Intitulé de la matière:

Introduction à la théorie des groupes

(semestre 6: licence Mathématiques LMD).

Contenu de la matière:

Chapitre 0. Rappels sur la théorie des ensembles, relation binaire, application, injection, surjection...

Chapitre 1. Groupes et morphismes

Groupe, sous groupe, classes d'équivalence modulo un sous-groupe, théorème de Lagrange, morphisme de groupes, image, noyau, isomorphisme, groupe distingué, groupe quotient, théorème d'isomorphisme, groupe cyclique, indicatrice d'Euler, sous groupes d'un groupe cyclique, étude des groupes $(\mathbb{Z}/n\mathbb{Z}, +)$et $(\mathbb{Z}/n\mathbb{Z}, \times)^{\times}$.

Chapitre 2. Action d'un groupe sur un ensemble,

Définition de l'action d'un groupe, orbite, stabilisateur, point fixe, théorème de Burnside, exemples et applications.

Mode d'évaluation : Examen (60 pour cent), control continu (40 pour cent).

Références.

1. Modern Algebra, John R. Durbin
2. Aujourd'hui les mathématiques, Paul Vissio
3. Introduction to abstract algebra. Keith Nicholson.
4. Introduction à l'algèbre, A. Kostrikin.
5. Algèbre pour la licence 3 (groupes, anneaux et corps), Jean Jacques , Pascal Boyer Dunod paris 2006.
6. Algèbre et géomètrie, Jean Delcourt, Remit Goblot, Dunod Paris 2005.

I.1 Rappels sur la théorie des ensembles.

Un ensemble E est une collection d'objets dits éléments de l'ensemble E. Si e est un élément de E on note $e \in E$, sinon on note $e \notin E$.
Pratiquement, on peut définir un ensemble de deux façons:
1) par extension: en décrivant tous ses éléments entre accolades $E = \{0, 2, 4, 6, 8, 10\}$.
2) par compréhension: en donnant une propriété commune caractérisant tous ses éléments.
$E = \{x/x \text{ vérifie la propriété } p\}$. Par exemple, l'ensemble des entiers pairs peut etre défini par :
$P = \{n \in \mathbb{N}/ \text{ l'entier } n \text{ est pair}\}$.
Soit E un ensemble, on note par $\wp(E)$ l'ensemble des parties de E, on a:

$$A \subseteq E \iff A \in \wp(E)$$

Donc $\wp(E) = \{A/A \subseteq E\}$. Il suffit de prendre $A = E$ ou bien $A = \emptyset$, pour voir qu'on a respectivement: $E \in \wp(E)$ et $\emptyset \in \wp(E)$. En particulier, si $a \in E$ alors le singleton $\{a\} \in \wp(E)$, on a:

$$\mathtt{a} \in \mathtt{E} \iff \{a\} \subset \mathtt{E} \iff \{a\} \in \wp(E)$$

Soient E, F deux ensembles. On a

$$E = F \iff E \subseteq F \text{ et } F \subseteq E \text{ (double inclusion)}$$

$$\mathtt{E} \subseteq \mathtt{F} \iff (\mathtt{a} \in \mathtt{E} \implies \mathtt{a} \in \mathtt{F})$$

Exercice 1
1/ Soient $A_1 = \left\{x \in \mathbb{N}/x^2 - x - 2 = 0\right\}$, $B_1 = \{2\}$. Montrer que $A_1 = B_1$.
2/ Soient $A_2 = \{x \in \mathbb{Z} \ / \ x \text{ est divisible par } 6\}$, $B_2 = \{x \in \mathbb{Z} \ / \ x \text{ est multiple de 2 et 3}\}$. Montrer qu'on a $A_2 = B_2$.

I.2 Partition et recouvrement d'un ensemble.

Soit E un ensemble et soit $(A_i)_{i\in I}$ une famille de parties de E, i.e, $\forall i \in I$, $A_i \subseteq E$ (ou bien $A_i \in \wp(E)$), avec I un ensemble d'indices fini ou infini. On dit que $(A_i)_{i\in I}$ est une partition de E si d'une part, l'union ces parties donnent E, et d'autres parts ces parties sont disjoints 2 à 2 i.e,

a) $\forall i \in I : A_i \neq \emptyset$,
b) $A_i \cap A_j = \emptyset$, pour tous $i, j \in I$,avec $i \neq j$.
c) $\bigcup\limits_{i\in I} A_i = E$

La famille $(A_i)_{i\in I}$ est dite un recouvrement de E si on a $\bigcup\limits_{i\in I} A_i = E$, dans ce cas des parties de $(A_i)_{i\in I}$ peuvent avoir des éléments en

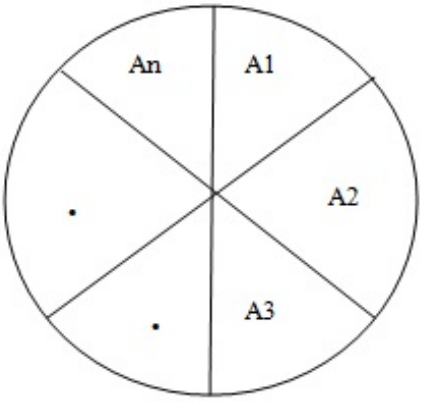
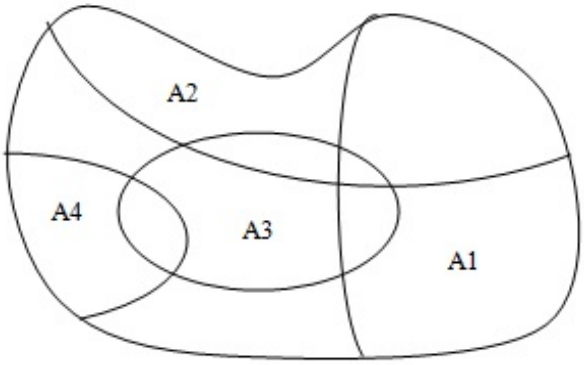


Figure 1: partition de E

commun, c.à.d, il peut exister $i,\ j \in I,\ i \neq j$ avec $A_i \cap A_j \neq \emptyset$.



recouvrement de E

Exercice 2 Montrer que si un ensemble E contient n éléments, alors l'ensemble $\wp(E)$ des parties de E, contient 2^n parties.

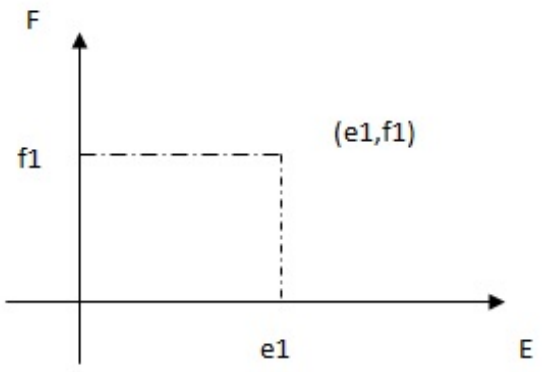
Preuve: voir td

Exercice 2 Soient $E = \mathbb{R}$ et $I = \mathbb{Z}$. On définit $\forall i \in I : A_i = [i, i+1[$. Par exemple, $A_0 = [0,1[,\ A_1 = [1,2[,\ A_{-1} = [-1,0[,\ A_{-2} = [-2,-1[$. On a

1/ Pour $i \neq j$: $A_i \cap A_j = \emptyset$,
2/ $\bigcup_{i \in I} A_i = \bigcup_{i \in Z} [i, i+1[= \mathbb{R}$. Vérifier les résultats 1 et 2.

