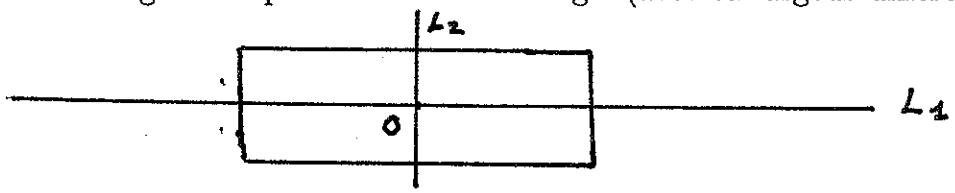
CHAPITRE 3 GROUPES, STRUCTURES ALGÉBRIQUES

La formalisation des structures algébriques –groupes, anneaux, corps, espaces vectoriels– est relativement récente mais l'idée est présente partout dans les sciences et en particulier en mathématique. Il s'agit grosso modo d'extraire des règles opératoires, valables indépendemment de la nature des objets considérés. Par exemple les règles pour faire la somme de deux nombres, la somme de deux vecteurs du plan ou la composition de deux rotations sont les mêmes. L'idée sous-jacente à la notion de groupe est celle de la symétrie ; c'est pourquoi nous choisissons d'étudier dans une première partie les symétries de quelques figures simples avant d'introduire formellement la définition de groupe.

3.1 SYMÉTRIES ET GROUPES.

Considérons une figure simple comme un rectangle (avec sa largeur différente de sa longueur) :



On distingue deux axes de symétrie : l'axe horizontal L_1 et l'axe vertical L_2 ; on voit qu'on peut aussi appliquer le rectangle sur lui-même en le faisant pivoter d'un demi-tour autour du point O (on peut aussi interpréter cela par une symétrie par rapport au point O). On admettra que ce sont les seules transformations (avec l'identité!) qui appliquent le rectangle sur lui-même en respectant les formes.

On vérifie sans peine les faits suivants :

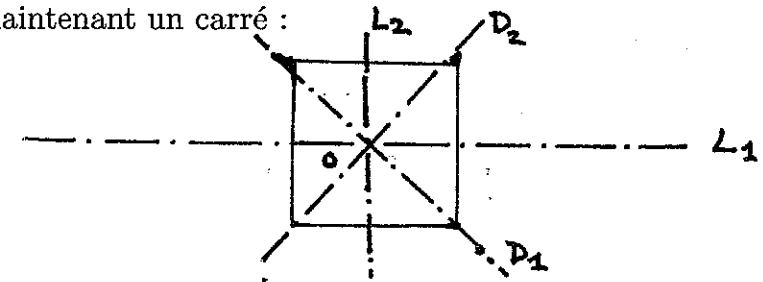
1) Appliquer deux fois la même transformation revient à appliquer l'identité

2) Appliquer la symétrie s_1 par rapport à L_1 puis la symétrie s_2 par rapport à L_2 revient à appliquer la symétrie s_O par rapport à O ; en fait appliquer deux de ces trois symétries revient à appliquer la troisième (l'ordre étant indifférent).

On peut regrouper cela dans un tableau où l'on inscrit dans la ligne de l'élément s et la colonne de l'élément t la composée $s \circ t$:

$\circ$	id	s_O	s_1	s_2
id	id	s_O	s_1	s_2
s_O	s_O	id	s_2	s_1
s_1	s_1	s_2	id	s_O
s_2	s_2	s_1	s_O	id

Considérons maintenant un carré :



Les transformations qui appliquent le carré sur lui-même, en respectant les formes, sont maintenant :

Les symétries par rapport à l'axe horizontal L_1 et à l'axe vertical L_2 (que nous noterons s_1 et s_2), les symétries par rapport à la diagonale D_1 et à la diagonale D_2 (que nous noterons s_3 et s_4), les rotations autour du point O faisant un quart de tour (que nous noterons r_1), un demi-tour (que nous noterons r_2), trois quarts de tour (que nous noterons r_3), et enfin bien sûr l'identité.

On vérifiera que : 1) Appliquer deux fois la même symétrie ou la rotation d'un demi-tour revient à appliquer l'identité ; mais appliquer deux fois la même rotation d'un quart ou trois quarts de tour revient à appliquer la rotation d'un demi-tour. Toutefois appliquer quatre fois la même rotation d'un quart ou trois quarts de tour revient à appliquer l'identité.

2) Appliquer la symétrie par rapport à L_1 puis la symétrie par rapport à L_2 revient à appliquer la rotation d'un demi-tour ; en fait appliquer deux des trois symétries revient à appliquer une des rotations, appliquer une des rotations et une des symétries revient à appliquer une des symétries. Toutefois, l'ordre n'est pas cette fois indifférent : par exemple $s_1 s_3 = r_3 \neq r_1 = s_3 s_1$.

On peut regrouper cela dans un tableau où l'on inscrit dans la ligne de l'élément s et la colonne de l'élément t la composée $s \circ t$:

$\circ$	id	r_1	r_2	r_3	s_1	s_2	s_3	s_4
id	id	r_1	r_2	r_3	s_1	s_2	s_3	s_4
r_1	r_1	r_2	r_3	id	s_3	s_4	s_2	s_1
r_2	r_2	r_3	id	r_1	s_2	s_1	s_4	s_3
r_3	r_3	id	r_1	r_2	s_4	s_3	s_1	s_2
s_1	s_1	s_4	s_2	s_3	id	r_2	r_3	r_1
s_2	s_2	s_3	s_1	s_4	r_2	id	r_1	r_3
s_3	s_3	s_1	s_4	s_2	r_1	r_3	id	r_2
s_4	s_4	s_2	s_3	s_1	r_3	r_1	r_2	id

Observons expérimentalement quelques faits : tous les éléments apparaissent une et une seule fois dans chaque ligne et colonne ; dans le premier tableau, l'ordre dans lequel on compose des éléments n'importe pas ; dans le second tableau, l'ordre est important, mais une chose est préservée : si on veut faire le produit : $s \circ t \circ u$ alors on sait qu'il n'est pas nécessaire de "mettre les parenthèses", c'est-à-dire que $(s \circ t) \circ u = s \circ (t \circ u)$.

Nous venons de décortiquer l'archétype d'un groupe ; de manière générale :

L'ensemble des transformations préservant une figure forme un groupe.

Pour voir l'intérêt de définitions plus abstraites, essayez de donner une description des 48 transformations préservant un cube.

3.2 GROUPES, EXEMPLES

Définition: Une *loi de composition* sur un ensemble E est une application de $E \times E$ vers E.

Exemples : La plupart des opérations usuelles sont des lois de composition : l'addition ou la multiplication sont des lois de composition sur $\mathbf{N}$,$\mathbf{Z}$,$\mathbf{Q}$,$\mathbf{R}$ ou $\mathbf{C}$; la soustraction définit une loi de composition sur $\mathbf{Z}$,$\mathbf{Q}$,$\mathbf{R}$ ou $\mathbf{C}$ (mais pas sur $\mathbf{N}$) ; l'application de $\mathcal{F}(E,E) \times \mathcal{F}(E,E)$ vers $\mathcal{F}(E,E)$ définie par $(f,g) \mapsto f \circ g$ est aussi une loi de composition.

Définition: Un *groupe* est la donnée d'un ensemble G et d'une loi de composition $(x, y) \mapsto x * y$ telle que :

(i) (élément neutre) Il existe e dans G tel que pour tout x dans G on a $e*x = x*e = x$.

(ii) (associativité) Pour tout x, y, z dans G on a : $(x * y) * z = x * (y * z)$.

(iii) (élément inverse) Pour tout x dans G il existe x' dans G tel que : $x*x' = x'*x = e$.

Si de plus pour tout x, y dans G on a : $x*y = y*x$, on dit que la loi $*$ est *commutative* et que le groupe $(G, *)$ est *commutatif.*

Convention : pour calculer dans un groupe, on omettra souvent le signe $*$ et on écrira gh au lieu de $g * h$.

Exemples : 1) L'ensemble des transformations du rectangle (respectivement du carré) avec la loi de composition naturelle forme un groupe de cardinal 4 (respectivement 8). Le premier groupe est commutatif, le second ne l'est pas.

2) Les ensembles $\mathbf{Z}$,$\mathbf{Q}$,$\mathbf{R}$ et $\mathbf{C}$, munis de l'addition sont des groupes (noter que $(\mathbf{N}, +)$ ne vérifie pas (iii)). Les ensembles $\mathbf{Q}^*$,$\mathbf{R}^*$ ou $\mathbf{C}^*$ munis de la mutiplication sont des groupes (noter que $(\mathbf{Z} \setminus \{0\}, \times)$ ne vérifie pas (iii)). Tous ces groupes sont commutatifs.

3) Soit E un ensemble et soit $\mathcal{S}(E)$ l'ensemble des bijections de E vers E ; soit $\circ$ la loi de composition naturelle de deux bijections, alors $(\mathcal{S}(E), \circ)$ est un groupe. En particulier l'ensemble des bijections de $\{1, 2, 3, \ldots, n\}$ vers lui-même, muni de la composition des applications, forme un groupe qu'on note $\mathcal{S}_n$. C'est un groupe avec $n!$ éléments, on l'appelle le *groupe des permutations* sur n éléments.

Définition: Un *sous-groupe* H d'un groupe $(G, *)$ est un sous-ensemble de G tel que la loi $*$ restreinte à $H \times H$ définisse une loi interne qui donne une loi de groupe sur H.

Ainsi un sous-groupe est stable pour la loi $*$ (c'est-à-dire que si $x, y \in H$ alors $x * y \in H$), l'élément neutre e appartient à H et si $x \in H$ alors $x^{-1} \in H$. Remarquons qu'il est inutile de vérifier l'associativité : puisque $\forall x, y, z \in G$, $(xy)z = x(yz)$, il est clair qu'on a $\forall x, y, z \in H$, $(xy)z = x(yz)$. En fait on peut même raccourcir ces vérifications :

PROPOSITION: *Soit H un sous-ensemble d'un groupe G, c'est un sous-groupe si et seulement si il satisfait :*

(i) $e \in H$

(ii) $x, y \in H$ entraîne $xy^{-1} \in H$.

Démonstration: Ces conditions sont nécessaires. Réciproquement, supposons les propriétés (i) et (ii) vérifiées et montrons qu'alors H est un sous-groupe. Si $y \in H$ alors $ey^{-1} = y^{-1} \in H$; si x est également dans H alors $xy = x(y^{-1})^{-1} \in H$ donc H est bien un sous-groupe. □

Exemples :

1) L'ensemble μ_n des racines complexes de l'équation $X^n = 1$, muni de la multiplication des nombres complexes forme un sous-groupe de $\mathbf{C}^*$: en effet si $z, z' \in \mu_n$ alors $(z/z')^n = z^n/z'^n = 1$ donc $z/z' \in \mu_n$.

