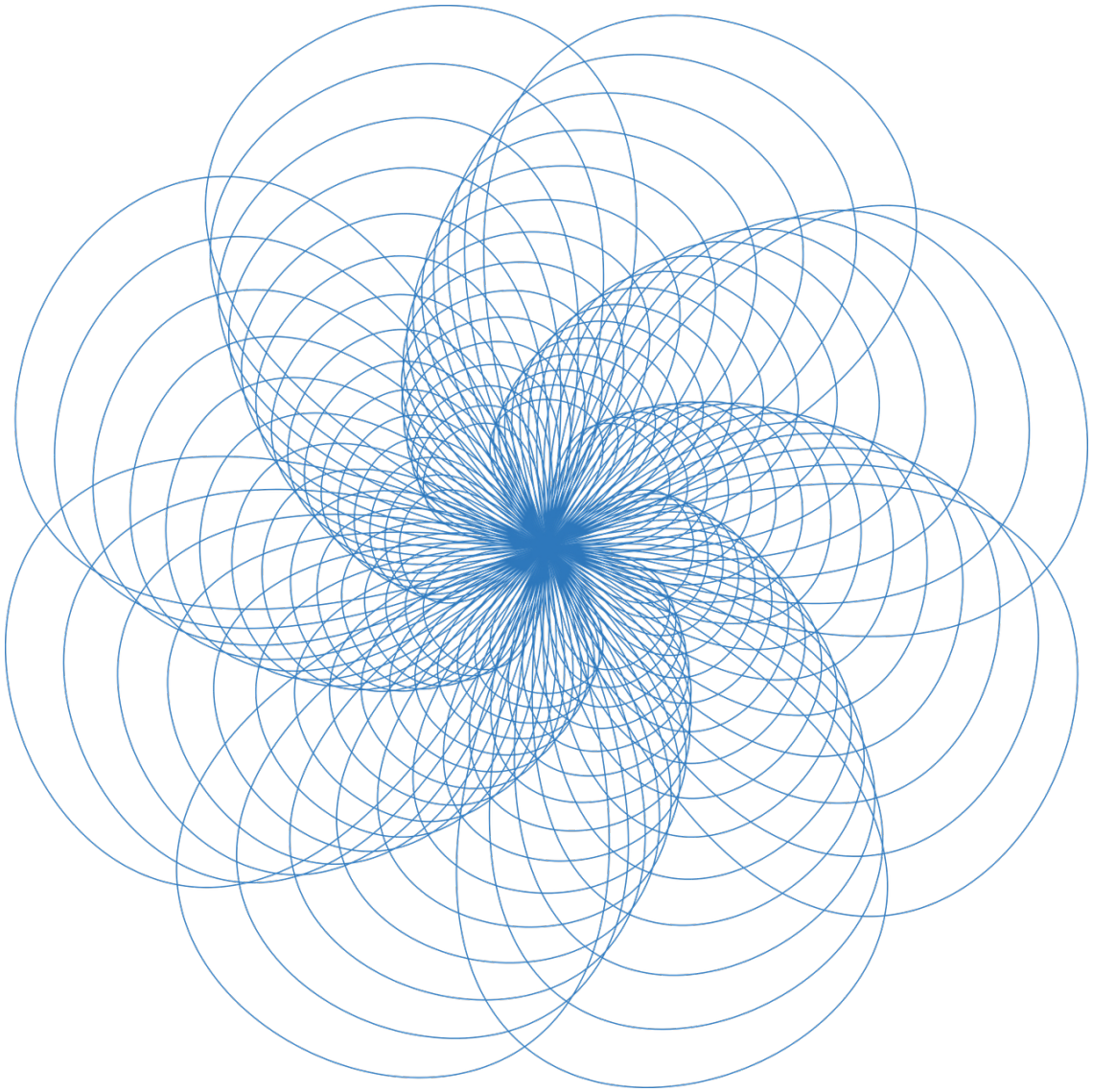
Mathématiques

Licence



Université Jean-François Champollion
Année 2022 - 2025

Table des matières

I — Raisonnements

Soit $\mathscr{P}$ une proposition et n un entier naturel.

Disjonctions & Conjonctions :

Si $\mathscr{P}$ est une disjonction de la forme $\mathscr{A} \vee \mathscr{B}$, il suffit alors de supposer **l'une des deux propriétés fausse** et de montrer que l'autre est vraie.

Si $\mathscr{P}$ est une conjonction de la forme $\mathscr{A} \wedge \mathscr{B}$, il faut simplement prouver $\mathscr{A}$ et $\mathscr{B}$.

Raisonnements par l'absurde :

Raisonner par l'absurde revient à utiliser le principe du **tiers exclu**, ie l'axiome qui affirme que la proposition ci-dessous est toujours vraie:

$$\mathscr{P} \vee \neg\mathscr{P}$$

Donc si on veut prouver $\mathscr{P}$, on peut alors simplement montrer que $\neg\mathscr{P} \implies \bot$ avec "$\bot$" comme notation d'une contradiction logique. Alors on peut conclure d'après l'axiome du tiers exclu que $\mathscr{P}$ est vraie.

Raisonnement par Analyse / Synthèse :

Le raisonnement par Analyse / Synthèse permet de déterminer **l'ensemble des solutions d'un problème**, il s'effectue en deux étapes, tout d'abord l'étape d'analyse suppose qu'une telle solution existe, alors on circonscrit son existence à des propriétés connues qu'elle vérifie nécessairement. Cette étape permet de "cerner" les solutions en question. Si les propriétés sont assez contraignantes, alors on peut même prouver **l'unicité**, ie l'ensemble des solutions se réduit à un singleton.