I.3 Produit cartésien

Soient E, F deux ensembles. Leur produit cartésien, noté $E \times F$, est l'ensemble $E \times F = \{(x, y) / \ x \in E \text{ et } y \in F\}$.



produit cartésien

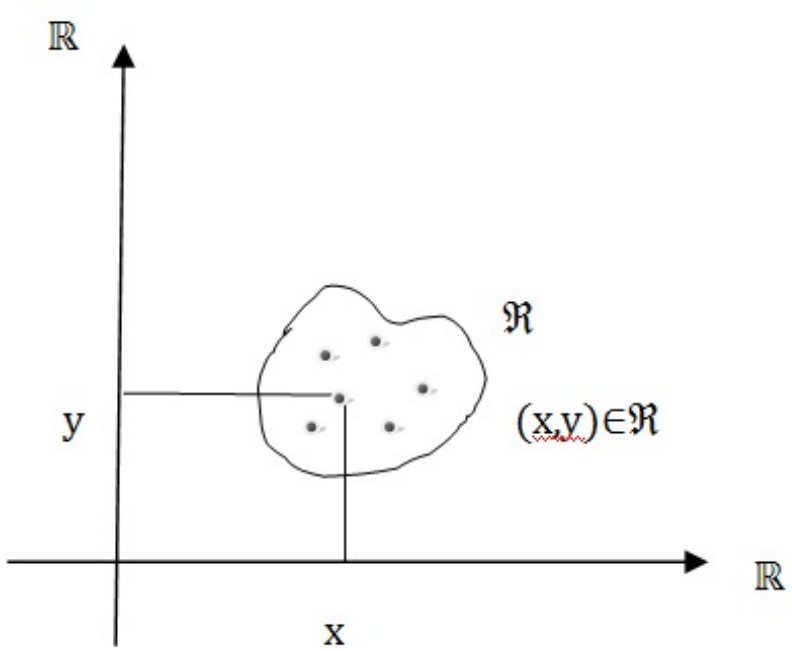
En général, si $E_1, E_2, ..., E_n$ sont n ensembles, leur produit cartésien est l'ensemble $E_1 \times E_2 ... \times E_n = \{(x_1, x_2, ..., x_n) / \forall i \in \{1, 2, ..., n\} \ x_i \in E_i\}$. Un élément $(x_1, x_2, ..., x_n) \in E_1 \times E_2 ... \times E_n$ est dit un n-uplet. L'élément $(x, y) \in E_1 \times E_2$ est dit un couple, l'élément $(x, y, z) \in E_1 \times E_2 \times E_3$ un triplet, l'élément $(x, y, z, t) \in E_1 \times E_2 \times E_3 \times E_4$ un quadruplet...etc. Si $E_1 = E_2 = ... = E_n = E$, on note par E^n (n copies de E), le produit cartésien $E \times E ... \times E$ (n fois).

Exemples.
1/ $\mathbb{R}^2 = \{(x, y) / x \in \mathbb{R} \text{ et } y \in \mathbb{R}\}$, $\mathbb{R} \times \{0\} = \{(x, 0) / x \in \mathbb{R}\}$ on a $\mathbb{R} \times \{0\} \subset \mathbb{R}^2$.
De meme, $\{0\} \times \mathbb{R} = \{(0, x) / x \in \mathbb{R}\} \subset \mathbb{R}^2$et $(\mathbb{R} \times \{0\}) \cap (\{0\} \times \mathbb{R}) = \{(0, 0)\}$.
Exercice 3 Soit A, B et C trois ensembles quelconques. Démontrer l'égalité
A$\times (B \cap C) = (A \times B) \cap (A \times C)$
Si $A \times B = A \times C$ avec $A \neq \emptyset$ alors $B = C$.

I.4 Relation.

Soient E, F deux ensembles. Une relation binaire $\Re$ de E vers F est une partie de $E \times F$, i.e, $\Re \subseteq E \times F$. Si $(x, y) \in \Re$ on note par $x\Re y$ le fait que l'élément x est en relation avec l'élément y selon la relation $\Re$, sinon on a $(x, y) \notin \Re$ (x et y ne sont pas en relation selon $\Re$). Comme $\emptyset \subseteq E \times F$, alors $\emptyset$ est dite la relation vide qui ne contient aucun couple (aucun élément de E n'est en relation avec aucun élément de F). De même comme on a $E \times F \subseteq E \times F$, alors $E \times F$ est dite la relation pleine (tout élément de E est en relation avec tout élément de F).

Soit $\Re : A \to B$ une relation, on note par
$Dom(\Re) = \{a \in A / \exists b \in B : (a, b) \in \Re\} \subseteq A$
le domaine de la relation $\Re$ et par
$Rang(\Re) = \{b \in B / \exists a \in A : (a, b) \in \Re\} \subseteq B$.



l'image de la relation $\Re$

L'image d'un élément $a \in A$ est l'ensemble $\Re(a) = \{b \in B : (a, b) \in \Re\}$ des éléments de B avec lequels l'élément a est en relation. Les antécedents de $b \in B$ est l'ensemble $\Re^{-1}(b) = \{a \in B : (a, b) \in \Re\}$ des éléments de A en relation avec b.

Inverse relation(relation inverse):

If $\Re \subseteq A \times B$ then the inverse of $\Re$ is a relation from the set B to set A which is denoted by $\Re^{-1}$ and is defined by $\Re^{-1} = \{(b,a) / (a,b) \in \Re\}$ or equivalently, $(a,b) \in \Re \iff (b,a) \in \Re^{-1}$.

On fait remarquer ici qu'on peut calculer la relation inverse $\Re^{-1}$ de toute relation binaire $\Re$. Alors que la réciproque f^{-1} d'une application f de E vers F ne peut être définie que si f est une bijection (au moins une injection).

Une relation binaire sur un ensemble E est une partie de $E \times E$. On note par I_E ou bien $\triangle_E$ le relation identité de E, c.à.d, $I_E = \{(a,a) / a \in E\}$ qui représente aussi la diagonale dans la table du produit cartésien $E \times E$. Certaines propriétés remarquables d'une relation binaire $\Re$ sur un ensemble E sont: La relation $\Re$ est dite réflexive si $(a,a) \in \Re$ pour tout $a \in E$; symétrique si $(b,a) \in \Re$ lorsque $(a,b) \in \Re$; antisymétrique si $(a,b) \in \Re$ et $(b,a) \in \Re$ alors $a = b$, et transitive si $(a,b) \in \Re$ et $(b,c) \in \Re$ alors $(a,c) \in \Re$.

Exemples a). Soient $E = \{1,2,3,4,5\}$, $F = \{5,6,7,8,9\}$ et la partie $\Re = \{(a,b) / a \in E \text{ et } b = 2a+3 \in F\} = \{(1,5),(2,7),(3,9)\}$ est une relation sur $E \times F$.

b). Toute fonction $f : E \longrightarrow F$ est une relation binaire de E vers F, i.e , $f \subseteq E \times F$ avec la condition: si $(a,b) \in f$ et $(a,c) \in f$ alors $b = c$ on écrit donc $f(a) = b$ (pour une fonction un élément ne peut avoir plus d'une image).