2) L'ensemble $n\mathbf{Z} := \{nx \mid x \in \mathbf{Z}\}$ muni de l'addition est un sous-groupe de $\mathbf{Z}$. Nous verrons au chapitre 5 que ce sont les seuls sous-groupes de $\mathbf{Z}$.

3) L'ensemble des rotations préservant le carré s'écrit en reprenant les notations du premier paragraphe $\{id, r_1, r_2, r_3\}$ et est un sous-groupe du groupe des transformations préservant le carré.

4) les inclusions suivantes sont des inclusions de sous-groupes : $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$ (pour la loi d'addition) ; $\{+1, -1\} \subset \mathbf{Q}^* \subset \mathbf{R}^* \subset \mathbf{C}^*$ (pour la loi de multiplication). L'ensemble $\mathbf{R}_+^*$ (mais pas $\mathbf{R}_-^*$) est un sous-groupe de $\mathbf{R}$; le cercle $\{z \in \mathbf{C} \mid |z| = 1\}$ est un sous-groupe de $\mathbf{C}^*$.

Définition: Un *homomorphisme de groupe* est une application $f : (G, *) \to (H, \circ)$ telle que :

$$\forall x, y \in G,\ f(x * y) = f(x) \circ f(y)$$

Si de plus f est une bijection, on dit que f est un *isomorphisme* de groupe et que G et H sont *isomorphes.*

Exemples :

1) Considérons l'application $x \mapsto x^n$. C'est un homomorphisme de $\mathbf{Q}^*$ dans $\mathbf{Q}^*$ (resp. $\mathbf{R}^*$, resp. $\mathbf{C}^*$). Cette application donne un isomorphisme de groupe de $\mathbf{R}_+^*$ dans $\mathbf{R}_+^*$ (en effet tout réel positif possède une unique racine n-ème positive, voir chapitre 4).

2) Soit G le groupe des transformations du carré ; soit $E := \{A, B, C, D\}$ l'ensemble des sommets du carré et H l'ensemble des bijections de E dans E. Toute transformation du carré, préservant les formes, doit envoyer un sommet sur un sommet et donne donc une bijection de E sur E. L'application qui à un élément $s \in G$ associe sa restriction à E est un homomorphisme de groupes de G vers H.

3) Soit G un groupe et g un élément de ce groupe, définissons par récurrence $g^0 := e$ et $g^{n+1} := gg^n$ (pour $n \in \mathbf{N}$) et enfin $g^{-n} := (g^n)^{-1}$. L'application $n \mapsto g^n$ de $\mathbf{Z}$ vers G est un homomorphisme de groupes, c'est-à-dire que $g^{m+n} = g^m g^n$. Remarquons que si G est fini alors cette application n'est pas injective et il existe donc un plus petit entier positif et non nul d tel que $g^d = e$.

Définition: Le plus petit entier $d \geq 1$ tel que $g^d = e$, s'il existe, s'appelle l'*ordre* de g, s'il n'existe pas on dit que g est d'ordre infini.

Par exemple, l'élément 2 est d'ordre infini dans $\mathbf{Q}^*$ alors que -1 est d'ordre 2 dans le même groupe.

Nous avons vu qu'il est important de savoir si une application est injective ou surjective. Dans le cas d'homomorphismes de groupes il existe un critère simple qui nécessite les définitions suivantes :

Définition: Le *noyau* d'un homomorphisme de groupe $f : G \to H$ est l'ensemble $f^{-1}(\{e_H\}) = \{g \in G \mid f(g) = e_H\}$. On le note $Ker(f)$ (à cause de l'allemand "Kern").

L'importance du noyau vient du théorème suivant :

THÉORÈME: Un homomorphisme de groupe $f : G \to H$ est injectif si et seulement si $Ker(f) = \{e_G\}$. Le noyau de f est toujours un sous-groupe de G.

Démonstration: En effet $f(x) = f(y)$ équivaut à $f(x)f(y)^{-1} = e_H$ ou encore $f(xy^{-1}) = e_H$, ce qui signifie $xy^{-1} \in Ker(f)$. Si $Ker(f) = \{e_G\}$ on voit que $f(x) = f(y)$

entraîne $xy^{-1} = e$ ou encore $x = y$ donc f est injective. Si $Ker(f)$ contient un élément $g \neq e_G$ alors $f(g) = f(e_G) = e_H$ et f n'est pas injective.

La deuxième affirmation est facile : si $x, y \in Ker(f)$ alors $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = ee^{-1} = e$ donc $xy^{-1} \in Ker(f)$. □

Dans le paragraphe suivant nous étudions toutes les notions définies ici, sur l'exemple du groupe des permutations sur n éléments.

3.3 LE GROUPE $\mathcal{S}_n$.

Un élément s de $\mathcal{S}_n$ est une permutation de l'ensemble $\{1, 2, 3, \ldots, n\}$ et est donc défini par la suite $s(1), s(2), s(3), \ldots, s(n)$. On doit aussi se souvenir que si $i \neq j$ alors $s(i) \neq s(j)$. L'élément neutre sera noté id. On notera en général une permutation par un tableau :

$$s = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ s(1) & s(2) & s(3) & \ldots & s(n) \end{pmatrix}$$

Par exemple le groupe $\mathcal{S}_2$ possède 2 éléments : id et $t = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$; le groupe $\mathcal{S}_3$ possède 6 éléments : l'identité et les cinq permutations : $\tau_{23} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \tau_{13} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ Le tableau de la loi de groupe de $\mathcal{S}_3$ est :

$\circ$	id	τ_{12}	τ_{23}	τ_{13}	ρ_1	ρ_2
id	id	τ_{12}	τ_{23}	τ_{13}	ρ_1	ρ_2
τ_{12}	τ_{12}	id	ρ_1	ρ_2	τ_{23}	τ_{13}
τ_{23}	τ_{23}	ρ_2	id	ρ_1	τ_{13}	τ_{12}
τ_{13}	τ_{13}	ρ_1	ρ_2	id	τ_{12}	τ_{23}
ρ_1	ρ_1	τ_{13}	τ_{12}	τ_{23}	ρ_2	id
ρ_2	ρ_2	τ_{23}	τ_{13}	τ_{12}	id	ρ_1

On voit en particulier que $\mathcal{S}_3$ n'est pas commutatif.

Sur ces deux exemples on peut facilement définir le *signe* d'une permutation : $\varepsilon(id) = +1$ et $\varepsilon(t) = -1$ pour $\mathcal{S}_2$ et ensuite $\varepsilon(id) = \varepsilon(\rho_1) = \varepsilon(\rho_2) = +1$ et $\varepsilon(\tau_{12}) = \varepsilon(\tau_{23}) = \varepsilon(\tau_{13}) = -1$ pour $\mathcal{S}_3$. On vérifie facilement que ε est un homomorphisme de groupes (à valeurs dans le groupe à deux éléments $\{+1, -1\}$).

Pour étudier les groupes $\mathcal{S}_n$, commençons par y définir des éléments particulièrement simples.

Définition: Un *m-cycle* ou *cycle de longueur m* dans $\mathcal{S}_n$ est une permutation s de l'ensemble $E := \{1, \ldots, n\}$ qui laisse fixes $n - m$ éléments et permute circulairement les autres. Plus précisément, il existe un sous-ensemble à m éléments $I = \{i_1, \ldots, i_m\}$ de E tel que : si $i \notin I$ alors $s(i) = i$ mais $s(i_k) = i_{k+1}$ (pour $k = 1, \ldots, m-1$) et $s(i_m) = i_1$. L'ensemble I s'appelle le *support* du cycle.

Une *transposition* est un cycle de longueur 2.

Nous noterons $s = (i_1, i_2, \ldots, i_m)$ le cycle décrit dans la définition. Une transposition ayant pour support $\{i, j\}$ sera aussi notée τ_{ij} (ce qui est cohérent avec la notation déjà utilisée pour les éléments de $\mathcal{S}_2$ et $\mathcal{S}_3$).

Exemple : l'élément $t \in \mathcal{S}_2$ est une transposition, tout comme $\tau_{12}, \tau_{13}, \tau_{23} \in \mathcal{S}_3$. Les éléments $\rho_1, \rho_2 \in \mathcal{S}_3$ sont des 3-cycles. Par contre la permutation $s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ n'est pas un cycle. On peut vérifier que la permutation $s' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 7 & 5 & 1 & 6 & 4 \end{pmatrix}$ est un cycle de longueur 5 et de support $\{1, 3, 7, 4, 5\}$, c'est-à-dire que $s' = (1, 3, 7, 4, 5)$.

THÉORÈME: *Toute permutation se décompose de manière unique (à l'ordre près) en produit de cycles dont les supports sont deux à deux disjoints.*

Démonstration: On utilise une récurrence sur l'entier n, l'affirmation étant claire pour $n \leq 3$ (puisque toutes les permutations sont alors des cycles). Supposons donc l'énoncé démontré pour les permutations de k éléments avec $k < n$ et considérons $s \in \mathcal{S}_n$. En regardant la suite $1, s(1), s^2(1) \ldots$ on voit qu'il existe un plus petit entier $m \geq 1$ tel que $s^m(1) = 1$ (on n'exclut pas que $m = 1$). Définissons l'ensemble $I := \{1, s(1), s^2(1) \ldots, s^{m-1}(1)\}$ et le m-cycle $r := (1, s(1), s^2(1) \ldots, s^{m-1}(1))$; alors la permutation $t := sr^{-1}$ laisse fixe les éléments de I et pour $i \notin I$ on a $t(i) = s(i)$. La restriction de t à $J := \{1, \ldots, n\} \backslash I$ est donc une permutation des éléments de J que nous notons s'. Comme $card(J) < n$ on sait (par l'hypothèse de récurrence) que $s' = s'_1 \ldots s'_r$ avec s'_i des cycles de J à supports disjoints. Définissons $s_i \in \mathcal{S}_n$ par $s_i(j) = s'_i(j)$ si $j \in J$ et $s_i(j) = j$ si $j \notin I$; on voit qu'alors on a $t = s_1 \ldots s_r$ et par conséquent $s = s_1 \ldots s_r r$. Ceci prouve l'existence de la décomposition en cycles ; pour l'unicité on observe que le cycle r est uniquement déterminé par s et que par hypothèse de récurrence $s'_1, \ldots, s'_r$ (et par conséquent $s_1, \ldots, s_r$) sont uniques. □

Voyons comment on obtient en pratique cette décomposition sur un exemple : Prenons la permutation $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 5 & 1 & 2 & 4 \end{pmatrix}$. On choisit un premier élément disons 1 et on calcule ses images successives par ρ : on a $\rho(1) = 3$, $\rho^2(1) = \rho(3) = 7$, $\rho^3(1) = \rho(7) = 4$, $\rho^4(1) = \rho(4) = 5$ et $\rho^5(1) = \rho(5) = 1$ et on obtient ainsi un premier cycle s' qui est le 5-cycle dans l'exemple précédant le théorème. On prend alors un autre élément qui n'est pas dans le suppport de s', par exemple 2 et on recommence : $\rho(2) = 6$, $\rho^2(2) = \rho(6) = 2$. on obtient ainsi la décomposition $\rho = s'\tau_{26}$.