Puis lors de l'étape de synthèse, on considère un objet vérifiant les propriétés qu'on a utilisé lors de l'étape d'analyse, et on **vérifie** que cet objet est bien une solution au problème initial. C'est lors de cette étape qu'on prouve bien **l'existence** de solutions. Si aucun des objets circonscrits par l'analyse ne conviennent, le problème n'a alors pas de solutions.

Implications & Équivalences :

Si $\mathscr{P}$ est une implication de la forme $\mathscr{A} \implies \mathscr{B}$, on a les équivalences suivantes:

$$\mathscr{P} \iff \neg\mathscr{A} \vee \mathscr{B} \iff \neg\mathscr{B} \implies \neg\mathscr{A}$$

Aussi en raisonnant **par l'absurde**, il suffit alors de prouver:

$$\mathscr{A} \wedge \neg\mathscr{B} \implies \bot$$

Il est important de noter que l'implication **n'est pas une opération associative**, en effet, soit une propriété de la forme:

$$\mathscr{A}_1 \implies \mathscr{A}_2 \implies \mathscr{A}_3$$

Alors de manière générale, on a:

$$\mathscr{A}_1 \implies (\mathscr{A}_2 \implies \mathscr{A}_3) \not\iff (\mathscr{A}_1 \implies \mathscr{A}_2) \implies \mathscr{A}_3$$

Prouver une équivalence revient à prouver une **double implication** dans la majorité des cas.

Cas particulier : Si $\mathscr{P}$ est de la forme $A_1 \iff A_2 \iff \cdots \iff \mathscr{A}_{n-1} \iff \mathscr{A}_n$, il suffit alors de montrer:

$$\mathscr{A}_1 \implies \mathscr{A}_2 \implies \cdots \implies \mathscr{A}_{n-1} \implies \mathscr{A}_n \implies \mathscr{A}_1$$

Ainsi pour toute paire de $\mathscr{A}_i$, on a bien double implication entre les deux membres et donc la chaîne d'équivalence est démontrée.

Raisonnements par récurrence :

Soit $\mathscr{P}$ une propriété dépendante de n qu'on veut démontrer sur $[\![\alpha\ ;\ +\infty]\!]$, soit k en entier fixé supérieur à α, démontrer $\mathscr{P}$ par récurrence simple revient à utiliser **l'axiome de récurrence** (issu de la construction de $\mathbb{N}$) ci-dessous:

$$\Big[\mathscr{P}_\alpha \wedge \big[\mathscr{P}_k \implies \mathscr{P}_{k+1}\big]\Big] \implies \forall n \in \mathbb{N}\ ;\ \mathscr{P}_n$$

Si la propriété à prouver est plus complexe, on peut avoir besoin de récurrences d'une autre type, en effet si $\mathscr{P}$ dépend **des deux rangs précédents**, et on utilise alors une récurrence à deux pas qui s'exprime:

$$\Big[\mathscr{P}_\alpha \ \wedge\ \mathscr{P}_{\alpha+1} \wedge \big[\mathscr{P}_{k-1} \wedge \mathscr{P}_k \implies \mathscr{P}_{k+1}\big]\Big] \implies \forall n \in \mathbb{N}\ ;\ \mathscr{P}_n$$

Enfin pour le cas limite, si $\mathscr{P}$ dépends **d'exactement tout les rangs précédents**, alors on peut utiliser une récurrence forte qui s'exprime:

$$\Big[\mathscr{P}_\alpha \wedge\big[\mathscr{P}_{\alpha+1} \ \wedge\ \ldots\ \mathscr{P}_{k-1} \ \wedge\ \mathscr{P}_k \implies \mathscr{P}_{k+1}\big]\Big] \implies \forall n \in \mathbb{N}\ ;\ \mathscr{P}_n$$

Un dernier type de récurrence appelé **récurrence limitée** permet simplement d'utiliser la récurrence sur un intervalle entier fini, et donc on initialise et on prouve l'hérédité avec la contrainte de cette intervalle.

Remarque sur la récurrence forte :

Une telle récurrence forte ne nécessitera qu'une **unique** initialisation pour compléter l'hérédité.

D'un point de vue heuristique, il peut arriver d'engager une récurrence forte sur un problème qui n'aurait nécessité qu'une récurrence à p pas.
Ce cas précis reviendra alors, lors de l'étape d'hérédité, à **ne pas utiliser l'ensemble de l'hypothèse de récurrence**, et alors il faudra modifier le nombre d'initialisation à réaliser et l'intervalle de notre hypothèse de récurrence.

Admettons que $\mathscr{P}_\alpha$ soit vraie, supposons qu'elle soit vraie sur $[\![\alpha\ ;\ k]\!]$. Alors, on doit montrer que la propriété est vraie au rang $k+1$.

Alors, selon **le plus petit rang** nécessaire à compléter l'hérédité, on a:

Si on a besoin de $\mathscr{P}_k$ alors **on se ramène à une récurrence simple.**
Si on a besoin de $\mathscr{P}_{k-1}$ alors **on se ramène à une récurrence double.**
Si on a besoin de $\mathscr{P}_{k-2}$ alors **on se ramène à une récurrence triple.**
.....

Et donc, les initialisations et l'intervalle de notre hypothèse de récurrence changeront en conséquence et on remarque alors que si le plus petit rang nécessaire est $\mathscr{P}_{k-p}$, alors on se ramène nécessairement à une **récurrence à p pas**, avec p initialisations et l'hypothèse de récurrence qui commence à $\alpha+p$.