Exercice 4

a/ Soit E un ensemble. Montrer que toute relation d'équivalence $\Re$ sur E détermine une partition $P = (A_i)_{i \in I}$ de l'ensemble E. Inversement, à toute partition $P = (A_i)_{i \in I}$ de E on peut définir une relation d'équivalence correspondante. Donc le nombre de partitions d'un ensemble est égal au nombre de relations d'équivalences sur cette ensemble.

b/ Soient P et P' 2 partitions d'un ensemble E. On dit que P est plus fine que P' si:

$\forall p \in P, \exists p' \in P'$ tel que $p \subseteq p'$.

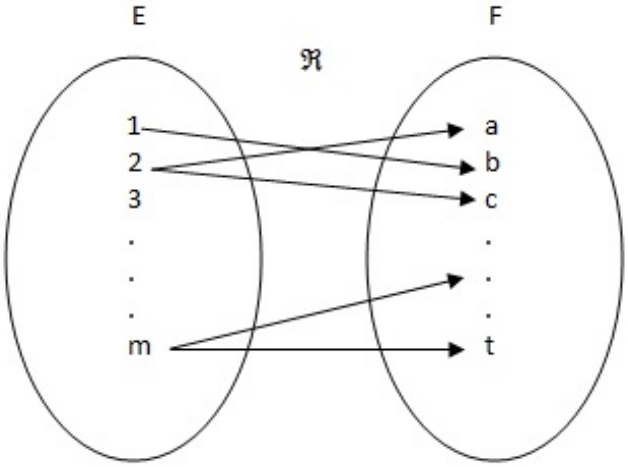
Soient R et R' deux relations d'équivalences sur E. Montrer que $\Re \subseteq \Re' \iff E/\Re$ est plus fine que $E/\Re'$.

c/ Soit $E = \mathbb{Z}$ et les relations $\Re = (\equiv \bmod [4])$, $\Re' = (\equiv \bmod [2])$. Montrer que $\mathbb{Z}/\equiv \bmod [4]$ est plus fine que $Z/\equiv \bmod [2]$.

Graphe d'une relation.

Soit $\Re \subseteq A \times B$ une relation. On peut représenter $\Re$ d'une manière saggitale, cartésienne ou bien matricielle.

Représentation saggitale



Représentation saggitale d'une relation

Représentation cartésienne de $\Re$

E\F	Y1	Y2	.	.	.	.	Ym
X1	x						
X2		x					
.							
.							
Xn							

Représentation cartésienne de $\Re$

Représentation Matricielle d'une relation.
On peut représenter une relation $\Re$ par une matrice $M_{\Re}$qu'on définie

par $M_{\Re}(i,j) = 1$ si $(i,j) \in \Re$ sinon on pose $M_{\Re}(i,j) = 0$, par exemple $M_{\Re} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.
Une relation binaire intéressante sur un ensemble E est la relation d'équivalence qui permet de quotienter l'ensemble E en une partition. Si la relation binaire $\Re$ sur l'ensemble E est une relation d'équivalence, alors la classe de l'élément $a \in E$ est la partie de E définie par: $\overline{a}_{\Re} = \{b \in E / a \Re b\}$. Evidemment, on a $\forall a, b \in E$, soit $\overline{a}_{\Re} \cap \overline{b}_{\Re} = \emptyset$ soit

$\overline{a}_{\Re} = \overline{b}_{\Re}$. Comme exemple de congruence (une congruence est une relation d'équivalence compatible avec les lois de la structure), prenons $E = \mathbb{Z}$ (l'ensemble des entiers) et la congruence, notée $\equiv$, définie sur $\mathbb{Z}$ par: Soit $(n \geq 2) \in \mathbb{N}$, pour $x, y \in \mathbb{Z}$ on dit que $a \equiv b \,[\mathrm{mod}\, n]$ si et seulement si l'entier n divise $a-b$. Evidemment, cette relation est réflèxive, symétrique et transitive. La classe $\overline{a}_{\equiv}$d'un élément $a \in \mathbb{Z}$ est $\overline{a}_{\equiv} = a + n\mathbb{Z}$. Comme pour tout entier $a \in \mathbb{Z}$, on a par division euclidienne de l'entier a par l'entier naturel n:

$a = nq + r$ (q :le quotient de la division et r son reste), avec $0 \leq r < n$. Par passage aux classes on obtient:

$\overline{a} = \overline{\overline{nq+r}} = \overline{nq} + \overline{r} = \overline{0} + \overline{r} = \overline{r}$ avec $0 \leq r < n$. Et par suite, l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ est :

$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, ..., \overline{n-1}\right\}$ avec $\overline{0} = n\mathbb{Z}$, $\overline{1} = 1 + n\mathbb{Z}$, ..., $\overline{n-1} = (n-1) + n\mathbb{Z}$. Il est clair que le cardinal de toute classe est infini.

Exercice 5

Soit n un entier naturel donné. On suppose $n \geq 2$. On définit dans $\mathbb{Z}$ une relation $a \equiv b [\mathrm{mod}\, n]$ qui signifie que $(\exists k \in \mathbb{Z})$ tel que $a - b = kn$.
1/ Montrer que cette relation est une relation d'équivalence. Cette relation est appelé congruence modulo n. On désigne par $\overline{a}$ la classe d'équivalence de l'entier relatif a. Déterminer tous les éléments de $\mathbb{Z}/n\mathbb{Z}$.
2/
a/ On définit dans $\mathbb{Z}/n\mathbb{Z}$ une addition et une multiplication par: $\overline{a} \oplus \overline{b} = \overline{a+b}$ et $\overline{a} \odot \overline{b} = \overline{ab}$.
Montrer que $(\mathbb{Z}/n\mathbb{Z}, \oplus, \odot)$ est un anneau commutatif. Est il intègre?
b/ Montrer que si n est premier alors $\mathbb{Z}/n\mathbb{Z}$ est un corps.
3/ Donner les tables d'addition et multiplication de $\mathbb{Z}/5\mathbb{Z}$ et résoudre le système d'équations suivant dans $\mathbb{Z}/5\mathbb{Z}$

$$\begin{array}{l} 1x \oplus 2y = 3 \\ 2x \oplus 3y = 4 \end{array}$$ où x, y sont des éléments cherchés dans $\mathbb{Z}/5\mathbb{Z}$.

4/ Résoudre l'équation $x^2 - 4x - 2 = 0$, x étant un élément cherché dans $\mathbb{Z}/5\mathbb{Z}$.
5/ Soit $a \in \mathbb{Z}$, on désigne par $a\mathbb{Z}$ l'ensemble $a\mathbb{Z} = \{ay / y \in \mathbb{Z}\}$.
5a/ Montrer que $a\mathbb{Z} \oplus b\mathbb{Z} = p\gcd(a,b)\,\mathbb{Z}$.
5b/ Montrer que $a\mathbb{Z} \cap b\mathbb{Z} = ppcm(a,b)\,\mathbb{Z}$.

Exercice 6

Soit E un ensemble à n éléments Trouver:
1/ Le nombre de relations binaires dans E,
2/ Le nombre de relations réflexives dans E,
3/ Le nombre de relations symétriques dans E.
Preuve: Voir td

I.5 Application.