Cette décomposition est très utile pour calculer l'ordre d'une permutation (si vous n'avez jamais vu la notion de PPCM – plus petit commun multiple– consultez le chapitre 5) :

PROPOSITION: *Soit s une permutation qui se décompose en le produit de r cycles à supports disjoints de longueurs $m_1, \ldots, m_r$, alors l'ordre de la permutation s est égal au* PPCM$(m_1, \ldots, m_r)$.

Démonstration: Démontrons d'abord que si la permutation s est un m-cycle, elle a pour ordre m : il suffit de le faire pour le cycle $s = (1, 2, \ldots, m)$. Or, si $i > m$ on a $s(i) = i$ et

donc $s^m(i) = i$; si maintenant $1 \leq i \leq m$ on a $s^m(i) = s^i(s^{m-i}(i)) = s^i(m) = s^{i-1}(1) = i$ donc au total $s^m = id$. Par ailleurs si $1 \leq k \leq m-1$ alors $s^k(1) = k+1 \neq 1$ donc $s^k \neq id$; ainsi l'ordre de s est bien m.

Dans le cas général où $s = s_1 \dots s_r$ avec s_i cycles de longueurs m_i à supports disjoints, notons $N := \text{PPCM}(m_1, \dots, m_r)$. Observons que, comme les s_i commutent, on a $s^k = s_1^k \dots s_r^k$ et que, d'après l'unicité de la décomposition en cycles on a $s^k = id$ si et seulement si $s_1^k = \dots = s_r^k = id$ donc si et seulement si l'ordre de s_i (c'est-à-dire m_i) divise k donc si et seulement si N divise k. □

Exemples : considérons les deux permutations suivantes dans $\mathcal{S}_{10}$:

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 10 & 6 & 8 & 9 & 3 & 1 & 7 & 2 & 5 \end{pmatrix}, \; t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 & 10 & 9 \end{pmatrix}$$

alors les décompositions en cycles de s et t s'écrivent $s = (1,4,8,7)(2,10,5,9)(3,6)$ et $t = (1,2,3,4,5)(6,7,8)(9,10)$ et donc $ordre(s) = PPCM(4,4,2) = 4$ et $ordre(t) = PPCM(5,3,2) = 30$.

PROPOSITION: *Tout cycle peut s'écrire comme produit de transpositions et donc toute permutation peut s'écrire comme produit de transpositions.*

Démonstration: Quitte à changer de notation il suffit de montrer que le cycle $s = (1,2,\dots,m)$ s'écrit comme produit de transpositions. Or considérons le produit $s' = \tau_{12}\tau_{23}\dots\tau_{i,i+1}\dots\tau_{m-1,m}$ on vérifie que $s'(m) = \tau_{12}\tau_{23}\dots\tau_{m-2,m-1}(m-1) = \dots = \tau_{12}\tau_{23}\dots\tau_{i,i+1}(i+1) = \dots = \tau_{12}(2) = 1$ et que si $i \leq m-1$ alors $s'(i) = \tau_{12}\tau_{23}\dots\tau_{i,i+1}(i) = \tau_{12}\tau_{23}\dots\tau_{i-1,i}(i+1) = i+1$ et finalement on a bien $s = s'$, ce qui achève la preuve. □

Remarque : la décomposition en produit de transpositions n'est pas du tout unique mais la parité du nombre de transposition ne change pas comme on pourra le vérifier à l'aide de la notion suivante.

Définition: Le *signe* d'une permutation $s \in \mathcal{S}_n$ est défini par le produit :

$$\varepsilon(s) = \prod_{1 \leq i < j \leq n} \frac{s(j) - s(i)}{j - i}$$

Il est aisé de vérifier que $\varepsilon(s) \in \{+1, -1\}$ et que le signe d'une transposition est -1 ; la principale propriété est la suivante :

PROPOSITION: *Le signe est un homomorphisme de $\mathcal{S}_n$ vers $\{+1,-1\}$. Son noyau (l'ensemble des permutations paires que l'on notera $\mathcal{A}_n$) est un sous-groupe de cardinal $\frac{n!}{2}$.*

Démonstration: Pour montrer la première propriété, on calcule le signe du produit de deux permutations s, t :

$$\varepsilon(st) = \prod_{1 \leq i < j \leq n} \frac{st(j) - st(i)}{j - i} = \prod_{1 \leq i < j \leq n} \left(\frac{st(j) - st(i)}{t(j) - t(i)} \right) \left(\frac{t(j) - t(i)}{j - i} \right) =$$

$$= \prod_{1 \leq i < j \leq n} \frac{s(j) - s(i)}{j - i} \prod_{1 \leq i < j \leq n} \frac{t(j) - t(i)}{j - i} = \varepsilon(s)\varepsilon(t)$$

Le signe d'une transposition τ est -1 ; considérons l'application $s \mapsto s\tau$. C'est une application de $\mathcal{A}_n$ vers $\mathcal{S}_n \setminus \mathcal{A}_n$ qui est injective (car $s\tau = s'\tau$ entraîne $s = s'$) et surjective (car $(s\tau)\tau = s$) donc bijective. Ainsi $n! = card(\mathcal{S}_n) = card(\mathcal{A}_n) + card(\mathcal{S}_n \setminus \mathcal{A}_n) = 2card(\mathcal{A}_n)$. □

Remarque : on voit donc $\varepsilon(s) = +1$ si s est le produit d'un nombre pair de transpositions et $\varepsilon(s) = -1$ si s est le produit d'un nombre impair de transpositions. Plus généralement un cycle de longueur m aura donc un signe $(-1)^{m+1}$, ce qui donne une méthode de calcul du signe d'une permutation connaissant sa décomposition en cycles.

3.4 STRUCTURE D'ANNEAU ET STRUCTURE DE CORPS.

Définition: Un *anneau* est la donnée d'un ensemble A et de deux lois de composition $+$ (addition) et $*$ (Multiplication) telles que :

(i) $(A, +)$ est un groupe commutatif (dont on note l'élément neutre $0 = 0_A$).

(ii) La loi $*$ est associative.

(iii) La loi $*$ possède un élément neutre (qu'on notera $1 = 1_A$)

(iv) La loi $*$ est distributive par rapport à l'addition :

$$\forall x, y, z \in A,\ x * (y + z) = (x * y) + (x * z) \ \text{ et } \ (y + z) * x = (y * x) + (z * x)$$

Si de plus la loi $*$ est commutative on dit que l'anneau A est commutatif.

Remarquons que l'on a toujours $x * 0 = 0 * x = 0$ dans un anneau ; en effet $x * 0 = x * (0 + 0) = x * 0 + x * 0$ et donc (la loi $+$ est une loi de groupe) $x * 0 = 0$.

Définition: Un *corps* est un anneau tel que :

(v) Tout élément $x \in A \setminus \{0_A\}$ possède un inverse.

Convention : Un anneau (ou un corps) est donc un triplet $(A, +, *)$, l'ensemble A s'appelle l'ensemble *sous-jacent* à l'anneau ; toutefois on parle souvent de l'anneau A en sous-entendant les lois $+$ et $*$ quand il est clair dans le contexte de quelles lois il s'agit.

Exemples : Nous étudierons tout spécialement l'anneau des entiers relatifs $(\mathbf{Z}, +, \times)$; ce n'est pas un corps car les seuls éléments de $\mathbf{Z}$ possédant un inverse pour la multiplication sont $+1$ et -1. Les corps les plus importants que nous étudierons sont le corps des nombres rationnels $\mathbf{Q}$, le corps des nombres réels $\mathbf{R}$ et le corps des nombres complexes $\mathbf{C}$. Un nombre rationnel peut bien sûr s'écrire comme une fraction $\frac{a}{b}$ avec $a \in \mathbf{Z}$ et $b \in \mathbf{Z} \setminus \{0\}$ avec la règle $\frac{a}{b} = \frac{a'}{b'}$ si $ab' = a'b$; l'addition et la multiplication sont définis par $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. Nous verrons aussi que, si K désigne $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$, l'ensemble des polynômes à coefficients dans K, que l'on note $K[X]$, muni de l'addition et de la multiplication naturelles, forme un anneau qui possède beaucoup de propriétés communes avec $\mathbf{Z}$. Tous ces anneaux sont commutatifs.

L'ensemble des matrices 2×2 à coefficients réels (voir chapitre 7) muni des lois :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

forme un anneau qui n'est pas commutatif ; par exemple :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Règles de calcul dans un anneau :
(distibutivité généralisée) $x \sum_{i=1}^{n} y_i = \sum_{i=1}^{n} xy_i$
Attention : dans un anneau, il n'est pas vrai en général que lorsque $x \in A \setminus \{0\}$ on ait $xy = xz \Rightarrow y = z$; par exemple $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix}$ mais $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix}$
Si l'anneau est commutatif : $(xy)^n = x^n y^n$
L'expression de la puissance n-ème d'une somme est souvent utile :

THÉORÈME: *(Formule du binôme de Newton) Soient a, b deux éléments d'un anneau commutatif et soit n un entier ≥ 1, on a la formule :*

$$(a+b)^n = \sum_{p=0}^{n} C_n^p a^p b^{n-p}$$

où $C_n^p = \frac{n!}{p!(n-p)!}$ est le nombre de parties à p éléments dans un ensemble à n éléments.

A cause de cette formule, les coefficients C_n^p sont aussi appelés *coefficients binômiaux.* Les premiers exemples de cette formule s'écrivent :

$$(a+b)^1 = a+b,\ (a+b)^2 = a^2+2ab+b^2,\ (a+b)^3 = a^3+3a^2b+3ab^2+b^3$$

$$(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4,\ (a+b)^5 = a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5$$

Démonstration: La démonstration se fait par récurrence sur le nombre n : la formule est évidente pour $n = 0$ ou $n = 1$, on la suppose donc vraie pour l'entier n, pour tout a, b et on cherche à en déduire la formule pour l'entier $n+1$.