Une récurrence forte n'est alors qu'une récurrence qui nécessite des hypothèses sur **tout les rangs précédents.**

Récurrences imbriquées :

Soit $\mathscr{P}_{n,m}$ une propriété qui dépend **de deux variables entières**, alors on pourrait prouver $\mathscr{P}_{n,0}$ par récurrence et alors cela constituerait l'initialisation d'une récurrence imbriquée qui supposerait par exemple $\mathscr{P}_{n,k}$ vraie pour prouver $\mathscr{P}_{n,k+1}$.

I — Ensembles

Soit E, F et X trois ensembles quelconques. On note tout d'abord que l'intersection est prioritaire sur la réunion lors d'opérations sur les ensembles et que les deux opérations sont **distributives** l'une par rapport à l'autre.

Inclusion :

L'inclusion est une **relation d'ordre** sur l'ensemble des parties de E, et donc on en déduit qu'elle est **réflexive, transitive et antisymétrique**. Si l'inclusion est stricte, on parle de **sous-ensemble propre**.

Si $E \subseteq F$, on a:

$$E \cap F = E$$
$$E \cup F = F$$

Aussi, les opérations élémentaires préservent l'inclusion:

$$E \cap X \subseteq F \cap X$$
$$E \cup X \subseteq F \cup X$$

Complémentaire et de la différence :

Si $F \subseteq E$, alors F^c est l'ensemble qui contient tout les éléments de E qui **ne sont pas** dans F et on a définit alors **la différence ensembliste**:

$$E \setminus F = E \cap F^c$$

Par ailleurs, **les lois de De Morgan** nous donnent:

$$(E \cap F)^c = E^c \cup F^c$$
$$(E \cup F)^c = E^c \cap F^c$$

Cas particulier : On peut aussi définir l'opération de **différence symétrique** notée Δ qui permet d'obtenir tout les éléments qui appartiennent exactement à un seul des deux ensembles:

$$E \Delta F = (E \cup F) \setminus (E \cap F)$$

Produit cartésien :

Soit n une entier naturel, le produit cartésien des ensembles E_1, E_2, ... , E_{n-1}, E_n est l'ensemble des n-uplets de la forme $(e_1, e_2, \ldots, e_{n-1}, e_n)$ avec $e_i \in E_i$ pour $i \in [\![1\ ;\ n]\!]$. Il y a **unicité** de ces n-uplets.
Plus formellement, on note:

$$\prod_{i=1}^{n} E_i = \Big\{ (e_1, e_2, \ldots, e_{n-1}, e_n)\ ;\ e_1 \in E_1, e_2 \in E_2, \ldots, e_n \in E_n \Big\}$$

Cardinalité :

Supposons que E et F tout deux inclus dans X et ayant **un nombre fini d'éléments**. On a alors différentes propriétés:

$$\begin{aligned} |E \cup F| &= |E| + |F| - |E \cap F| \\ |E \times F| &= |E| \times |F| \\ |E^c| &= |X| - |E| \\ |\mathcal{P}_E| &= 2^{|E|} \end{aligned}$$

Partitions et recouvrements:

Soit $(P_i)_{i\in\mathbb{N}}$ une famille de parties **non vides et deux à deux disjointes** de E.
On dit que (P_i) est une **partition** de E si et seulement si:

$$\bigcup_{i\in\mathbb{N}} P_i = E$$

On remarque immédiatement deux partitions singulières:

- La famille contenant uniquement E qu'on appelle **partition grossière**.
- La famille contenant tout les singletons de E qui est la partition **la plus fine**.

On peut donc intuitivement parler de **finesse** d'une partition, en regard de la taille des parties de la famille.

On peut généraliser le concept de partitition à celui de **recouvrement**, alors E ne nécessite que d'être contenu par l'union des (P_i).

Algèbre de Boole :

On peut montrer que l'ensemble **ordonné** des parties de E muni de l'union, l'intersection, le complémentaires forment une **Algèbre de Boole**.

Cela signifie que la structure $(\mathcal{P}(E), \cup, \cap, X^c)$ vérifie les axiomes suivants:

- Les deux opérations binaires sont **associatives, commutatives et distributives l'une sur l'autre.**
- Les deux opérations binaires sont **idempotentes.**
- **L'élément neutre** pour l'union est l'ensemble vide, et pour l'intersection l'ensemble E.
- **L'élément absorbant** pour l'union est l'ensemble E, et pour l'intersection l'ensemble vide.

- Le complémentaire est **involutif**.
- L'intersection d'un élément et de son complémentaire est **vide**.
- L'union d'un élément et de son complémentaire est **l'ensemble tout entier**.
- Les **lois de De Morgan** sont vérifiées.

De manière analogue, en considérant $\{0, 1\}$ comme les valeurs de vérité d'une proposition, on a:

La structure $(\{0, 1\}, \vee, \wedge, \neg)$ est aussi une algèbre de Boole.

Cette structure est à la base de la logique formelle et vérifie les même axiomes que l'algèbre de l'ensemble des parties d'un ensemble.

I — Relations

Une **relation** entre des objets d'un ensemble est une propriété que vérifient ces objets **entre eux**.
Les relations sont des objets **fondamentaux** en mathématiques, elles sont entre autres des objets primitifs de la théorie des ensembles.

On appelle **arité** le nombre d'éléments mis en jeu par la relation.
Par exemple une relation d'arité 2 est appelée **relation binaire** et met en jeu deux éléments. On définit ainsi le cas général de relation **n-aire** qui met en jeu n éléments $x_1, x_2, \ldots, x_{n-1}, x_n$ et on note:

$$\mathscr{R}(x_1, x_2, \ldots, x_{n-1}, x_n)$$

Par abus de langage, on appelle **classe** un ensemble d'ensembles.
Formellement une classe n'est pas un ensemble mais un élément primitif de la théorie ZFC, mais ici on verra qu'on appelle classe des objets qui **sont** des ensembles.