Soit E, F deux ensembles. Une application f de E vers F est une relation binaire de E vers F, qui vérifie en plus la condition suivante: si on a $(a,b) \in f$ et $(a,c) \in f$ alors $b = c$ (c.à.d, l'élément $a \in E$, ne peut avoir plus d'une image $f(a) \in F$).
Soit f une application de E vers F.
a/ L'application f est dite injective (one to one)
si pour $x_1, x_2 \in E$ on a $f(x_1) = f(x_2)$ alors $x_1 = x_2$,
ceci est équivalent à dire si $x_1 \neq x_2$ alors on a aussi $f(x_1) \neq f(x_2)$
(deux éléments différents de l'ensemble de départ ont des images différents dans l'ensemble d'arrivé). Tout cela est équivalent à dire qu'on a:
$\forall y \in F$ on $\left|f^{-1}(y)\right| \leq 1$.
b) L'application f est dite surjective(onto),
si $\forall y \in F \Longrightarrow \exists x \in E$ tel que $y = f(x)$.
Ceci est équivalent à dire qu'on a : $f(E) = F$, ce qui revient à dire qu'on a aussi : $\forall y \in F$ on a $\left|f^{-1}(y)\right| \geq 1$.

c/ L'application f est dite bijective si elle est injective et surjective ce qui est équivalent à dire: $\forall y \in F$ on $\left|f^{-1}(y)\right| = 1$.

Exercice 7
Soit E, F deux ensembles finis avec $|E| = |F|$. Pour montrer qu'une application f de E vers F est une bijection, il suffit de montrer que c'est une injection (ou bien une surjection). En d'autres mots, on doit montrer f est injective si et seulement si f est surjective.
Preuve: Voir td.

Notion de cardinal.
Soit E un ensemble. Le cardinal de l'ensemble E mesure la taille (size) de l'ensemble E. Pour mesurer la taille d'un ensemble, on utilise les applications (Cantor). Si l'ensemble E est fini, alors il existe un entier naturel $n \in \mathbb{N}$ tel que E soit en bijection avec l'ensemble $\{1, 2, ..., n\}$ et note $Card(E) = |E| = n$. Par exemple, on a $|\emptyset| = 0$, $|\{2\}| = 1$, $|\{1, 2, ..., n\}| = n$. Si l'ensemble E est infini, on compare sa taille avec les ensembles infinis usuels tels que $\mathbb{N}$, $\mathbb{R}$,...etc. On dit qu'un ensemble E est infini dénombrable, s'il est en bijection avec l'ensemble des entiers naturels $\mathbb{N}$ dans ce cas, on définit $|E| = \aleph_0$ (aleph zéro), qui est le plus petit cardinal infini, evidemment $\aleph_0 \notin \mathbb{N}$. Sinon, l'ensemble E est dit infini non dénombrable, dans ce cas on a $|E| > \aleph_0$.
Exercice 8
1/ Montrer que les ensembles $\mathbb{Z}$, $\mathbb{Q}$ sont dénombrables.
2/ Montrer que l'intervalle(ensemble) $[0, 1] \subset \mathbb{R}$ est non dénombrable.
Preuve: voir td

The symbols $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are reseved to denote the following sets:
$\mathbb{N}$ the set of all natural numbers, $\{1, 2, 3, ..\}$,
$\mathbb{Z}$ the set of all integers, $\{..., -2, -1, 0, 1, 2, ...\}$,
$\mathbb{Q}$ the set of all rational numbers, that is, real numbers that can expressed in the form a/b, with $a, b \in \mathbb{Z}$ and $b \neq 0$,
$\mathbb{R}$ the set of real numbers.
$\mathbb{C}$ the set of all complex numbers.

Chapitre 1 Préliminaires

.

Rappels.
Lois de composition internes (opérations internes), Qualités d'une loi de composition interne.

,

Définition. *Une loi de composition interne (ou opération interne) sur un ensemble non vide E est une application $f : E \times E$ vers E. Cela signifie qu'a tout couple $(a, b) \in E \times E$ correspond un seul élément $c = f(a, b) \in E$ bien déterminé, appelé le composé de l'élément a par l'élément b par l'opération en considération.*

En général, une opération binaire est notée par un symbole désignant cette opération, on emploie généralement des symboles tels que: $+$, $\times$, $\div, -, \circ, \cup, \cap, ...$

Exemples. 1. Si $E = \mathbb{N}$ l'ensemble des entiers naturels, les applications suivantes définissent des opérations internes sur $\mathbb{N}$ (opérations arithmétiques usuelles):

Addition : $\mathbb{N}\times\mathbb{N} \xrightarrow{+} \mathbb{N}$, Addition $(a, b) = a+b$ (au couple d'entiers naturels (a, b) est associé leur somme $s = a + b$).

Multiplication : $\mathbb{N} \times \mathbb{N} \xrightarrow{\times} \mathbb{N}$, Multiplication $(a, b) = a \times b$ (au couple entiers naturels (a, b) est associé leur produit $p = a \times b$).

Elevation à la puissance : $\mathbb{N} \times \mathbb{N} \xrightarrow{\times} \mathbb{N}$, $(a, b) \longmapsto a^b$.

2. Considérons l'ensemble $\wp(E)$ des parties d'un ensemble E.On peut définir les opérations suivantes sur $\wp(E)$:

- Opération intersection : à deux parties A et B on peut associer une nouvelle partie appelée intersection de A et B (notée $A\cap B$)).

-Opération réunion : à deux parties A et B on peut associer une nouvelle partie appelée union de A et B (notée $A \cup B$)).

3. Let S denote any nonempty set , and let $M(S)$ denote the set of all mappings from S to S. For $\alpha \in M(S)$ and $\beta \in M(S)$ then $\alpha : S \longrightarrow S$, $\beta : S \longrightarrow S$ and $\beta \circ \alpha \in M(S)$ (the operation " $\circ$ "is called the composition of the mapping α with mapping β.

En général, différentes opérations peuvent être définies sur le même ensemble X. On peut définir aussi des opérations $n-$aires (unaire pour $n = 1$, par exemple pour $A \in \wp(E)$ on peut calculer son complémentaire $\overline{A} = E - A \in \wp(E)$. De même, pour $a \in \mathbb{Z}$ on peut définir son opposé $-a \in \mathbb{Z}$. Pour n vecteurs $\{v_1, v_2, ..., v_n\}$de $\mathbb{R}^n$, on peut définir leur unique point barycentrique $G(v_1, v_2, ..., v_n) \in \mathbb{R}^n$.

Fermeture d'un ensemble par une opération.

Si $\circledast$ est opération binaire sur un ensemble E, il est possible de l'étendre l'opération $\circledast$ à des parties de cet ensemble grâce à la formule suivante:

$$\mathtt{A} \circledast \mathtt{B} = \{a \circledast b / a \in A \text{ et } b \in B\}$$

Etendons l'addition aux ensembles d'entiers en posant: $A+B = \{a+b/a \in A \text{ et } b \in B\}$,
Nous aurons,par exemples, $\{2,3,4\}+\{2,3,4\} = \{4,5,6,7,8\}$,
$\{1\}+\{0,2,4,6\} = \{1,3,5,7\}$,
$\{0,1\}+\{0,2,4,6\} = \{0,1,2,3,4,5,6,7\}$,
$\mathbb{Z}^+ + \mathbb{Z} = \mathbb{Z}$,
$\mathbb{Z}^+ + \mathbb{Z}^- = \mathbb{Z}$
Supposant que $\oplus$ est une opération binaire sur l'ensemble E avec $A \subseteq E$, on dit que la partie A est fermée,ou bien stable par l'opération binaire $\oplus$, si pour toute paire d'éléments (non nécessairement distincts) x et y de A, on a $x \oplus y \in A$, i.e., $A \oplus A \subseteq A$.

Exemple: Les ensembles $\{0\}$, $\mathbb{N}$, $\mathbb{Z}^+$ sont fermés pour l'addition, alors que $\{0,1\}$ ne l'est pas on a $1+1=2 \notin \{0,1\}$.
- L'ensemble des entiers impairs est fermé par multiplication. En effet, soient $x = 2m+1$ et $y = 2n+1$ deux entiers impairs, on a bien $xy = (2m+1)(2n+1) = 4mn+2m+2n+1 = 2(2mn+m+n)+1 = 2k+1$ avec $k = (2mn+m+n)$ ce qui confirme que le produit est aussi impair.

