)=1.
D'où, l'ordre de f(b) divise n.

Si m est un entier strictement positif tel que f(b)^m=1 alors f étant un homomorphisme, f(b^m)=1 et comme f est injectif, b^m=1.
D'où, l'ordre de b c'est à dire n divise m. f(b) est donc d'ordre n.
Les éléments de D_n d'ordre n sont les générateurs de <b> (cf Exercice 2) donc il y a φ(n) éléments de D_n d'ordre n (cf Cours *Congruence*).
f(b) peut prendre φ(n) valeurs donc F_a est d'ordre φ(n).
4)Soit f un élément de F_b et g un élément de Aut(D_n).
On a vu à la question précédente que g^{-1}(b) appartient à <b> donc il existe k compris entre 1 et n-1 tel que g^{-1}(b)=b^k.
D'où, gofog^{-1}(b)=g(f(b^k))=g((f(b))^k)=g(b^k)=b et gofog^{-1} appartient donc à F_b.
F_b est un sous-groupe normal de D_n.
5)Un élément de F_b est déterminé par f(a).
En reprenant le raisonnement fait à la question 3, on montre que f(a) est d'ordre 2.
Les éléments de D_n d'ordre 2 sont les éléments ab^k pour k compris entre 0 et n-1 et, si n est pair, l'élément b$^{\frac{n}{2}}$.
Supposons n pair et f(a)=b$^{\frac{n}{2}}$.
Alors pour tout élément x=a^{m_1}b^{k_1} ... a^{m_s}b^{k_s} de D_n, f(x)=f(a)^{m_1}b^{k_1} ... f(a)^{m_s}b^{k_s} $\in$<b>.
D'où, f(D_n) est inclus dans <b> et f n'est donc plus surjective. Contradiction.
Ainsi, f(a) peut prendre n valeurs et donc F_b est d'ordre n.
6)Soit f appartenant à D_n.
Définissons l'élément β de F_b par β(a)=f(a) et définissons l'élément α de F_a par α(b)=β^{-1}(f(b)).
On a f(a)=$\beta\circ\alpha$(a) et f(b)=$\beta\circ\alpha$(b) donc f=$\beta\circ\alpha$ et Aut(D_n) est par conséquent inclus dans F_bF_a. Puisque F_bF_a est inclus dans Aut(D_n), on a Aut(D_n)=F_bF_a.
Remarque : On montre de manière similaire que Aut(D_n)=F_aF_b.
7)Soit f un élément de $F_a \cap F_b$. on a alors f(a)=a et f(b)=b.
D'où, puisque f est déterminé par f(a) et f(b), on a f=Id.
Remarque : Les questions 5, 6 et 7 montrent que Aut(D_n)=$F_b \rtimes F_a$.
8)Puisque F_b est normal dans Aut(D_n)=F_aF_b, on peut appliquer le Second Théorème d'isomorphisme : Aut(D_n)/F_b est isomorphe à $F_a/F_a \cap F_b$.
D'où, $F_a \cap F_b$ étant réduit à {1}, |Aut(D_n)| = $\frac{|F_a||F_b|}{|F_a \cap F_b|}$=$|F_a||F_b|$=$\varphi$(n)n.
9)φ(3)=2 donc Aut(D_3) est de cardinal 6.
Puisque Z(D_3)={1}, D_3 est isomorphe d'après le Premier Théorème d'isomorphisme à Int(D_3) sous-groupe de Aut(D_3).
D'où, on a |Int(D_3)| = $|D_3|$=6 et donc Aut(D_3)=Int(D_3) et Aut(D_3) est isomorphe à D_3.