Zoologie :

Il existe un grand nombre de relations très connues et élémentaires, par exemple:

- La relation d'appartenance à un ensemble
- La relation d'égalité
- La relation d'ordre
- La relation d'inclusion
- La relation de congruence
- La relation de parallélisme de deux droites du plan

On peut remarque que la relation d'appartenance à un ensemble est une relation binaire fondamentale, à la base de la théorie des ensembles.

Relations binaires :

Soit $x, y, z \in E$, une relation entre deux éléments peut vérifier plusieurs propriétés remarquables:

- **Réflexivité :** $\mathscr{R}(x, x)$
- **Irréflexivité :** $\not\mathscr{R}(x, x)$
- **Symétrie :** $\mathscr{R}(x, y) \implies \mathscr{R}(y, x)$
- **Antisymétrie :** $\mathscr{R}(x, y) \wedge \mathscr{R}(y, x) \implies x = y$

Elle peut aussi être **transitive**:

$$\mathscr{R}(x, y) \wedge \mathscr{R}(y, z) \implies \mathscr{R}(x, z)$$

On appelle aussi relation **totale** une relation telles si pour toute paire d'éléments, on a $\mathscr{R}(x, y) \vee \mathscr{R}(y, x)$.

Relations d'ordre :

Une **relation d'ordre** est une relation **réflexive, antisymétrique et transitive**. Elle induit un ordre sur l'ensemble E, qui peut potentiellement être **total**.

Des relations d'ordre très connues sont la relation $\leq$ sur les ensembles de nombres ou la relation $\subseteq$ sur l'ensemble des parties de E.

On appelle relation de **préordre** toute relation relation d'ordre qui n'est pas antisymétrique. Intuitivement, une relation de préordre est une relation d'ordre à "équivalence près" des éléments.

Relations d'équivalence :

Une **relation d'équivalence** est une relation **réflexive, symétrique et transitive**. Intuitivement, elle met en relation les éléments des ensembles qui sont "similaires".

Des relations d'équivalence très connues sont la relation $=$ et $\equiv$ sur les ensembles de nombres, ou encore la relation $\sim$ sur l'ensemble des fonctions.

Classes d'équivalence :

Soit $(E, \sim)$ un ensemble muni d'une relation d'équivalence.
Les **classes d'équivalence** de E par rapport à la relation $\sim$ sont alors les parties de E contenant des éléments en relation.

Soit $x \in E$, on définit alors la **classe d'équivalence** de x et on note $[x]$ l'ensemble:

$$[x] := \Big\{ \alpha \in E \ ; \ \alpha \sim x \Big\}$$

D'après les propriété de la relation, on a alors:

$$\boxed{x \sim y \iff [x] = [y]}$$

Et on appelle **représentant** de $[x]$ tout élément qui appartient à $[x]$.

Ensembles quotient :

L'ensemble des classes d'équivalence de E forme alors une **partition** de E, et on appelle **ensemble quotient**, ou encore **ensemble quotienté par la relation d'équivalence** l'ensemble:

$$E/\sim := \Big\{ [x] \in \mathcal{P}(E) \ ; \ x \in E \Big\}$$

C'est alors un ensemble de classes d'équivalences par rapport à la relation $\sim$.

Travailler avec l'ensemble quotient revient alors à ne pas distinguer les éléments équivalents entre eux.
On peut aussi créer des **structures** quotient, il suffit alors de quotienter une structure algébrique de telle sorte que les propriétés de structure soient conservées.

Quelques exemples connus de structures quotient:

- **L'anneau** $\mathbb{Z}/n\mathbb{Z} := (\mathbb{Z}/\sim, +, \times)$ **pour la relation** $a \sim b \iff a \equiv b[n]$
- **Le corps** $\mathbb{Q} := ((\mathbb{Z}\,;\, \mathbb{Z}\setminus\{0\})/\sim, +, \times)$ **pour la relation** $(a,b) \sim (c,d) \iff ad = bc$

I — Fonctions & Applications

On appelle **fonction** ou **application** des cas particulier de relation entre deux ensembles, soit f, g deux fonctions telles que:

$$\begin{aligned} f : E &\longrightarrow F & \qquad g : G &\longrightarrow H \\ x &\longmapsto f(x) & \qquad x &\longmapsto g(x) \end{aligned}$$

On note D_f le sous-ensemble de E tel que $f(x)$ existe, alors f est une **application** si et seulement si $E = D_f$ et on note alors $\mathscr{F}(E, F)$ l'ensemble des **applications** de E vers F.

Si $F \subseteq G$, alors on définit **la composée** $g \circ f$ par la fonction $h : x \in E \longmapsto g(f(x)) \in H$

Cas des suites :

Une suite à valeurs dans E n'est alors qu'un cas particulier en la forme d'une fonction $u : \mathbb{N} \longrightarrow E$, ce sont des objets d'étude trés importants en analyse et notamment en topologie. Dans le cas des suites on peut définir la notion de **suite extraite**, car si u_n est une suite dans E et k_n est **suite d'entiers croissante**, alors on définit une suite extraite de u_n par:

$$u \circ k : \mathbb{N} \longrightarrow E$$

C'est simplement les termes de la suite u_n dont on ne choisit que les termes d'indices donnés par k_n.

Graphe :

On définit **le graphe** de f comme suit:

$$G_f := \Big\{(x, f(x)) \in E \times F \ ; \ x \in E\Big\}$$

Intuitivement, c'est l'ensemble des points de l'espace d'arrivée qui sont sur la courbe de la fonction.