Table d'une opération sur un ensemble fini

Une façon commode de décrire ou bien représenter une opération binaire "$*$" sur un ensemble fini $E = \{a_1, a_2, ..., a_n\}$ est de construire une table T, dite table de Cayely (Arthur Cayely mathématicien anglais $1821-1895$), contenant n lignes numérotées $\{a_1, a_2, ..., a_n\}$ et n colonnes numérotées aussi $\{a_1, a_2, ..., a_n\}$ (on a donc un tableau carré $n \times n$) tel que l'élément d'indice ij contient le composé $c = a_i * a_j$ i.e., $T(i,j) = a_i * a_j$. Chaque élément de la table peut prendre une valeur de $E = \{a_1, a_2, ..., a_n\}$ indépendemment des autres. Chaque table définie une opération binaire sur E. Le changement d'au moins une seule case définit une opération nouvelle, et par suite le nombre d'opérations qu'on peut définir sur E est : $n \times n \times ... \times n$ (chaque case peut prendre n éléments et on a n^2 cases) $= n^{n^2}$ opérations ou bien tables différentes. Il faut noter içi que ce nombre représente le nombre d'applications qu'on peut construire de l'ensemble $E \times E$ vers E dont le cardinal est, si E est fini, $|E|^{|E \times E|} = n^{n^2}$ opérations différentes.
Par exemple la table d'addition modulo m,, peut être représenter par le tableau
Rappel sur le nombre d'applications d'un ensemble $E = \{a_1, a_2, ..., a_n\}$ vers un ensemble $F = \{b_1, b_2, ..., b_m\}$. On peut représenter une application

f de E vers F par $f = \begin{pmatrix} a_1 & a_2 & . & . & . & a_n \\ f(a_1) & f(a_2) & . & . & . & f(a_n) \end{pmatrix}$. Chaque élément $a_i \in E$ peut prendre, indépendamment des autres, pour image $f(a_i) \in \{b_1, b_2, ..., b_m\}$. Et par suite, le nombre des applications de E vers F est égale à : $m \times m \times ... \times m$ (n fois)$= m^n = |F|^{|E|}$.

Qualités d'une loi de composition interne.

The notion of operation is so fundamental in algebra that algebra could almost be defined as the sudy of operations. In calculs, for example, it is not all functions f:$\mathbb{R} \longrightarrow \mathbb{R}$ that are of interest, but only functions that have some property such as continuity or differentiability. In the same way, in algebra the operations that are of interest usually possess certain special properties. See[].

We now introduce some of the most important of these properties.

1. Associativité (Associativity).

Definition An operation $*$ on a set S is said to be associative if it satisfies the condition

$$a * (b * c) = (a * b) * c \text{ for all } a, b, c \in S$$

For example, the addition of real numbers is associative: $a+(b+c) = (a+b)+c$ for all $a, b, c \in \mathbb{R}$, however, the subtraction is not associative: $(6-5)-3 = -2 \neq 6-(5-3) = 4$.

- On peut verifier que les lois $\cup$, $\cap$ sont associatives dans l'ensemble $\wp(E)$.

- La loi "$\circ$" composition des applications est associative: pour les ensembles F, G, H avec $E \overset{f}{\longrightarrow} F \overset{g}{\longrightarrow} G \overset{h}{\longrightarrow} H$ on a $(f \circ g) \circ h = f \circ (g \circ h)$. Il en est de même, si les applications f, g, h sont définies sur le même ensemble E.

Remarque: Il faut noter que si la loi est définie par une table sur un ensemble fini E, il faut vérifier l'associativité pour chaque triplet $(a, b, c) \in E^3$ en considérant que $(a, b, c) \neq (a, c, b) \neq (b, a, c) \neq (b, c, a) \neq (c, a, b) \neq (c, b, a)$. Par exemple, l'opération $\intercal$ définie sur l'ensemble $E = \{a, b, c\}$ par la table suivante n'est pas associative:

$\begin{vmatrix} \intercal & a & b & c \\ a & a & c & b \\ b & c & b & a \\ c & b & a & c \end{vmatrix}$, on a $(a \intercal b) \intercal c = c \intercal c = c \neq a \intercal (b \intercal c) = a \intercal a = a$.

2. Commutativité (Commutavity).

Definition An operation $*$ on a set S is said to be commutative if

$$a * b = b * a \text{ for all } a, b \in S$$

Exemples: Dans les ensembles usuels $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ les opérations addition "$+$" et multiplication "$\times$" sont commutatifs alors que les opérations soustraction "$-$", division "$\div$",exponentition "a^b ne le sont pas.

-Dans l'ensemble des parties $\wp(E)$, les opérations suivantes sont commutatives: $\cup, \cap$.

-Dans l'ensemble $M(S)$ des applications de S vers S l'opération composition des applications "$\circ$" n'est pas commutative.

- On fait remarquer que lorsque la loi $*$ est commutative dans un ensemble fini E, sa table de Cayley est symétrique par rapport à la diagonale.

Éléments commutables.

Lorsque la loi $*$ n'est pas pas commutative, il peut exister des éléments x et y tels que $x*y = y*x$. De tels éléments sont dits permutables ou bien commutables pour la loi $*$.

Par exemple, dans $\mathbb{N}^*$ la loi d'exponentition $(a,b) \longmapsto a^b$ n'est pas commutative, mais les éléments 2 et 4 sont commutables. En effet, on a $(2,4) \longmapsto 2^4 = 16$ et $(4,2) \longmapsto 4^2 = 16$ i.e., $2^4 = 4^2 = 16$.

Elément neutre à gauche (resp. à droite), élément neutre.

Définition 1. Dans un ensemble E muni d'une opération interne notée $*$, un élément e est dit neutre à gauche (resp. à droite) pour la loi $*$ si, quelque soit l'élément a de l'ensemble E on a:

$$e * a = a$$
$$\textit{(resp. } a * e = a)$$

2 Dans un ensemble E muni d'une opération interne notée $*$, un élément e est dit élément neutre s'il est neutre à gauche et neutre à droite , i.e., $e * a = a * e$ quelque soit l'élément $a \in E$.

Exemples.

Pour l'opération exponentiation dans $\mathbb{N}$, l'entier naturel 1 est neutre à droite car $(a,1) \longmapsto a^1 = a$, par contre 1 n'est pas neutre à gauche: $(1,a) \longmapsto 1^a = 1 \neq a$ pour tout entier naturel a différent de 1.

Dans $\mathbb{N}$, l'élément 0 est neutre pour l'addition et l'élément 1 est neutre pour la multiplication.

Dans $\wp(E)$, l'élément $\emptyset$ est neutre pour l'opération union: $A \cup \emptyset = \emptyset \cup A = A$, $\forall A \subseteq E$ et l'élément E est neutre pour l'opération intersection: $A \cap E = E \cap A = A$.

Dans l'ensemble $M(S)$ des applications de S vers S, l'application identique i_S est l'élément neutre pour la composition des applications "$\circ$" :

$\forall x \in S$ and $\alpha \in M(S)$ on a : $\alpha \circ i_S(x) = \alpha(i_S(x)) = \alpha(x)$ and $(i_S \circ \alpha)(x) = i_S(\alpha(x)) = \alpha(x)$, ce qui prouve le résultat. ,

Eléments symétriques.