On a : $(a+b)^{n+1} = (a+b)(a+b)^n$ qui d'après l'hypothèse de récurrence vaut :

$$(a+b)\sum_{p=0}^{n} C_n^p a^p b^{n-p} = \sum_{p=0}^{n} C_n^p a^{p+1} b^{n-p} + \sum_{p=0}^{n} C_n^p a^p b^{n-p+1},$$

cette dernière expression est égale à :

$$a^{n+1} + \sum_{h=1}^{n} (C_n^h + C_n^{h-1}) a^h b^{n+1-h} + b^{n+1}$$

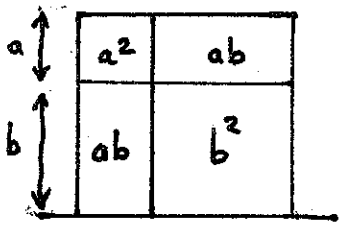
et, si on se rappelle que $C_n^h + C_n^{h-1} = C_{n+1}^h$ celle-ci vaut :

$$\sum_{h=0}^{n+1} C_{n+1}^h a^h b^{n+1-h}$$

ce qui est bien la formule de Newton pour l'entier $n+1$. □

Remarque : L'hypothèse que l'anneau est commutatif ne peut pas être enlevée (dans un anneau non commutatif, en général $ba^p b^{n-p}$ n'est égal à $a^p b^{n+1-p}$ comme le montre l'exemple des matrices $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ puisque $(A+B)^2 = \begin{pmatrix} 3 & 6 \\ 3 & 6 \end{pmatrix}$ mais $A^2 + 2AB + B^2 = \begin{pmatrix} 4 & 7 \\ 1 & 5 \end{pmatrix}$.

Exercice : Le dessin suivant fournit une illustration de la formule $(a+b)^2 = a^2+2ab+b^2$ en décomposant un carré de côté $a+b$ en deux carrés de côtés a et b et deux rectangles de longueur b et largeur a.



Donner une illustration de la formule $(a+b)^3 = a^3+3a^2b+3ab^2+b^3$ en décomposant un cube de coté $a+b$ en deux cubes de côtés a et b, trois parallélipipèdes d'arêtes a, a et b et trois parallélipipèdes d'arêtes a, b et b.

Un peu d'histoire :

Les notions de groupes et corps ont tiré leur première illustration spectaculaire du problème de la "résolution des équations polynomiales". On connait depuis le lycée la résolution de $a+bx+cx^2 = 0$ à l'aide de la fonction racine carrée $\sqrt{}$; au XVIème siècle, Cardan (également inventeur du système d'articulation mécanique portant son nom) a donné des formules pour résoudre $a+bx+cx^2+dx^3 = 0$ à l'aide des fonctions $\sqrt{}$ et $\sqrt[3]{}$; son élève Ferrari (aucun rapport connu avec Enzo) a ensuite donné des formules pour résoudre $a+bx+cx^2+dx^3+ex^4 = 0$ à l'aide des fonctions $\sqrt{}$, $\sqrt[3]{}$ et $\sqrt[4]{}$. Les mathématiciens ont longtemps cherché à résoudre ainsi les équations de degré ≥ 5 avant que Abel (1802-29) et Galois (1811-32) ne montrent que cela est impossible. Par exemple les solutions de $x^5 - x + 1 = 0$ ne peuvent pas s'exprimer à l'aide de $\sqrt{}$, $\sqrt[3]{}$, $\sqrt[4]{}$ et $\sqrt[5]{}$. Ces propriétés des équations de degré 3,4,5, etc sont liées aux propriétés des groupes S_3, S_4, S_5 etc. La théorie de Galois (à l'université Paris 7) s'étudie en maîtrise (M1) de mathématiques.

Galois Evariste (1811–1832)

CHAPITRE 4 LE CORPS DES RÉELS R ET DES COMPLEXES C

Les nombres "réels" ont été ainsi baptisés car on pensait que ce sont ceux qui permettaient de décrire les phénomènes physiques. Il est vrai que tout le calcul différentiel, et donc toute la mécanique classique repose sur la notion de nombre réel (même si cela n'est pas explicite chez Newton et Leibniz). Les nombres réels ont donc été utilisés très tôt bien que la démonstration de leurs propriétés et surtout de leur existence (du point de vue mathématique!) date du siècle dernier. Nous n'aborderons donc pas cet aspect et renvoyons aux traités classiques pour une description de $\mathbf{R}$ *par les coupures de Dedekind ou les classes d'équivalence de suites de Cauchy (Voir par exemple l'ouvrage de Dixmier cité en bibliographie). Quant aux nombres complexes, même les mathématiciens ont mis longtemps à accepter leur emploi (ils se sont longtemps appelés nombres imaginaires tant leur existence était sujette à doute). Néanmoins ils sont assez faciles à construire à partir des nombres réels et s'avèrent aussi utiles que les réels, y compris dans les autres sciences comme la physique.*

4.1 NOMBRES RÉELS.

La nécessité de considérer des nombres plus généraux que les nombres rationnels apparaît déjà avec l'absence de solution à l'équation $x^2 = 2$*, plus généralement l'existence de suite de nombres rationnels (ou de points d'une droite) "ayant l'air de converger" vers un point mais ne convergeant pas vers un nombre rationnel (ou un point commensurable) conduit à l'introduction des nombres réels que nous définirons ici de manière axiomatique, i.e. sans démontrer leur existence. Nous introduisons aussi la notion de limite –déjà abordée en terminale– qui est fondamentale dans toute l'analyse : les nombres réels permettent de nombreux procédés "infinitésimaux" ou de "passage à la limite". Ceci nous permet aussi de traiter précisément et rigoureusement le développement décimal des nombres réels : il est classique de représenter un nombre réel sous forme de développement décimal* $x = \pm a_0, a_1 a_2 a_3 \dots a_n \dots$ *avec* $a_0 \in \mathbf{N}$ et $a_i \in \{0,1,2,3,4,5,6,7,8,9\}$*. Par exemple :*

$$\pi = 3,14159265358979323846264338327950288419716939937510582097494459230 78\dots$$

Mais si on cherche à définir un nombre réel comme une telle suite on trouve quelques difficultés ; considérons par exemple le "nombre" $x := 0,99999\dots9\dots$*, il est raisonnable de penser que* $10x = 9,99999\dots9\dots$ *et aussi que* $10x - x = 9$ *et donc* $x = 1$ *; la multiplication est assez difficile à définir sur les développements décimaux.*

Une notion fondamentale sur les réels est celle d'ordre ; l'ensemble des réels est muni d'une addition et d'une multiplication qui en font un corps ; la relation d'ordre pour être utile doit être compatible avec ces opérations, plus précisément elle doit vérifier les règles suivantes :

(i) Pour tous x, y, z réels, $x \leq y \Rightarrow x + z \leq y + z$

(ii) Pour tous x, y réels, pour tout a réel positif $x \leq y \Rightarrow ax \leq ay$

On peut aussi en déduire :

(iii) $0 < x \leq y \Rightarrow 0 < \frac{1}{y} \leq \frac{1}{x}$

(iv) $x \leq y \Rightarrow -x \geq -y$ et $\forall x,\ x^2 \geq 0$

Un corps satisfaisant ces règles est appelé un *corps ordonné.*

A ces règles il faut rajouter une propriété qui formalise une intuition :

Définition: Un corps ordonné est dit *archimédien* si pour tout $x > 0$ et $y > 0$ il existe un entier $n \geq 1$ tel que $nx = x + \ldots + x > y$ (ici 0 désigne l'élément neutre).

Autrement dit, une quantité, aussi petite soit-elle, ajoutée suffisamment de fois à elle-même dépasse n'importe quelle quantité donnée. Par exemple le groupe $(\mathbf{Z}, +)$ est bien sûr archimédien, de même que $(\mathbf{Q}, +)$; les réels forment aussi un corps archimédien :

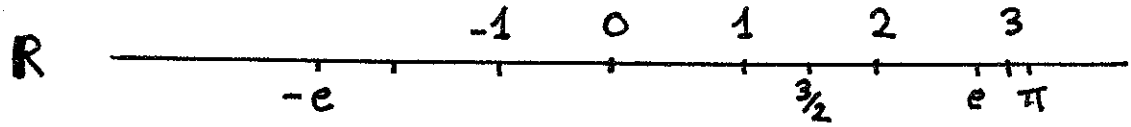
CARACTÉRISATION : *Le corps $(\mathbf{R}, +, \times, \leq)$ contient le corps des rationnels, est un corps totalement ordonné archimédien et vérifie la propriété dite des intervalles emboités :*

Soit $I_n = [a_n, b_n]$ une suite décroissante d'intervalles fermés bornés non vides alors $\bigcap_{n \in \mathbf{N}} I_n$ est non vide (c'est-à-dire : il existe $x \in \mathbf{R}$ tel que pour tout n on ait $x \in I_n$).

Un élément de ce corps s'appelle un nombre réel.

Ainsi, $\mathbf{R}$ est caractérisé par le fait d'être un corps (il y a une addition et une multiplication avec les "bonnes" propriétés) d'être totalement ordonné (ce qui le différencie de $\mathbf{C}$), archimédien et enfin la dernière propriété le différencie de $\mathbf{Q}$.

La représentation la plus usuelle des réels est celle des points d'une droite, nous la supposons connue.



La relation d'ordre permet aussi de définir la distance entre deux réels et donc de dire si deux réels sont proches :

Définition: La *valeur absolue* d'un nombre réel x est $\max\{x, -x\}$ et se note $|x|$. La distance entre deux réels x et y est $|x - y|$.

La valeur absolue d'un nombre est donc toujours positive. Rappelons les deux propriétés bien connues et fondamentales de la valeur absolue :

THÉORÈME: *(i)* $|xy| = |x||y|$

(ii) (inégalité triangulaire) $|x + y| \leq |x| + |y|$

Démonstration: Laissée en exercice (ou voir les cours au lycée). □

La deuxième inégalité s'appelle triangulaire (bien qu'il n'y ait pas ici de vrai triangle : les points sont situés sur une droite) ; en effet, si l'on désigne par $d(x, y)$ la distance entre deux nombres réels x et y, on peut aussi exprimer l'inégalité (ii) sous la forme $d(a, c) \leq d(a, b) + d(b, c)$

Remarque : l'inégalité $|x - a| \leq b$ équivaut à $a - b \leq x \leq a + b$. Ainsi les ensembles du type $\{x \in \mathbf{R} \mid |x - a| \leq b\}$ (respectivement $\{x \in \mathbf{R} \mid |x - a| < b\}$) sont des intervalles fermés (respectivement ouvert) aux deux extrémités. Inversement un intervalle $[a, b]$ peut aussi s'écrire $[a, b] = \{x \in \mathbf{R} \mid |x - \frac{a+b}{2}| \leq \frac{b-a}{2}\}$.