Restrictions & Prolongements :

On note $f|_A$ la restriction de **l'ensemble de départ** de f à une partie A de E.
On note $f|^B$ la restriction de **l'ensemble d'arrivée** de f à une partie B de F.

Soit $x \in D_f$, on appelle **prolongement** de f, l'application g telle que $D_f \subset D_g$ et $g(x) = f(x)$

Image directe :

On appelle **image directe** d'une partie A de E l'ensemble des images par f des éléments de A, ie:

$$f(A) := \Big\{f(x) \ ; \ x \in A\Big\}$$

L'image directe est compatible avec **certaines opérations ensemblistes**, plus précisément:

- $f(A \cap B) = f(A) \cap f(B)$
- $f(A \cup B) \subset f(A) \cup f(B)$

Image Réciproque :

On appelle **image réciproque** d'une partie B de F l'ensemble des antécédents par f des éléments de B, ie:

$$f^{-1}(B) := \Big\{x \in A \ ; \ f(x) \in B\Big\}$$

L'image réciproque est compatible avec **toutes les opérations ensemblistes**, plus précisément:

- $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$
- $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$

Injections :

L'application f est injective si et seulement si:

$$\forall x_1, x_2 \in E^2 \ ; \ f(x_1) = f(x_2) \implies x_1 = x_2$$

En particulier, il suffit de montrer que l'équation $f(x) = y$ admet **au maximum une solution dans E** pour montrer que f est injective.
Si $g \circ f$ est injective alors f est nécessairement injective.

Si E et F sont des ensembles finis, et que f est une injection, alors on a nécessairement $|E| \leq |F|$

Surjections :

L'application f est surjective si et seulement si:

$$\forall y \in F \ , \ \exists x \in E \ ; \ f(x) = y$$

En particulier, il suffit de montrer que l'équation $f(x) = y$ admet **au moins une solution dans E** pour montrer que f est surjective.
Si $g \circ f$ est surjective alors g est nécessairement surjective.

Si E et F sont des ensembles finis, et que f est une surjection, alors on a nécessairement $|F| \leq |E|$

Bijections :

L'application f est bijective si et seulement si elle est surjective et injective.
Dans ce cas, **une application réciproque** g existe et elle vérifie:

$$\begin{cases} f \circ g &= Id_F \\ g \circ f &= Id_E \end{cases}$$

Réciproquement, si il existe une application g telle que f soit inversible à gauche et à droite par g, alors f est bijective.

Intuitivement, les bijections sont exactement ***les applications inversibles à gauche et à droite*** *par une même application.*

Si f et g sont bijectives, alors $f \circ g$ est bijective et $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$

Equipotence :

Soit E et F deux ensembles quelconques.
Si il existe une bijection de E vers F, alors on dit que ces ensembles sont **équipotents**, et on a:

$$|E| = |F|$$

Cette définition du cardinal par les bijections permet de parler de cardinal d'un ensemble dans le cas **infini**.
Si il existe une bijection entre $\mathbb{N}$ et E, on dit que E est un ensemble **dénombrable** et on note:

$$|E| = \aleph_0$$

Si il existe une bijection de $\mathbb{R}$ dans E, alors on dit que E est un ensemble **indénombrable** et on note:

$$|E| = \aleph_1$$

Il n'existerait aucun ensemble dont le cardinal se situerait entre $\aleph_0$ et $\aleph_1$, c'est **l'hypothèse du continu**.

I — Dénombrement

Soit E un ensemble, on dit que E est **fini** si il existe une bijection de $[\![1\ ;\ n]\!]$ sur E.

On considère maintenant que E est fini, dénombrer E consiste à déterminer sa cardinalité. Informellement il s'agit souvent de compter le nombres **d'issues possibles** d'une situation donnée, on dispose alors de trois grands modèles, les **listes**, les **arrangements** et les **combinaisons**.

Listes

On appelle **liste** à p éléments de E un p-uplet constitué d'éléments de E, c'est à dire **un élément du produit cartésien** E^p on remarque alors la propriété:

Dans une liste, l'ordre compte et les répétitions sont possibles

En effet, dans $\mathbb{N}^2$ par exemple, on sait que $(1,2) \neq (2,1)$ et que $(1,1)$ est un 2-uplet valide.

On peut alors montrer que le nombre d'applications d'un ensemble à p éléments dans un ensemble à n éléments est p^n

Arrangements

On appelle **arrangement** tout liste à p éléments **distincts** de E, on remarque alors:

Dans un arrangement, l'ordre compte mais les répétitions sont impossibles

On note alors A_n^p le nombre d'arrangements de p éléments d'un ensemble à n éléments et on a:

$$A_n^p = \frac{n!}{(n-p)!}$$

Et on peut alors montrer que le nombre d'applications **injectives** d'un ensemble à p éléments dans un ensemble à n éléments est A_n^p.

Un arrangement de la forme A_n^n est apellée une **permutation** de E qui est simplement donnée par $n!$, c'est aussi le nombre de **bijections** de E dans E.

Combinaisons

On appelle **combinaison** de p éléments tout **partie** de E à p éléments, on remarque alors:

Dans une combinaison, l'ordre ne compte pas et les répétitions sont impossibles

On apelle alors **coefficient binomial** et on note $\binom{n}{p}$ le nombre de parties à p éléments d'un ensemble à n éléments et on a:

$$\binom{n}{p} = \frac{n!}{p!(n-p)!}$$

On peut remarquer que le nombre de parties à p éléments de E est exactement le nombre d'arrangements à p éléments de E auquel on retire toutes les permutations des p éléments choisis, ce qui revient exactement à **retirer la contrainte d'ordre**.