Definition Assume that $*$ is an operation on S, with identity e, and that $a \in S$. An element a' in S is an inverse of a relative to $*$ if

$$a * a' = a' * a = e$$

On dit aussi que a' est le symètrique de $a \in S$. On dit aussi qu'un élément est symétrisable), ou inversible (invertible), s'il admet un symétrique.

Examples.

1. Relative to the addition as binary operation on the set of integers $\mathbb{Z}$, each integer a has an inverse, its negative $-a$: $a+(-a) = (-a)+a = 0$ for each integer a.

2. Relative to the multiplication on the set of real number $\mathbb{R}$, each non zero element a has an inverse $\frac{1}{a}$: $a \times \left(\frac{1}{a}\right) = \left(\frac{1}{a}\right) \times a = 1$.

3. Relative to the multiplication on the set of integers $\mathbb{Z}$, the integer 1 is the identity element for the multiplication, but only 1 and -1 have inverses in this case: $1 \times 1 = 1$ and $(-1) \times (-1) = 1$.

4. Relative to the composition of applications on the set $M(S)$ of applications from S to S, with 1_S as the neutral element, the element α of $M(S)$ is invertible if, and only if, there is an element $\beta \in M(S)$ satisfying : $\alpha \circ \beta = \beta \circ \alpha = i_S$.

Remarque.

Dans les ensembles de nombres: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, l'usage donne le nom d'opposé au symétrique pour la loi " $+$ " et d'inverse au symétrique pour la loi " $\times$ ".

Dans les ensembles de bijections, le nom d'application réciproque est donné au symétrique pour la loi "$\circ$" composition des applications.

Composition AS An operation.

Let S denote any nonempty set, and let $M(S)$ denote the set of all mappings from S to S.

(a) Composition is an associative operation on $M(S)$, with i_S the identity element of the operation " $\circ$ "composition of applications.

(b). Composition is an associative operation on the set of all invertible mappings in $M(S)$, with identity i_S.

Introduction to Groups.

Définition d'un groupe.

Soit G Un ensemble non vide G muni d'une opération interne notée $*$. L'ensemble G a une structure de groupe pour l'opération $*$ si les trois conditions (axiomes) suivantes sont satisfaites:

1) La loi $*$ est associative c.à.d, $\forall x, y, z \in G : \; x*(y*z) = (x*y)*z$;

2) Il existe dans G un élément neutre (ou élément unité) pour la loi $*$ c.à.d, $\exists \; e \in G$ tel que : $\forall x \in G$ on a $x*e = e*x = x$;

3) Tout élément $x \in G$ possède un symétrique unique x' c.à.d, $\forall x \in G$, $\exists! x' \in G$ tel que : $x*x' = x'*x = e$.

Remarque.

- a) Le groupe est le couple $(G, *)$ vérifiant les trois conditions ci-dessus. Il n'est jamais vide, il contient au moins l'élément neutre e.

- b) Si de plus la loi $*$ est commutative c.à.d, $\forall x, y \in G$ on a $x*y = y*x$, le groupe est dit commutatif ou bien Abélien (en l'honneur de Henrik Abel, mathématicien Norvégien, 1802-1829 who used groups in order to show that for of degree ≥ 5 there cannot be any solution formula for polynomials equations of degree ≥ 5. see [Lidl]).

Groupe additif.

On appelle ainsi un groupe, abélien en général, dans lequel l'opération est notée " + ", le composé $a + b = b + a$ de deux éléments est dit somme de ces éléments, l'élément neutre est noté 0, dit le zéro du groupe, le symétrique a' de l'élément a est noté $-a$, dit opposé de a.

Dans ce cas, $\overbrace{a + a + ... + a}^{n \text{ éléments}} = na$ avec par convention $\left\{ \begin{array}{c} 0a = 0 \\ 1a = a \\ (-n)\, a = n\,(-a) = -na \end{array} \right\}$,

On a pour $m, n \in \mathbb{Z} : \; ma + na = (m+n)\, a$ et $m\,(na) = n\,(ma) = mna$.

Par exemple, $(\mathbb{Z}, +, 0)$ est un groupe additif.

Groupe multiplicatif *

C'est un groupe, abélien ou non, dans lequel la loi est noté $\times$ ou $\cdot$ (ou même sans aucun signe opératoire $c = ab$). L'élément neutre est noté 1, dit élément neutre ou bien unité du groupe, le symétrique de a,appelé inverse de a et noté a^{-1}, le composé de deux éléments a, b noté ab dit le produit de a et b.

Dans ce cas on pose $\overbrace{a \times a \times ... \times a}^{n \text{ éléments}} = a^n$, avec par convention $\left\{ \begin{array}{c} a^0 = 1 \\ a^1 = a \\ a^{-n} = \left(a^{-1}\right)^n \end{array} \right\}$.

On obtient les résultats suivants: pour $m \in \mathbb{Z}$ et $n \in \mathbb{Z}$ on a: $a^m \times a^n = a^{m+n}$ et $\left(a^m\right)^n = a^{mn}$,

Par exemple $(\mathbb{R}^*, \times)$ est un groupe multiplicatif.

Ordre d'un groupe.

Soit $(G, *)$ un groupe. Si le cardinal $|G|$ est fini le groupe est dit d'ordre fini, sinon il est dit d'ordre infini. Dans le cas où l'ordre du groupe est fini sa loi est définie par une table dite table de Cayley.

Propriétés d'un groupe.

Dans un groupe , tout élément est régulier à gauche et à droite (ou bien simplifiable à gauche et à droite)

c.à d, $a * x = a * y \Longrightarrow a^{-1} * a * x = a^{-1} * a * y \Longrightarrow x = y$. De même, $x * a = y * a \Longrightarrow x = y$.

Dans un groupe, l'équations $a * x = b$ (resp. $x * a = b$) admet une solution unique: $x = a' * b$ (resp. $x = b * a'$).

En notation additive : $x + a = b \Longleftrightarrow x = b + (-a) = b - a$.

En notation multiplicative: $ax = b \Longleftrightarrow x = a^{-1}b$ et $xa = b \Longleftrightarrow x = a^{-1}b$.

Exercice 9 Montrer que tout groupe d'ordre premier est cyclique

faire le preuve en utilisant le Th Lagrange

Propriétés de la table d'un groupe fini.

Cette table dite aussi carré Latin (les éléments de la table sont énumérés dans le même ordre par ligne comme par colonne) On peut relever de la table les propriétés suivantes:

1° Chaque élément du groupe figure une fois, et une seule, dans chaque ligne et dans chaque colonne de la table (conséquence de la régularité).

2° L'élément neutre e occupe des places symétriques par rapport à la diagonale principale (conséquence du fait que, si a et $a\prime$ sont des éléments inverses, on a: $a * a' = a' * a = e$ (a'est le symétrique de a à gauche et à droite).

3° Dans le cas d'un groupe commutatif, deux éléments quelconques de la table symétriques par rapport à la diagonale principale sont égaux.

Examples from [lidl]

1) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), ((n\mathbb{Z}, +)/z \in \mathbb{Z} \text{ and } n \in \mathbb{N}))$ sont des groupes abéliens d'ordres infinis avec 0 pour élément neutre et le symétrique de g est son opposé $-g$.

2) $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times), (\mathbb{C}^*, \times)$ sont des groupes abéliens d'ordres infinis avec 1 pour élément neutre et le symétrique de $g \neq 0$ est son inverse $\frac{1}{g}$.