La notion de distance permet de formaliser l'idée de "tendre vers un point". Intuitivement une suite u_n tend vers $\ell \in \mathbf{R}$ si u_n est de plus en plus proche de ℓ quand n augmente

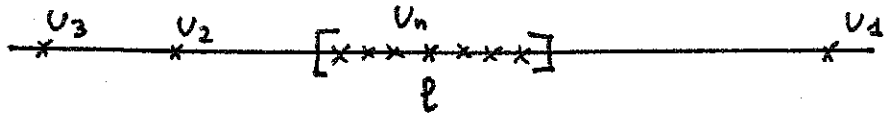
ou encore si u_n se retrouve dans n'importe quel intervalle autour de ℓ, aussi petit soit-il, dès que n est assez grand.

Définition: Une suite u_n de nombres réels (ou rationnels) *tend vers* 0 si elle vérifie :

$$\forall \varepsilon > 0, \exists n_0 \in \mathbf{N}, n \geq n_0 \Rightarrow |u_n| \leq \varepsilon$$

Une suite u_n de nombres réels (ou rationnels) *tend vers* ℓ si $u_n - \ell$ tend vers 0. On dit aussi que u_n *converge* vers ℓ ou que ℓ est la *limite* de la suite u_n, ce que l'on note $\lim u_n = \ell$.

Autrement dit : soit n'importe quel (petit) intervalle centré en ℓ, alors tous les termes de la suite, sauf un nombre fini sont situés dans l'intervalle.



Exemples : La suite $u_n = \frac{1}{n+1}$ a pour limite $\ell = 0$; montrons cela directement à partir de la définition. Soit $\varepsilon > 0$, le corps $\mathbf{R}$ étant archimédien, il existe un entier n_0 plus grand que $1/\varepsilon$; soit alors $n \geq n_0$ alors $0 < 1/n \leq 1/n_0 \leq \varepsilon$ donc $|u_n| \leq \varepsilon$. Par contre, la suite $u_n = (-1)^n$ ne converge pas (si ℓ est différent de ± 1 un intervalle suffisamment petit centré en ℓ ne contient aucun terme u_n et si $\ell = \pm 1$, un nombre infini de termes éviteront un petit intervalle centré en ℓ).

THÉORÈME: *Soit u_n une suite convergente vers une limite ℓ, supposons que pour tout n on ait $u_n > a$ (respectivement $u_n \geq a$) alors $\ell \geq a$.*

Démonstration: Raisonnons par l'absurde et supposons que $\ell < a$. Choisissons un intervalle I contenant ℓ mais pas a (par exemple $I = \{x \in \mathbf{R} \mid |x - \ell| \leq \frac{a-\ell}{2}\}$) alors les éléments de la suite u_n sont dans I (sauf un nombre fini d'entre eux) mais pour tous les éléments x de I on a $x < a$ d'où une contradiction. □

Remarque : Si $u_n := \frac{1}{n+1}$ on a $u_n > 0$ mais $\lim u_n = 0$; on ne peut donc pas garder les inégalités strictes en passant à la limite.

Exploitons maintenant la propriété des intervalles emboités :

THÉORÈME: *(i) Tout sous-ensemble de $\mathbf{R}$ non vide et majoré admet une borne supérieure. Tout sous-ensemble de $\mathbf{R}$ non vide et minoré admet une borne inférieure.*

(ii) Toute suite croissante et majorée (respectivement décroissante et minorée) est convergente.

(Ce résultat est très important mais on peut omettre la démonstration assez technique)

Démonstration: (i) Soit E un ensemble non vide majoré de réels on va construire des intervalles emboités $I_n = [a_n, b_n]$ tels que l'intersection contienne au plus un point (et donc exactement un point) qui sera la borne supérieure. Soit $e \in E$ et M un majorant de E, on pose $I_0 := [e, M]$. Pour construire I_1 on distingue deux cas : si $\frac{M+e}{2}$ est un majorant de E on choisit $a_1 = e$ et $b_1 = \frac{M+e}{2}$; sinon il existe dans E un élément qui est plus grand que $\frac{M+e}{2}$ et on choisit a_1 égal à cet élément et $a_2 = M$. En itérant ce procédé on obtient une suite décroissante d'intervalles $I_n = [a_n, b_n]$ tels que b_n soit un majorant de E, tel que a_n

soit un élément de E et tel que $|b_{n+1} - a_{n+1}| \leq \frac{|a_n - b_n|}{2}$ donc $|a_n - b_n| \leq \frac{(M-e)}{2^n}$. Montrons maintenant qu'il ne peut y avoir qu'un seul point dans l'ensemble $S := \bigcap_{n\in\mathbf{N}} I_n$ et que c'est la borne supérieure. Tout d'abord soit $s, t \in S$ alors ces deux nombres appartiennent aussi I_n donc, pour tout n on a $|s-t| \leq \frac{(M-e)}{2^n}$ donc $|s-t| = 0$ et $s = t$. Par construction la suite des a_n comme celle des b_n converge vers s. Comme tous les b_n sont des majorants de E, s est aussi un majorant de E ; comme tous les a_n sont des éléments de E, on a que s est le plus petit majorant.

(ii) Considérons $E = \{u_n \mid n \in \mathbf{N}\}$, c'est un ensemble majoré par hypothèse donc il admet une borne supérieure ℓ. Montrons que u_n converge vers ℓ. Soit $\varepsilon > 0$, la définition de la borne supérieure entraîne qu'il existe un élément de E, disons u_{n_0} tel que $\ell - \varepsilon \leq u_{n_0} \leq \ell$; mais alors comme u_n est croissante on a pour tout $n \geq n_0$ les inégalités $\ell - \varepsilon \leq u_{n_0} \leq u_n \leq \ell$ et donc $|u_n - \ell| \leq \varepsilon$, ce qui prouve bien que u_n tend vers ℓ.

□

Notation : on sait que si $x \in \mathbf{R}$ alors il existe un unique entier relatif m tel que $m \leq x < m+1$ on l'appelle la *partie entière* de x et on le note $[x]$. Par exemple $[\pi] = 3$ et $[-3/2] = -2$.

APPLICATION: DÉVELOPPEMENT DÉCIMAL D'UN NOMBRE RÉEL.

On appelle bien sûr *chiffre* un élément de $C := \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (on pourrait d'ailleurs faire les mêmes raisonnements dans une autre base que 10). Considérons une suite $a_1, a_2, a_3, \ldots$ de chiffres et associons lui la suite de nombres rationnels

$$s_n := \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_n}{10^n}$$

qu'on notera aussi $s_n := 0, a_1 a_2 \ldots a_n$.

1ère étape : la suite s_n converge vers un réel x appartenant à l'intervalle $[0, 1]$.

Démonstration: En effet la suite s_n est croissante (car $s_{n+1} = s_n + a_{n+1} 10^{-n-1} \geq s_n$) et majorée par 1 :

$$s_n \leq 9\left(\frac{1}{10} + \frac{1}{10^2} + \ldots + \frac{1}{10^n}\right) = 1 - \frac{1}{10^n} \leq 1$$

enfin comme $0 \leq s_n \leq 1$ on a bien $0 \leq x = \lim s_n \leq 1$. □

On introduit naturellement la notation : $x = 0, a_1 a_2 a_3 \ldots a_n \ldots$ et on appelle cette écriture *un développement décimal* de x. Deux questions se posent naturellement :

1) Est-ce-que tout nombre réel admet un développement décimal? Autrement dit tout nombre $x \in [0, 1]$ est-il limite d'une suite s_n?

2) Un tel développement est-il unique?

(en remarquant que $x - [x] \in [0, 1[$, on peut se borner à considérer les réels dans l'intervalle $[0, 1[$).

2ème étape : Tout nombre réel $x \in [0, 1[$ admet un développement décimal $x = 0, a_1 a_2 a_3 \ldots a_n \ldots$.

Démonstration: Fabriquons la suite $a_1 := [10x]$, $a_2 := [10^2x - 10a_1] \ldots a_n := [10^n x - 10^{n-1}a_1 - \ldots - 10a_{n-1}]$ et ensuite $s_n := \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_n}{10^n}$. Comme $0 \leq x < 1$ on a $0 \leq 10x < 10$ donc $a_1 \leq 10x < a_1 + 1$ donc $a_1 \leq 9$ et l'entier a_1 est bien un chiffre. Par ailleurs $s_1 = \frac{a_1}{10} \leq x < \frac{a_1}{10} + \frac{1}{10}$ donc $0 \leq x - s_1 < \frac{1}{10}$. Montrons par récurrence que $a_n \leq 9$ (i.e. l'entier a_n est un chiffre) et $0 \leq x - s_n < \frac{1}{10^n}$; ce qui prouvera que $x = 0, a_1 a_2 a_3 \ldots a_n \ldots$. Si $0 \leq x - s_n < \frac{1}{10^n}$ alors $0 \leq 10^{n+1}x - 10^{n+1}s_n = 10^{n+1}x - 10^n a_1 - \ldots - 10a_n < 10$ donc $0 \leq a_{n+1} < 10$ et donc a_{n+1} est bien un chiffre. Ensuite $a_{n+1} \leq 10^{n+1}x - 10^n a_1 - \ldots - 10a_n < a_{n+1} + 1$ donc $0 \leq x - \frac{a_1}{10} - \ldots \frac{a_n}{10^n} - \frac{a_{n+1}}{10^{n+1}} < 10^{-n-1}$; ce qu'il fallait démontrer. □

3ème étape : Le développement décimal $x = 0, a_1 a_2 a_3 \ldots a_n \ldots$ existe et est unique si l'on impose la condition :

$$\forall N \in \mathbf{N},\ \exists n > N,\ a_n \neq 9$$

Autrement dit on exclut les développements du type $0, a_1 a_2 \ldots a_n 9999 \ldots 9 \ldots$ (avec $a_n \neq 9$) que l'on remplace par $0, a_1 a_2 \ldots (a_n + 1)0 \ldots$

Par exemple 0,1234567899999...=0,12345679

Démonstration: Supposons $x = 0, a_1 a_2 a_3 \ldots a_n \ldots = 0, b_1 b_2 b_3 \ldots b_n \ldots$ et disons $a_1 = b_1, \ldots, a_{r-1} = b_{r-1}$ mais $a_r < b_r$. On obtient facilement $(b_r - a_r)10^{-r} = 0, 0 \ldots 0 a_{r+1} \ldots - 0, 0 \ldots 0 \ldots b_{r+1} \ldots$. Le membre de gauche vaut au moins 10^{-r} car $b_r - a_r \geq 1$ mais

$$0, 0 \ldots 0 a_{r+1} \ldots = \frac{a_{r+1}}{10^{r+1}} + \ldots + \frac{a_n}{10^n} \ldots < \frac{9}{10^{r+1}} + \ldots + \frac{9}{10^n} \ldots = 10^{-r}$$

L'inégalité est stricte car il existe des $a_n < 9$ par hypothèse ; on obtient donc une contradiction du type $10^{-r} < 10^{-r}$.