Propriétés du coefficient binomial

Le coefficient binomial possède plusieurs propriétés intéréssantes, on peut tout d'abord remarquer une **symétrie** évidente mais aussi:

Formule de Pascal: $\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$ **Formule du capitaine:** $p\binom{n}{p} = n\binom{n-1}{p-1}$

La **formule de Pascal** se comprends si on considère un élément fixé de l'ensemble et qu'on dénombreux tout ceux qui le contiennent, et les autres, ie:

Le nombre de parties à p éléments est exactement la somme du nombre de parties qui ne contiennent pas un certain x et du nombre de partie qui contiennent ce x.

La **formule du capitaine** se comprends si on considère le choix d'une équipe sportive de p joueurs (dont un capitaine) parmi un groupe de n candidats:

Choisir une équipe de p joueurs puis un capitaine parmi les p joueurs revient à choisir un capitaine parmi les n candidats, puis les $p-1$ joueurs restants.

Enfin on a aussi:

$$\sum_{p=0}^{n} \binom{n}{p} = 2^n$$

Le cardinal de l'ensemble des parties d'un ensemble à n éléments est donc exactement la somme des parties qui ont respectivement $1, 2, \ldots, n$ éléments.

Généralisation

On peut remarquer que le coefficient binomial est le nombre de partitions en deux parties de E telles que le cardinal de la première soit p. Par exemple si on considère les partitions de $E := \{1, 2, 3\}$ en deux parties dont la première ait 1 élément, on remarque qu'il y a 3 telles partitions:

$$P = \big(\{1\}, \{2, 3\}\big) \text{ ou } \big(\{2\}, \{1, 2\}\big) \text{ ou } \big(\{3\}, \{1, 2\}\big)$$

On peut alors généraliser cette idée et définir le **coefficient multinomial** $\binom{n}{k_1,\ldots,k_p}$ qui sera le nombre de partitions en p parties telles que la p-ième partie soit de cardinal k_p avec la somme des k_p **qui soit égale au cardinal total**:

$$\boxed{\binom{n}{k_1, \ldots, k_p} = \frac{n!}{k_1! k_2! \ldots k_p!}}$$

Pour fixer les idées on remarque que si $p = 2$ on a bien notre coefficient binomial usuel[1][2]:

$$\binom{n}{k_1, k_2} = \binom{n}{k_1, n - k_1} = \binom{n}{k_1} = \frac{n!}{k_1!(n - k_1)} = \frac{n!}{k_1! k_2!}$$

On peut alors utiliser ce coefficient multinomial, pour compter le nombre d'anagramme d'un mot de n lettres avec m lettres distinctes répétées k_m fois, ou encore le nombre de façon de mettre n objets dans m boites qui peuvent en contenir k_m.
Par exemple, le nombre d'anagrammes de MISSISSIPI est donné par $\binom{11}{1,4,4,1} = \frac{11!}{4!4!} = 34650$

On peut même pour définir la **formule du multinôme de Newton** qui généralise celle du binôme:

$$(x_1 + x_2 + \ldots + x_p)^n = \sum_{k_1 + k_2 + \ldots + k_p = n} \binom{n}{k_1, k_2 \ldots, k_n} x_1^{k_1} x_2^{k_2} \ldots x_p^{k_p}$$

[1] La première égalité vient de la contrainte sur la somme des k_p.

[2] La seconde égalité se comprends par symétrie, compter le nombre de partitions en deux parties dont la première contient k_1 éléments revient à compter le nombre de parties à k_1 éléments et le reste sera nécessairement dans la seconde partie.

II — Arithmétique élémentaire

Dans ce chapitre on énonce quelques définitions et propriétés arithmétiques simples dans $\mathbb{Z}$, qui seront généralisées plus tard dans le chapitre d'algèbre au cas général.

Division Euclidienne :

Soit $a, b \in \mathbb{Z} \times \mathbb{Z}^*$, on peut montrer qu'il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ avec $r < |b|$ tel que:

$$a = bq + r$$

On appelle alors cette décomposition **la division euclidienne** de a par b. La preuve se fait par l'exibition de l'algorithme bien connu.

Plus grand diviseur commun :

Soit $a, b \in \mathbb{Z}$ non simultanément nuls, alors le pgcd est l'entier $a \wedge b$ qui vérifie:

$$a \wedge b := \max\left\{n \in \mathbb{N} \ ; \ n|a \text{ et } n|b\right\}$$

Alors on l'appelle **plus grand diviseur commun** de a et de b et on le note $a \wedge b$. Pour le trouver en pratique, on peut utiliser l'algorithme d'Euclide. En effet c'est le dernier reste non-nul de celui ci.

Plus petit commun multiple:

Soit $a, b \in \mathbb{Z}$ non simultanément nuls, alors le ppcm est l'entier $a \vee b$ qui vérifie:

$$a \vee b := \min\left\{n \in \mathbb{N} \ ; \ a|n \text{ et } b|n\right\}$$

Alors on l'appelle **plus petit commun multiple** de a et de b et on le note $a \vee b$.

Identité de Bézout :

Soit $a, b \in \mathbb{Z}^2$, on peut montrer par une extension de l'algorithme d'Euclide appelé **algorithme d'Euclide étendu** qu'il existe deux entiers $u, v \in \mathbb{Z}^2$ tels que:

$$au + bv = a \wedge b$$

Il existe donc une combinaison linéaire (à coefficients entiers) de a, b qui donne leur PGCD.