3) $(\mathbb{N},+)$ n'est pas un groupe car l'opposé $-g$ de $g\in\mathbb{N}$ n'est pas dans $\mathbb{N}$. De même $(\mathbb{Z},-)$ n'est pas un groupe car la loi "$-$" n'est pas associative.

4) Soit $E=\{1,-1\}$ muni de la table de multiplication définie par

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

. On peut vérifier que $(E,\times)$ a une structure de groupe commutatif d'ordre 2.

5) Soit $G=\{a,b,c\}$, la table suivante représente une loi interne $*$ définie sur G :

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

. On peut vérifier que $(G,*)$ est un groupe d'ordre 3 d'élément neutre a avec $a'=a$, $b'=c$ et $c'=b$. La loi étant symétrique par rapport à la diagonale le groupe est donc commutatif.

6) Soit E un ensemble non vide et soit $S_E=\{f:E\longrightarrow E/\ f:\text{ est une bijection}\}$. L'ensemble S_E muni de la composition des applications "$\circ$" a une structure de groupe d'élément neutre l'application identité i_E; l'inverse de $f\in S_E$ est l'application réciproque f^{-1}, le groupe S_E est appelé le groupe symétrique de E, Si $|E|=n$, alors S_E est noté S_n d'ordre $n!$ et de degré n appelé le groupe de permutations de n letters.

7) Considérons l'ensemble de toutes les matrices carrées d'ordre n à coefficients dans $\mathbb{R}$ et déterminant non nul, cet ensemble muni de la multiplication des matrices a une structure de groupe non abélien, dit groupe linéaire général noté $GL(n,\mathbb{R})$. En effet, pour $A,B\in GL(n,\mathbb{R})$ on a bien $AB\in GL(n,\mathbb{R})$ car si $\det A\neq 0$ et $\det B\neq 0$ on bien $\det AB=\det A\times\det B\neq 0$. Le produit de matrices est associative: $A(BC)=(AB)C$, et admet la matrice carrée $I=(1)_{n\times n}$ de $\det I\neq 1$ comme élément neutre, enfin toute matrice $A\in GL(n,\mathbb{R})$ possède une matrice inverse A^{-1} telle que $AA^{-1}=A^{-1}A=I$.

8. Enfin, donnant un exemple de la géometrie. Soit ABC un triangle équilatéral de centre O. Soient R_0,R_1,R_2 les rotations de centre O et d'angles respectifs: $0°$, $120°$ et $240°$. L'ensemble $E=\{R_0,R_1,R_2\}$ muni de la composition des applications "$\circ$" est un groupe d'élément neutre la rotation nulle R_0. Ci-contre la table de ce groupe

$\circ$	R_0	R_1	R_2
R_0	R_0	R_1	R_2
R_1	R_1	R_2	R_0
R_2	R_2	R_0	R_1

II.4/ Bijection d'un ensemble sur lui même (permutation d'un ensemble E avec $|E|=n$).

Permutations et le groupe S_n.(voir voir voir)

Une permutation d'un ensemble non vide S est une application bijective de S vers S.

Rappelons que lorsque $|S| = n$, toute injection de S vers S est une permutation de S

Rappelons aussi qu'on appelle factorielle de l'entier naturel n et le note $n!$ l'entier $n! = n \times (n-1) \times (n-2) \times ... \times 2 \times 1$ avec la convention $0! = 1$ (le nombre de bijections d'un ensemble vide (de 0 éléments) vers lui même est l'application vide),Il y'a donc $A_n^n = n!$ (arrangements de n éléments) bijections de S sur lui même.

La permutation $\sigma = \begin{vmatrix} 1 & 2 & 3 & 4 & 5 & \text{ordre naturel} \\ 3 & 5 & 2 & 4 & 1 & \text{nouveau ordre} \end{vmatrix}$ de l'ensemble $\{1,2,3,4,5\}$ qui veut dire que 3 est devenu en 1^{ere} position 5 en 2^{eme} position ...etc, cette permutation sera notée $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix}$ avec $\sigma(1) = 3$, $\sigma(2) = 5$, $\sigma(3) = 2$, $\sigma(4) = 4$, $\sigma(5) = 1$.

En général, On note une permutation $\pi \in S_n$ par

$$\pi = \begin{pmatrix} 1 & 2 & . & . & n \\ \pi(1) & \pi(2) & . & . & \pi(n) \end{pmatrix}$$

L'application identité de l'ensemble $E = \{1,2,...,n\}$ est la permutation $id_E = \begin{pmatrix} 1 & 2 & . & . & n \\ 1 & 2 & . & . & n \end{pmatrix}$ généralement notée (1).

- Si $\pi, \sigma \in S_n$ alors la composition $\pi \circ \sigma$ est définie d'une manière usuelle par $(\pi \circ \sigma)(x) = \pi(\sigma(x))$.

Example: si $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$et $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ sont deux permutations de $E = \{1,2,3\}$ alors

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & \longleftarrow & 3 & \longleftarrow & 1 \\ 3 & \longleftarrow & 1 & \longleftarrow & 2 \\ 1 & \longleftarrow & 2 & \longleftarrow & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

(on compose de la droite vers la gauche)..

- Si $\pi \in S_n$, on calcul l'inverse $\pi^{-1} \in S_n$ à partir de π en lisant du bas vers le haut. Par exemple, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, en effet, on a bien $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$.

On note par S_n l'ensemble des permutations d'un ensemble de n éléments. L'ensemble S_n muni de la composition des applications $(S_n, \circ)$ est un groupe d'élément neutre $id_E = \begin{pmatrix} 1 & 2 & . & . & n \\ 1 & 2 & . & . & n \end{pmatrix}$ dit le groupe de permutations de n lettres.

Par exemple, le groupe $(S_2, \circ)$ sur l'ensemble $E = \{1,2\}$ est composé des permutations $\left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$ dont la table du groupe est définie

par $\begin{vmatrix} \circ & (1) & (12) \\ (1) & (1) & (12) \\ (12) & (12) & (1) \end{vmatrix}$. De même le groupe $(S_3, \circ)$ sur l'ensemble $E = \{1,2,3\}$ est composé des permutations $\pi_1 = \left(\begin{vmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{vmatrix}\right)$, $\pi_2 = \left(\begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{vmatrix}\right)$, $\pi_3 = \left(\begin{vmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{vmatrix}\right)$, $\pi_4 = \left(\begin{vmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{vmatrix}\right)$, $\pi_5 = \left(\begin{vmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{vmatrix}\right)$ et enfin, $\pi_6 = \left(\begin{vmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{vmatrix}\right)$. La table de Cayley du groupe $(S_3, \circ)$ est $\begin{vmatrix} \circ & \pi_1 & \pi_2 & \pi_3 & \pi_4 & \pi_5 & \pi_6 \\ \pi_1 & \pi_1 & \pi_2 & \pi_3 & \pi_4 & \pi_5 & \pi_6 \\ \pi_2 & \pi_2 & \pi_3 & \pi_1 & \pi_5 & \pi_6 & \pi_4 \\ \pi_3 & \pi_3 & \pi_1 & \pi_2 & \pi_6 & \pi_4 & \pi_5 \\ \pi_4 & \pi_4 & \pi_6 & \pi_5 & \pi_1 & \pi_3 & \pi_2 \\ \pi_5 & \pi_5 & \pi_4 & \pi_6 & \pi_2 & \pi_1 & \pi_3 \\ \pi_6 & \pi_6 & \pi_5 & \pi_4 & \pi_3 & \pi_2 & \pi_1 \end{vmatrix}$ par exemple $\pi_3 \circ \pi_5 = \left(\begin{vmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{vmatrix}\right) \circ \left(\begin{vmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{vmatrix}\right) = \left(\begin{vmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{vmatrix}\right) = \pi_4$ et $\pi_2 \circ \pi_4 = \left(\begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{vmatrix}\right) \circ \left(\begin{vmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{vmatrix}\right) = \left(\begin{vmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{vmatrix}\right) = \pi_5$.