□

Remarque : on peut observer que les seuls nombres réels qui admettent "deux" développements sont exactement les nombres rationnels "décimaux" $x = \frac{m}{10^n}$

APPLICATION: RACINE n-IÈME D'UN RÉEL POSITIF

Soit $a \in \mathbf{R}_+$ et n un entier ≥ 1 alors il existe un unique $x \in \mathbf{R}_+$ tel que $x^n = a$. On l'appelle la *racine n-ième* de a et on le note $x = \sqrt[n]{a}$.

Démonstration: L'unicité est facile car si $0 < x < x'$ alors $0 < x^n < x'^n$. Pour montrer l'existence, considérons $S := \{y \in \mathbf{R}_+ \mid y^n \geq a\}$ alors S est non vide et minoré (par exemple par 0) donc possède une borne inférieure que nous baptisons x. Comme pour tout $y \in S$ on a $y^n \geq a$ on en déduit $x^n \geq a$. Si on avait $x^n < a$ alors pour $e > 0$ (mais très petit) on en déduirait $(x+e)^n < a$ (on donne une démonstration de ce fait ci-dessous) et donc $x + e \notin S$. Mais alors S ne contient aucun point de l'intervalle $[x, x + e]$ ce qui contredit le fait que x est la borne inférieure de S.

Il nous reste à montrer la "continuité" de la fonction $y \mapsto y^n$, c'est-à-dire à montrer que si y est très proche de x alors y^n est très proche de x^n. Nous verrons au chapitre 13 une méthode générale pour démontrer cela ; donnons néanmoins une démonstration directe (où l'on pourra supposer que $x > 0$).

Vérifions par récurrence que pour $0 \leq h \leq \frac{x}{2}$ on a $(x+h)^n \leq x^n + (2^n-1)hx^{n-1}$ en effet $(x+h)^{n+1} = (x+h)(x+h)^n \leq (x+h)(x^n+(2^n-1)hx^{n-1}) = x^{n+1} + hx^n(2^n + (2^n-1)\frac{h}{x}) \leq x^{n+1} + (2^{n+1}-1)hx^n$ d'où la propriété annoncée. On en déduit que si $x \leq y \leq x + \frac{\varepsilon}{2^n x^{n-1}}$ alors $x^n \leq y^n \leq x^n + \varepsilon$; ce qu'il fallait démontrer. □

4.2 NOMBRES COMPLEXES.

La nécessité d'étendre le corps des réels se fait sentir si on cherche à résoudre des équations comme $x^2 + 1 = 0$. Si on ajoute formellement un "nombre" i tel que $i^2 + 1 = 0$ alors on peut déjà résoudre les équations de degré 2 ; en effet pour étudier $ax^2 + bx + c = 0$ on introduit $\Delta := b^2 - 4ac$ et si $\Delta \geq 0$ les racines sont $\frac{-b \pm \sqrt{\Delta}}{2}$ alors que si $\Delta < 0$ il n'y a pas de racines réelles mais on peut "fabriquer" des racines par la formule $\frac{-b \pm i\sqrt{-\Delta}}{2}$. Ceci suggère d'étudier les "nombres" de la forme $x + iy$; il est clair ce que doivent être la somme et le produit de tels expressions ; nous prendrons ce guide pour définir les nombres complexes.

Définition: Un *nombre complexe* s'écrit $z = x + iy$ avec $x, y \in \mathbf{R}$; l'ensemble des nombres complexes se note $\mathbf{C}$ et est en bijection avec $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$.

Définition: Soient $z = x + iy$ et $z' = x' + iy'$ deux nombres complexes.

On appelle partie *réelle* (respectivement *imaginaire*) de $z = x + iy$ le nombre réel x (respectivement le nombre y).

On définit la somme de deux nombres complexes par :

$$z + z' := (x + x') + i(y + y')$$

On définit le produit de deux nombres complexes par :

$$zz' := (xx' - yy') + i(yx' + xy')$$

Le *conjugué* de z est $\bar{z} := x - iy$. Le *module* de z est $|z| := \sqrt{x^2 + y^2} = \sqrt{z\bar{z}}$.

Remarque : on peut considérer un nombre réel x comme un nombre complexe en l'écrivant $x = x + i0$; un nombre réel est égal à son conjugué, la somme et le produit de deux nombres réels coïncident avec leur somme et produit comme nombres complexes, le module d'un nombre réel est sa valeur absolue.

THÉORÈME: *(i) L'ensemble $\mathbf{C}$ muni de la somme et de le multiplication est un corps commutatif. L'inverse d'un nombre complexe non nul $z = x + iy$ est donné par*

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{x}{x^2 + y^2} - i\frac{y}{x^2 + y^2}$$

(ii) La conjugaison complexe $z \mapsto \bar{z}$ est un isomorphisme de corps, c'est-à-dire que $\bar{1} = 1$, $\overline{x + y} = \bar{x} + \bar{y}$ et $\overline{xy} = \bar{x}\bar{y}$. La conjugaison est *involutive*, c'est-à-dire que $\bar{\bar{x}} = x$.

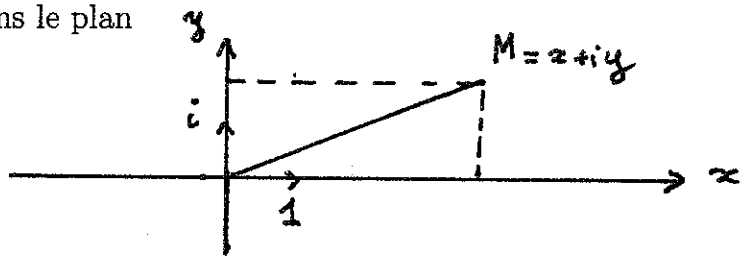
Démonstration: La vérification des axiomes d'un anneau ne pose aucune dificulté et est laissée au lecteur. Vérifions l'existence d'un inverse pour tout nombre complexe non

nul. Soit $z = x + iy \in \mathbf{C}^*$. Comme $|z|^2 = z\bar{z} = x^2 + y^2 \in \mathbf{R}^*$ on peut définir $z' := z/|z|^2$ et clairement $zz' = 1$. La deuxième partie de l'énoncé se vérifie par un calcul direct. □

Exemples : on vérifiera (en appliquant directement la définition) que :

$$(1+i)^2 = 2i,\ (1+i\sqrt{3})^3 = -8,\ \frac{(1+2i)}{(2+3i)} = \frac{8+i}{13},\ \left(\frac{-1+i\sqrt{3}}{2}\right)^2 + \left(\frac{-1+i\sqrt{3}}{2}\right) + 1 = 0$$

Donnons maintenant des représentations géométriques des nombres complexes :
Représentation dans le plan



On utilise la bijection $\mathbf{C} \to \mathbf{R}^2$ donnée par $z \mapsto (Re(z), Im(z))$ et on représente le nombre complexe z par le point $M = M(z)$ d'abscisse $Re(z)$ et d'ordonnée $Im(z)$. Le module $|z|$ est la distance entre O et M.

On peut définir la distance comme pour les nombres réels par $d(z, z') := |z - z'|$, on a alors :

THÉORÈME: *(i)* $|zz'| = |z||z'|$.
(ii) (inégalité triangulaire) Pour tous nombres complexes z, z' on a $|z+z'| \leq |z| + |z'|$.

Démonstration: (i) est immédiat car $|zz'|^2 = zz'\overline{zz'} = z\bar{z}z'\bar{z}' = |z|^2|z'|^2$. La preuve de (ii) est plus subtile : considérons la fonction de variable réelle $P(t) := |z + tz'|^2 = |z|^2 + t(z'\bar{z} + z\bar{z}') + t^2|z'|^2$; c'est un polynôme du second degré avec au plus une racine (aucune racine si z'/z n'est pas réel) donc $\Delta := (z'\bar{z} + z\bar{z}')^2 - 4|z|^2|z'|^2 \leq 0$ ou encore $|(z'\bar{z} + z\bar{z}')| \leq 2|z||z'|$. Nantis de cette inégalité, développons :

$$|z + z'|^2 = |z|^2 + z'\bar{z} + z\bar{z}' + |z'|^2 \leq |z|^2 + 2|z||z'| + |z'|^2 = (|z| + |z'|)^2$$

Ce qui donne bien l'inégalité cherchée. □

Remarque : Cette fois, l'inégalité (ii) peut se traduire par $d(M, M') \leq d(M, M'') + d(M'', M')$ qui est l'inégalité sur un triangle : la somme des longueurs de deux des côtés est plus grande que la longueur du troisième côté.

Ayant la notion de distance, on peut définir quand un point est proche d'un autre en particulier la notion de limite (on répète ici la définition par commodité) :

Définition: Une suite z_n de nombres complexes *tend vers* 0 si elle vérifie :

$$\forall \varepsilon > 0, \exists n_0 \in \mathbf{N}, n \geq n_0 \Rightarrow |z_n| \leq \varepsilon$$

Une suite z_n de nombres complexes *tend vers* $\ell \in \mathbf{C}$ si $z_n - \ell$ tend vers 0. On dit aussi que z_n *converge* vers ℓ ou que ℓ est la *limite* de la suite z_n, ce que l'on note $\lim u_n = \ell$.

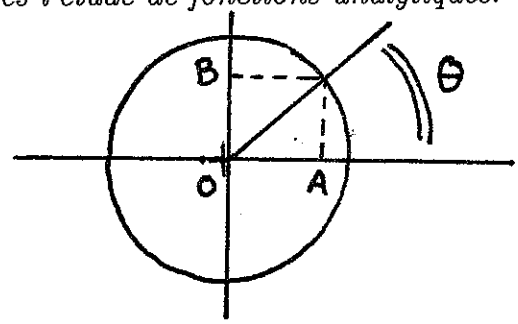
Autrement dit : soit n'importe quel (petit) disque de centre ℓ, alors tous les termes de la suite, sauf un nombre fini sont situés dans le disque.

THÉORÈME: *Soit z_n une suite de nombres complexes ;* $\lim z_n = z$ *équivaut à* $\lim Re(z_n) = Re(z)$ *et* $\lim Im(z_n) = Im(z)$.

Démonstration: En remplaçant z_n par $z_n - z$ il suffit de prouver que $\lim z_n = 0$ si et seulement si $\lim Re(z_n) = 0$ et $\lim Im(z_n) = 0$. Mais comme $|Re(z_n)| \leq |z_n|$, $|Im(z_n)| \leq |z_n|$ et $|z_n| \leq |Re(z_n)| + |Im(z_n)|$ ceci est clair. □

Exemple : Si $|\alpha| < 1$ alors la suite $z_n := \alpha^n$ converge vers 0 car $|z_n|$ converge vers 0. Cependant si $\alpha = e^{i\pi\sqrt{2}}$ la suite α^n ne converge pas, bien que $\lim |\alpha^n| = 1$.