Lemme de Gauss :

Soit 3 entiers $a, b, c \in \mathbb{Z}$, alors grâce à l'identité de Bézout, on peut montrer le **lemme de Gauss**:

$$\begin{cases} a \,|\, bc \\ a \wedge b = 1 \end{cases} \implies a \,|\, c$$

Indicatrice d'Euler :

En algèbre, il sera utile de connaître **le nombre d'entiers inférieurs à n et premiers avec n**, pour ceci on définit **la fonction indicatrice d'Euler** par:

$$\begin{aligned} \varphi : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto n \prod_{p|n} \left(1 - \frac{1}{p}\right) \end{aligned}$$

Le produit se faisant sur tout les diviseurs premiers distincts de n. L'utilité de cette fonction vient de la propriété suivante que justement $\phi(n)$ est exactement le nombre d'entiers inférieurs à n et premiers avec n.

Exemple: $\varphi(30) = \varphi(2 \times 3 \times 5) = 30 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 30 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 8$

II — Introduction

On appelle **structure algébrique** un ensemble muni d'une (ou plusieurs) opérations appelées **lois**, c'est l'étude de telles structures mathématiques, des relations entre celles-ci (que nous appeleront morphismes), et de leurs propriétés que nous appeleront **algèbre générale**.

Soit M un ensemble non-vide, on appelle **loi de composition interne** une opération binaire sur les éléments de M (qu'on notera temporairement $\star$) telle que:

$$\forall a, b \in M \ ; \ a \star b \in M$$

Soit E un ensemble non-vide, on appelle **loi de composition externe** une opération binaire entre un élément de E et un élément de M (qu'on notera temporairement $\cdot$) telle que:

$$\forall \lambda, a \in E \times M \ ; \ \lambda \cdot a \in M$$

On appelle **élément neutre** pour la loi un élément[1] $e \in M$ tel que pour tout élément de $a \in M$, on ait:

$$a \star e = e \star a = a$$

On appelle **inverse** pour la loi (si elle admet un élément neutre) un élément $a^{-1} \in M$ tel que pour tout élément de $a \in M$, on ait

$$a \star a^{-1} = a^{-1} \star a = e$$

Monoides :

Soit M un ensemble qu'on munit d'une **loi de composition interne**, alors le couple $(M, \star)$ est appelé un **magma**, c'est la structure algébrique primitive la plus faible, en effet la seule contrainte étant que la loi soit interne.

On peut alors enrichir la structure de magma par les deux contraintes supplémentaires suivantes:

- La loi est **associative**.
- Il existe **un élément neutre** pour la loi.

Cette structure plus riche, qu'on appelle **monoide** nous permet alors d'identifier des exemples remarquables:

- Les entiers naturels munis de l'addition forment un monoide.
- L'ensemble des chaines de caractères muni de la concaténation forme un monoide.

Les éléments neutres respectifs de ces exemples sont $0_{\mathbb{N}}$ et la chaine de caractère vide.

Morphismes :

Aprés avoir défini une structure, on peut alors définir les transformations qui **préservent cette structure**.

Soit $(M, \star)$ et $(N, \cdot)$ deux ensembles munis de la meme structure[2], $x, y \in M$ et $\varphi : M \to N$, alors φ est appelée **morphisme**, si elle vérifie:

$$\varphi(x \star y) = \varphi(x) \cdot \varphi(y)$$

Dans le cas particulier de structures qui requièrent l'existence d'un élément neutre, l'image de l'élement neutre de M par un morphisme doit etre l'élément neutre de N.

[1] Dans la suite on notera l'élément neutre d'une structure M par e_M

[2] Si les structures présentent plusieurs lois, alors les morphismes doivent vérifier la compatibilité pour **toutes les lois**.

En termes de vocabulaire, on définit alors:

- **Les endormorphismes** commme les morphismes de M dans lui-meme.
- **Les isomorphismes** commme les morphismes bijectifs.
- **Les automorphismes** commme les morphismes bijectifs de M dans lui-meme.

Moralement, on comprends que:

Les morphismes préservent dans une certaine mesure la structure opératoire.

En particulier:

Si il existe un isomorphisme entre deux structures, cela signifie que ces structures se comportent de la meme manière par rapport à leurs lois respectives.

De manière plus subtile, si il existe un morphisme injectif d'une structure dans une autre, alors cela signifie qu'une partie de la seconde se comporte de la meme manière que la première.

Enfin, si il existe un morphisme surjectif d'une structure dans une autre, cela signifie qu'on peut regrouper des élements de la première structure et ces groupes d'éléments se comporteront commes les élements de la seconde[1].

Propriétés des morphismes :

Pour une structure donnée, si φ est un morphisme de E vers F et ψ est un morphisme de F vers G, alors $\psi \circ \varphi$ est un morphisme de E vers G.

Si la structure admet un élément neutre pour la loi, alors:

$$\varphi(e_E) = e_F$$

Si la structure admet un symétrique pour la loi, alors:

$$\varphi(x^{-1}) = \varphi(x)^{-1}$$

Exemples :

On peut considérer quelques exemples remarquables:

- $\phi : n \in \mathbb{N} \longmapsto 2n \in 2\mathbb{N}$ est un morphisme (de monoide) de $(\mathbb{N}, +)$ dans $(2\mathbb{N}, +)$.
- $\phi : x \in \mathbb{R} \longmapsto \exp(x) \in \mathbb{R}^{+*}$ est un isomorphisme (de groupe) de $(\mathbb{R}, +)$ dans $(\mathbb{R}^{+*}, \times)$.
- $\phi : M \in GL_n(\mathbb{K}) \longmapsto \det(M) \in \mathbb{K}^*$ est un morphisme (de groupe) de $(GL_n(\mathbb{K}), \times)$ dans $(\mathbb{K}, \times)$.
- $\phi : z \in \mathbb{C} \longmapsto \overline{z} \in \mathbb{C}$ est un automorphisme (de corps) de $(\mathbb{C}, +, \times)$ dans $(\mathbb{C}, +, \times)$.