Cryptographie : Rappelons que pour crypter(ou bien chiffrer) les éléments d'un ensemble fini E par les éléments d'un ensemble fini F de même cardinal que E est de définir une bijection $f : E \longrightarrow F$ qui chiffre tout élément $x \in E$ par un unique élément $y = f(x)$, et en déchiffre $y \in F$ par l'unique élément de E tel que: $x = f^{-1}(y)$ où f^{-1} désigne la réciproque de l'application f. Il faut noter aussi que ce chiffrement est d'autant plus éfficace lorsque, étant donné $x \in E$ il est facile de calculer $y = f(x)$ mais inversement, étant donné $y \in F$ il très difficile de calculer x tel que: $x = f^{-1}(y)$. Il est important de souligner la croissance rapide de la factorielle en fonction du nombre n choisi, on a $n^n \geq n! \geq 2^n$.par exemple:.$52! \approx 8,06 \times 10^{67}$ ce qui rend le chiffrement par permutation éfficace en cryptographie.

EXERCICEv

Démontrer que $(S_n, \circ)$ est groupe .

Exercice 8 In how many ways can 7 women and 3 men be arranged in row if the 3 men must always stand next to each other

Proof: see the td

Exercice

How many 6-digit numbers without repetition of digits are there such that the digits are all non zero and 1 and 2 do not appear consecutively in either order.

cyclic notation

The permutation $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ has the effect of moving the elements around in a cycle. This is called a cycle of length 3 and we write this as (132) and this signify $(1 \to 3 \to 2 \to 1)$. Evidently, this permutation can be also written $(321) = (213) = (132)$.

In general, if $a_1, a_2, ..., a_r$ are distinct elements of $\{1, 2, 3, ..., n\}$ the permutation $\pi \in S_n$ defined by $\pi(a_1) = a_2,\ \pi(a_2) = a_3, ..., \pi(a_{r-1}) = a_r,$ $\pi(a_r) = a_1$ and $\pi(x) = x$ if $x \notin \{a_1, a_2, ..., a_r\}$, is called a cycle of length r or an r-cycle. We denote it by $(a_1 a_2 ... a_r) = (a_1 \to a_2 \to ... \to a_r \to a_1)$.

Proposition 1

A r-cycle in S_n has order r.

Proof:

If $\pi = (a_1 a_2 ... a_r)$ is an r-cycle in S_n, then $\pi(a_1) = a_2, \pi^2(a_1) = a_3, \pi^3(a_1) = a_4, ..., \pi^{r-1}(a_1) = a_r$ and $\pi^r(a_1) = a_1$.

Similarly, $\pi^r(a_i) = a_i$ for $i = 1, 2, ..., r$. Since π^r fixes all the other elements, it is the identity permutation, but none of the permutations $\pi, \pi^2, ..., \pi^{r-1}$ equal the identity, because they move the element a_1. Hence, the order of π is r.

Example 12

Write down $\pi = (1342)$, $\rho = (13)$ and $\sigma = (12) \circ (34)$ as permutation in S_4. Calculate $\pi \circ \rho \circ \sigma$.

Solution: We have $(1342) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, (13) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$, then $\sigma = (12) \circ (34) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ ...etc.

Permutations that are not cycles can be split up into two or more cycles as follows:

If $\pi \in S_n$ and $a \in \{1, 2, 3, ..., n\}$ the orbit of a under π consist of distinct elements $a,\ \pi(a),\ \pi^2(a),\ \pi^3(a)$,..., We can split a permutation up into its different orbits, and each orbit will give rise to a cycle. Consider the permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 8 & 1 & 5 & 7 & 6 & 4 \end{pmatrix} \in S_8$. We have: $\pi(1) = 3$, $\pi^2(1) = \pi(\pi(1)) = \pi(3) = 8$, $\pi^3(1) = 4$, $\pi^4(1) = 1$. Then the orbite of 1 is $orb(1) = \{1, 3, 8, 4\}$. Evidently, $orb(1) = orb(3) = orb(8) = orb(4)$. Since π leaves 2 and 5 fixed then $orb(2) = \{2\}$, $orb(5) = \{5\}$. And finally, $orb(6) = \{6, 7\}$ is a 2-cycle.

Disjoint cycle decomposition of π is:

Figure 2: orbites de la permutation π

We have $\pi = (1384) \circ (2) \circ (5) \circ (67) = (67) \circ (2) \circ (5) \circ (1384) = (67) \circ (1384)$.

Proposition

Every permutation can be written as a product of disjoint cycles

$$\pi = \gamma_1 \circ \gamma_2 \circ ...\gamma_k$$

where γ_i are the cycles obtained as described in the precedent example.

Corollaire

The order of a permutation is the least common multiple of lengths of its disjoint cycles.

Proof

If $\pi = \gamma_1 \circ \gamma_2 \circ ...\gamma_k$ is the decomposition π in disjoint cycles $\Longrightarrow$ $\forall m$, $\pi^m = \gamma_1^m \circ \gamma_2^m \circ ...\gamma_k^m$ Because the cycles are disjoint, and this is the identity iff γ_i^m is the identity for each $k \geq i \geq 1$, the least such integer is the least common multiple of the orders of the cycles.

Example 13

The cycle decomposition of π is

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 7 & 1 & 4 & 6 & 2 \end{pmatrix} = (13825) \circ (476).$$

Then the order of π is the $\operatorname{lcm}(5, 3) = 15$. we can calculate $\pi^2, \pi^3, \pi^4, ...,$ until we obtain the identity.

La formule suivante donne une éstimation de $n!$ pour n assez large.

Théorème (formule de Stirling)

lorsque n tend vers l'infini le rapport $\frac{n!}{n^n e^{-n}\sqrt{2\pi n}} \longrightarrow 1$,

ce qui donne

$$n! \approx n^n e^{-n}\sqrt{2\pi n}$$

Example

Les éléments du groupe S_n sont utilisés pour décrire les symétries des figures géométriques (on dit que si les nombres mesures les grandeurs alors les groupes mesures les symétries), pour une figure $\mathcal{F}$du plan ou bien l'espace, on cherche les applications qui laissent invariante globalement cette figure, c.à.d $f : P \longrightarrow P$ (f :bijection du plan vers lui meme) tel que: $f(\mathcal{F}) = \mathcal{F}$. Evidemment cet ensemble n'est jamais vide il contient toujours l'application identité. La figure $\mathcal{F}$ est d'autant symétrique si son groupe d'automorphisme est assez grand, par exemple le groupe d'automorphisme du cercle est infini (il contient une infinité de rotations et de réflexions qui laissent invariants globalement un cercle de centre O)fffffffffffffffffffffff

Sous groupe

Définition

Soit G un groupe, et H un sous ensemble non vide G. On dit que H est un sous groupe de G lorsque H est lui même un groupe pour la restriction à H de l'opération de G (loi induite sur H de G). L'élément neutre dans le sous groupe H est le même que l'élément neutre dans le groupe G. L'élément symétrique d'un élément a du sous groupe H est le meme que celui dans le groupe G.