On admet ici l'existence des fonctions sinus et cosinus telles que si l'angle θ sur la figure ci-dessous est donné en radians (un tour complet vaut 2π, un demi-tour π, un quart de tour $\frac{\pi}{2}$) alors $OA = \cos(\theta)$ et $OB = \sin(\theta)$. Il y a là une difficulté qui sera levée en deuxième année après l'étude de fonctions analytiques.



On voit donc que tout nombre complexe peut s'exprimer comme :

$$z = r(\cos(\theta) + i\sin(\theta))$$

avec $r = |z| \in \mathbf{R}_+$ et $\theta \in \mathbf{R}$. Ou encore : si $z = a + ib \neq 0$ avec a, b réels, alors il existe un "angle" (i.e. un réel) θ tel que $\cos(\theta) = a/\sqrt{a^2+b^2}$ et $\sin(\theta) = b/\sqrt{a^2+b^2}$. Le nombre θ n'est déterminé qu'à un multiple entier de 2π près, il s'appelle l'argument de z et se note $Arg(z)$ (si on veut être tout-à-fait rigoureux, on doit dire *un* argument). Plus précisément :

THÉORÈME: *(i) Supposons $r(\cos(\theta)+i\sin(\theta)) = r'(\cos(\theta')+i\sin(\theta'))$ avec $r, r' \in \mathbf{R}_+^*$ alors $r = r'$ et il existe $n \in \mathbf{Z}$ tel que $\theta = \theta' + 2\pi n$.*

(ii) $|\bar{z}| = |z|$, $Arg(zz') = Arg(z) + Arg(z') + 2\pi n$ et $Arg(\bar{z}) = -Arg(z) + 2\pi n$.

Démonstration: (i) En prenant les modules on arrive à $|r| = |r'|$ et comme r et r' sont positifs on a bien $r = r'$. On en tire $\cos(\theta) = \cos(\theta')$ et $\sin(\theta) = \sin(\theta')$ ce qui entraîne $\theta = \theta' + 2\pi n$. (ii) La formule donnant le module du conjugué est claire, celle donnant son argument découle de celle donnant l'argument d'un produit : $Arg(z\bar{z}) = Arg(z) + Arg(\bar{z}) +$

$2k\pi$ doit être un multiple de 2π car $z\bar{z}$ est réel et positif. La formule donnant l'argument d'un produit se déduit des formules classiques $\cos(y+y') = \cos(y)\cos(y') - \sin(y)\sin(y')$ et $\sin(y+y') = \cos(y)\sin(y') + \sin(y)\cos(y')$; en effet si $z = r(\cos(y) + i\sin(y))$ et $z' = r'(\cos(y') + i\sin(y'))$ alors le produit zz' vaut :

$$\begin{aligned} zz' =& rr'\{(\cos(y)\cos(y') - \sin(y)\sin(y')) + i(\cos(y)\sin(y') + \sin(y)\cos(y'))\} \\ =& rr'\{\cos(y+y') + i\sin(y+y')\} \end{aligned}$$

d'où $Arg(zz') = y + y' + 2n\pi$. □

La meilleure façon de décrire les cordonnées polaires à travers les nombres complexes est d'introduire la fonction exponentielle d'une variable complexe :

Définition: On pose $e^{i\theta} := \cos(\theta) + i\sin(\theta)$ et plus généralement si $z = x + iy$:

$$e^z = e^{x+iy} := e^x\cos(y) + ie^x\sin(y)$$

Exemples :

$$e^{2\pi i} = 1,\ e^{\pi i} = -1,\ e^{\frac{2\pi i}{3}} = \frac{-1+i\sqrt{3}}{2},\ e^{\log 2 + \frac{\pi i}{2}} = 2i.$$

THÉORÈME: *(i) Tout nombre complexe z non nul peut s'écrire $z = e^{z'}$ pour un certain nombre complexe z'.*

(ii) $e^z = e^{z'}$ équivaut à $Re(z) = Re(z')$ et $Im(z) = Im(z') + 2\pi n$.

(iii) $e^{z+z'} = e^z e^{z'}$

(iv) $\overline{e^z} = e^{\bar{z}}$

Démonstration: (i) provient du fait que tout point du cercle $|z| = 1$ peut s'écrire $z = \cos(\theta) + i\sin(\theta)$ pour un $\theta \in \mathbf{R}$ et du fait que l'exponentielle réelle est surjective de $\mathbf{R}$ sur $\mathbf{R}_+^*$.

(ii) est une redite du théorème précédent.

(iii) On sait que $e^{x+x'} = e^x e^{x'}$ pour $x, x' \in \mathbf{R}$; il suffit donc de vérifier que $e^{i(y+y')} = e^{iy}e^{iy'}$ pour $y, y' \in \mathbf{R}$. Mais cette dernière égalité équivaut à la formule donnée pour l'argument d'un produit de deux nombres complexes.

(iv) $e^{x-iy} = e^x(\cos(-y) + i\sin(-y)) = e^x(\cos(x) - i\sin(x)) = \overline{e^{x+iy}}$. □

On peut utiliser cette représentation pour déterminer les racines n-ième d'un nombre complexe :

THÉORÈME: *Soit $z_0 \in \mathbf{C}^*$ et n un entier ≥ 1, alors il existe n nombres complexes tels que $z^n = z_0$.*

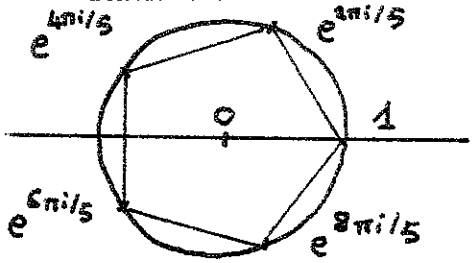
Plus explicitement si $z_0 = r_0 e^{i\theta}$ alors les n racines n-ième sont :

$$z = \sqrt[n]{r_0}e^{i\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)} \text{ avec } k \in \{0, 1, \ldots, n-1\}$$

Démonstration: Cherchons z sous la forme $re^{i\alpha}$; l'équation $z^n = z_0$ équivaut alors à $r^n e^{in\alpha} = r_0 e^{i\theta}$ ou encore à $r^n = r_0$ et $n\alpha = \theta + 2k\pi$ (avec $k \in \mathbf{Z}$), d'où l'énoncé. □

En particulier les racines n-ièmes de 1 s'appellent *racine de l'unité* ; elles forment les sommets d'un polygone régulier à n côtés :

Racines 5-ième de l'unité :



Ce dernier théorème est en fait un cas un peu particulier du célèbre théorème de D'Alembert-Gauss (il fut énoncé pour la première fois par D'Alembert mais démontré rigoureusement plus tard par Gauss) :

THÉORÈME: *(D'Alembert-Gauss). Soit $P(X)$ un polynôme à coefficients complexes, si P est non constant, alors il possède une racine, i.e. $\exists \alpha \in \mathbf{C},\ P(\alpha) = 0$.*

Tout polynôme P de degré $d \geq 1$ s'écrit :

$$P(X) = a_0(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_d)$$

avec $a_0 \in \mathbf{C}^*$ et $\alpha_1, \alpha_2, \dots, \alpha_d \in \mathbf{C}$ (non nécessairement distincts).

Démonstration: Nous admettrons la première partie. Le fait que la première partie de l'énoncé entraîne la seconde est un résultat assez simple d'algèbre que nous démontrerons dans le chapitre 6 sur les polynômes. □

Une autre application classique de la représentation exponentielle est la formule de Moivre :

$$\cos(nx) + i\sin(nx) = (\cos(x) + i\sin(x))^n$$

où $x \in \mathbf{R}$ et $n \in \mathbf{Z}$.

Démonstration: On sait que $e^{inx} = (e^{ix})^n$ d'où la formule.

C'est un exercice classique, en utilisant la formule du binôme de Newton et la formule $\cos^2(x) + \sin^2(x) = 1$ d'en tirer une expression de $\cos(nx)$ et $\sin(nx)/\sin(x)$ comme polynôme en $\cos(x)$. Faisons-le pour $\cos(nx)$:

$(\cos(x) + i\sin(x))^n = \sum_{k=0}^{n} C_n^k (i\sin(x))^k (\cos(x))^{n-k}$ donc $\cos(nx)$ vaut :

$$Re\{(\cos(x) + i\sin(x))^n\} = \sum_{h=0}^{[\frac{n}{2}]} C_n^{2h}(-1)^h(\sin(x))^{2h}(\cos(x))^{n-2h} =$$

$$\sum_{h=0}^{[\frac{n}{2}]} C_n^{2h}(-1)^h(1 - \cos^2(x))^h(\cos(x))^{n-2h}$$

Ainsi $\cos(nx) = P_n(\cos(x))$ avec $P_n(X) = \sum_{h=0}^{[\frac{n}{2}]} C_n^{2h}(-1)^h(1 - X^2)^h X^{n-2h}$. Par exemple $P_2(X) = 2X^2 - 1$, $P_3(X) = 4X^3 - 3X$ et $P_4(X) = 8X^4 - 8X^2 + 1$.

Ces formules permettent aussi d'exprimer $\cos^n(x)$ comme combinaison linéaire de $\cos(nx)$, $\cos((n-2)x)$,... Par exemple :

$$\cos^2(x) = \frac{\cos(2x)+1}{2},\ \cos^3(x) = \frac{\cos(3x)+3\cos(x)}{4} \text{ et } \cos^4(x) = \frac{\cos(4x)+4\cos(2x)+3}{8}$$

4.3 GÉOMÉTRIE ET NOMBRES COMPLEXES

Nous avons vu que les nombres complexes peuvent être représentés par des points du plan ; inversement les nombres complexes permettent une formulation élégante de nombreux problèmes de géométrie du plan. Nous donnons dans cette partie deux exemples de ce phénomène.

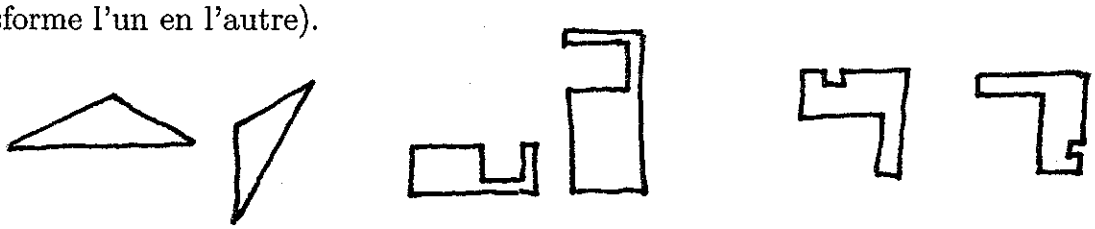
4.3.1 Similitudes du plan.

En géométrie comme en physique, on étudie toujours les transformations préservant les distances ou les formes (ou des quantités bien adaptées au problème que l'on veut traiter) ; on s'intéresse ici aux transformations du plan préservant les formes au sens suivant :

Définition: Une *similitude* est une application f du plan vers lui-même telle que, pour tout x, y dans le plan, $d(f(x), f(y)) = \lambda d(x, y)$, où $\lambda \in \mathbf{R}_+^*$ est une constante qui s'appelle le *rapport* de la similitude f. Une similitude de rapport 1 s'appelle une *isométrie.*

Exemples : une translation, une rotation (autour d'un point selon un angle donné), une symétrie (orthogonale par rapport à une droite), une homothétie sont des similitudes ; ce sont des isométries sauf les dernières.

Les figures suivantes sont semblables deux à deux (il existe une similitude du plan qui transforme l'un en l'autre).



Remarque : l'ensemble des similitudes forme un groupe ; l'application qui à une similitude associe son rapport est un homomorphisme de groupe à valeurs dans $\mathbf{R}_+^*$ et dont le noyau est constitué par le sous-groupe des isométries.

Les nombres complexes permettent une description simple des similitudes :

THÉORÈME: *L'ensemble des similitudes est décrit par les transformations de* $\mathbf{C}$ *dans* $\mathbf{C}$ *données par :*

$$z \mapsto az + b \text{ ou } z \mapsto a\bar{z} + b$$

où $a \in \mathbf{C}^*$ *et* $b \in \mathbf{C}$. *Ces transformations sont des isométries si et seulement si* $|a| = 1$.

Démonstration: Il est immédiat de vérifier que les transformations décrites sont des similitudes (de rapport $|a|$) ; pour la réciproque, quitte à remplacer f par $g(z) = (f(z) - f(0))/(f(1) - f(0))$, on peut supposer que $f(0) = 0$ et $f(1) = 1$. Ecrivons alors les deux conditions $|f(z) - f(0)| = |z - 0|$ et $|f(z) - f(1)| = |z - 1|$, on obtient : $|f(z)| = |z|$

et $|f(z)|^2 - 2Re\, f(z) + 1 = |z|^2 - 2Re\, z + 1$ d'où $Re\, f(z) = Re\, z$ et $|f(z)| = |z|$. On obtient ainsi que $\forall z \in \mathbf{C}$, $f(z) = z$ ou $\bar{z}$. Reste à voir que si, disons $f(z_0) = z_0$, pour un nombre complexe non réel, alors pour tout $z \in \mathbf{C}$ on a $f(z) = z$. On écrit bien sûr que $|f(z) - f(z_0)| = |z - z_0|$ donc $Re\,(f(z)\bar{z}_0) = Re\,(z\bar{z}_0)$. Or l'équation $Re\,(\bar{z}\bar{z}_0) = Re\,(zz_0)$ entraîne (puisque $\mathrm{Im}(z_0) \neq 0$) que $\mathrm{Im}(z) = 0$ donc dans tous les cas $f(z) = z$. □

Exemples. La rotation de centre l'origine et d'angle θ correspond à la multiplication par $a = e^{i\theta}$; l'application $z \mapsto \bar{z}$ correspond à la symétrie orthogonale par rapport à l'axe des abscisses.

4.3.2 Droites, cercles et transformations homographiques.

Commençons par exprimer dans le plan complexe l'équation d'une droite et d'un cercle. Si $z = x + iy$ (avec $x, y \in \mathbf{R}$) on sait que $x = \frac{z+\bar{z}}{2}$ et $y = \frac{z-\bar{z}}{2i}$; comme l'équation cartésienne d'une droite est de la forme $ax + by + c = 0$ (avec $a, b, c \in \mathbf{R}$ et a ou b non nul) on en tire, en terme de z, l'équation de la droite : $\frac{a-ib}{2}z + \frac{a+ib}{2}\bar{z} + c$ ou encore, en posant $\alpha = \frac{a+ib}{2}$, on obtient l'équation $\alpha\bar{z} + \overline{\alpha}z + c$. L'équation d'un cercle de centre β et de rayon r peut s'écrire $|z-\beta| = r$ ou encore en élevant au carré : $z\bar{z} + \overline{\beta}z + \beta\bar{z} + |\beta|^2 = r^2$. Réciproquement considérons l'équation $az\bar{z} + \overline{\beta}z + \beta\bar{z} + c = 0$ (où $\beta \in \mathbf{C}$ et $a, c \in \mathbf{R}$) ; si $a = 0$ on retrouve l'équation d'une droite (sauf si β est aussi nul, cas trivial qu'on écarte) ; si $a \neq 0$, on peut diviser par a l'équation et en tirer : $z\bar{z} + \frac{\overline{\beta}}{a}z + \frac{\beta}{a}\bar{z} + \frac{|\beta|^2}{a^2} = -\frac{c}{a} + \frac{|\beta|^2}{a^2} = \frac{-ca+|\beta|^2}{a^2}$. On a ainsi montré :

THÉORÈME: *L'ensemble des cercles et droites du plan complexe est décrit par des équations du type :*

$$az\bar{z} + \overline{\beta}z + \beta\bar{z} + c = 0$$

(où $\beta \in \mathbf{C}$ et $a, c \in \mathbf{R}$ non tous nuls). On obtient ainsi une droite si $a = 0$ et $\beta \neq 0$, un cercle si $a \neq 0$ et $ac < |\beta|^2$ (resp. un point et l'ensemble vide si $ac = |\beta|^2$ ou $ac > |\beta|^2$).

Il est clair que les similitudes préservent l'ensemble des droites et des cercles mais il y a des transformations beaucoup plus générales qui font cela :

Définition: On appelle *fonction homographique* toute transformation du type $z \mapsto \frac{az+b}{cz+d}$ où $ad - bc \neq 0$. On appelle *fonction anti-homographique* toute transformation du type $z \mapsto \frac{a\bar{z}+b}{c\bar{z}+d}$ où $ad - bc \neq 0$.

Il faut tout de suite observer que, si $c \neq 0$, la fonction $f(z) = \frac{az+b}{cz+d}$ n'est pas définie en $z = -\frac{d}{c}$; on dit que $-\frac{d}{c}$ est le *pôle* de f ; de même la fonction f n'atteint pas la valeur $\frac{a}{c}$ puisque $\frac{az+b}{cz+d} = \frac{a}{c}$ entraînerait $bd = ac$. Pour ne pas alourdir les énoncés, on sous-entend souvent ce fait. Par ailleurs la condition $ad - bc \neq 0$ est mise pour éviter les fonctions constantes ; en effet si $ad - bc = 0$ avec disons $c \neq 0$ alors $b = \frac{ad}{c}$ et donc $f(z) = \frac{az+\frac{ad}{c}}{cz+d} = \frac{a}{c}$. D'un autre coté considérons $g(z) = \frac{dz-b}{-cz+a}$, alors $f \circ g(z) = \frac{ad-bc}{ad-bc}z = z$ (si $ad - bc \neq 0$).

Exemples :
Les translations $f(z) = z + a$ sont des homographies.
Les homothéties $f(z) = \lambda z$ (avec $\lambda \in \mathbf{R}^*$) sont des homographies.

Les rotations $f(z) = \alpha z$ (avec $\alpha = e^{i\theta}$) sont des homographies.
La symétrie $f(z) = \bar{z}$ est une anti-homographie.
L'inversion $f(z) = 1/\bar{z}$ est une anti-homographie.

Les quatre premiers exemples sont des similitudes et préservent donc toutes les formes ; ce n'est pas le cas de l'inversion, mais elle a tout de même la propriété remarquable de transformer une droite D en une droite (si $0 \in D$) ou un cercle (si $0 \notin D$) et de transformer un cercle C en une droite (si $0 \in C$) ou un cercle (si $0 \notin C$). Nous allons voir que c'est une propriété générale des (anti-)homographies.

THÉORÈME: *Les fonctions homographiques (resp. anti-homographiques) préservent l'ensemble des droites et des cercles. Une droite D est transformée en cercle par f, si le pôle de f n'est pas situé sur la droite D, ou en droite, si le pôle de f est situé sur la droite D. Un cercle C est transformé en cercle par f, si le pôle de f n'est pas situé sur le cercle C, ou en droite, si le pôle de f est situé sur le cercle C.*

Démonstration: Nous vérifions seulement que les (anti-)homographies transforment cercles et droites en cercles et droites et admettrons que ce sont les seules transformations ayant cette propriété. Une première démonstration est fournit par un calcul formel : par exemple l'équation $uz\bar{z} + \overline{\beta}z + \beta\bar{z} + v = 0$ se transforme par $z \mapsto \frac{az+b}{cz+d}$ en

$$(u|a|^2 + \overline{\beta}a\bar{c} + \beta\bar{a}c + v|c|^2)z\bar{z} + \overline{(u\bar{a}b + \overline{\beta}b\bar{c} + \beta\bar{a}d + v\bar{c}d)}z$$

$$+(u\bar{a}b + \overline{\beta}b\bar{c} + \beta\bar{a}d + v\bar{c}d)\bar{z} + (u|b|^2 + \overline{\beta}bd + \beta\bar{b}d + v|d|^2) = 0.$$

Une deuxième démonstration consiste à écrire $f(z) = \frac{az+b}{cz+d}$ comme composée de transformations simples ; il reste alors à vérifier la propriété pour transformations simples. Or, si $c \neq 0$ on a $f(z) = \frac{bc-ad}{c(cz+d)} + \frac{a}{c}$, donc si l'on pose $g(z) = cz + d, i(z) = 1/z$ et $h(z) = \frac{bc-ad}{c}z + \frac{a}{c}$ alors $f = h \circ i \circ g$. Il suffit donc de vérifier la propriété pour i ou encore pour l'inversion $z \mapsto /\bar{z}$, ce que nous avons déjà fait. □

Remarque : on a omis de préciser dans l'énoncé que si $\frac{a}{c}$ appartient à une droite ou un cercle, ce point n'est jamais dans l'image.

Exemple d'application : on veut transformer le demi-plan $\mathcal{H} := \{z \in \mathbf{C} \mid Im(z) > 0\}$ en le disque $\mathcal{D} := \{z \in \mathbf{C} \mid |z| < 1\}$. La transformation $f(z) = \frac{z-i}{z+i}$ transforme l'axe des imaginaires en l'axe réel et l'axe réel en le cercle de centre O et de rayon 1 et $\mathcal{H}$ en $\mathcal{D}$.

D'Alembert Jean (1717-1783)