[1] Ces considérations plus avancées induiront l'idée générale des grands théorèmes de factorisation dans les groupes et les principaux morphismes canoniques.

Sous-structures :

Une fois une structure algébrique définie sur E, on peut alors s'intéresser aux parties de E qui conservent cette structure, on les appellera alors **sous-structures** de E.

En particulier, on dira que F est une **sous-structure** de E (et on notera $F < E$) si elle vérifie:

- La partie F est stable par les lois.
- Les éléments neutres[1] appartient à F
- Les inverses[2] des éléments de F appartient à F

On peut alors montrer les propositions suivantes:

- L'image et la préimage d'une sous-structure par un morphisme est une sous-structure.
- L'intersection d'une famille de sous-structures est une sous-structure

En particulier les noyaux de morphismes sont des sous-structures de la structure de départ.

Structures Quotients :

Dans le domaine ensembliste, on sait créer des ensembles quotients via une relation d'équivalence, on cherche par la suite à créer des ensembles quotients qui **conservent les propriétés de structure**, en particulier, on cherche des conditions sur une relation d'équivalence $\sim$ pour que $G/_\sim$ soit un groupe, un anneau, ou un corps.
On peut alors montrer qu'il faut et il suffit que $\sim$ soit **compatible** avec les lois, ie que pour toute loi $\star$, on ait:

$$x_1 \sim x_2 \text{ et } y_1 \sim y_2 \implies x_1 \star y_1 \sim x_2 \star y_2$$

On peut alors montrer que $G/_\sim$ conserve les propriétés de structure de G.

On peut alors définir la **surjection canonique** qui est le morphisme $\pi : E \to E/\sim$ qui a chaque élément associe sa classe d'équivalence pour la relation[1].

[1] **Si la structure impose leur existence**
[2] **Si la structure impose leur existence**
[1] Non spécifique aux structures, c'est une application générale liée aux ensembles quotients.

II — Groupes

Soit G un ensemble **non-vide** muni d'une loi de composition interne associative[1] telle que:

- Il existe **un élément neutre** pour la loi.
- Tout élément de G admet **un inverse** pour la loi.

Alors le couple $(G, \star)$ est appellé **groupe**. De plus si le groupe est **commutatif**, on dira alors que c'est un groupe **abélien**.

On appellera **ordre du groupe** le cardinal (potentiellement infini) de l'ensemble sous-jacent, noté $|G|$.

Exemples :

On peut alors considérer plusieurs groupes remarquables:

- Les **entiers relatifs** muni de l'addition usuelle.
- Les **isométries du plan** muni de la composition, on l'apelle le **groupe dihédral**.
- Les **matrices inversibles** muni de la multiplication, on l'apelle le **groupe linéaire**.
- Les **bijections** sur un ensemble muni de la composition, on l'apelle le **groupe symétrique**.

Morphismes de groupes :

Soit G, H deux groupes et $\varphi : G \to H$, l'existence d'un élément neutre nous permet de définir alors **le noyau d'un morphisme** par:

$$\mathrm{Ker}(\varphi) := \Big\{ x \in G \ ; \ \varphi(x) = e_H \Big\}$$

En particulier, on peut alors montrer:

> Un morphisme est injectif si et seulement si son noyau est réduit à l'élément neutre.

Sous-groupes :

Les sous-structures dans le cas des groupes sont naturellement les sous-groupes. Un cas remarquable est celui du **sous-groupe engendré** par H qu'on note:

$$\langle H \rangle := \Big\{ h_1^{k_1} h_2^{k_2} \dots h_n^{k_n} \ ; \ n \in \mathbb{N} \ , \ h_i \in H \ , \ k_i \in \mathbb{Z} \Big\}$$

Une propriété fondamentale est que $\langle H \rangle$ est un opérateur de cloture par la loi du groupe, ie c'est une application **idempotente, croissante et extensive**.

On peut alors considérer le sous-groupe engendré par un élément $h \in H$, en effet on a:

$$\langle h \rangle := \Big\{ h^k \ ; \ k \in \mathbb{Z} \Big\}$$

On peut alors définir **l'ordre d'un élément** comme étant l'ordre du sous-groupe engendré associé (potentiellement infini).

Ce sous-groupe permet de définir des groupes remarquables, en effet si un groupe est engendré par un unique élément, il est appelé **groupe cyclique** dont nous parleront plus loin dans ce chapitre.

[1] Dans la suite, la loi de composition des groupes sera notée multiplicativement sauf exceptions.

Classes :

On considère maintenant un sous-groupe $H \leq G$, alors on peut définir deux relations d'équivalences sur G par:

$$\begin{cases} g_1 \sim g_2 \iff \exists h \in H \ ; \ g_1 = g_2 h \\ g_1 \sim g_2 \iff \exists h \in H \ ; \ g_1 = h g_2 \end{cases}$$

On appelle alors **classe à gauche** (resp. classe à droite) les classes d'équivalences pour ces deux relations et on note alors gH (resp. Hg) la classe d'un élément g pour cette relation. On note alors G/H l'ensemble quotient associé aux classes à gauche.

Théorème de Lagrange :

Ces classes induisent donc une partition de G en classes **de même cardinal**, en effet:

$$|gH| = \left|\{gh \ ; \ h \in H\}\right| = |H|$$

En outre on a une bijection qui associe à chaque élément de g sa classe et l'élément de H lui correspondant:

$$\begin{aligned} f : G &\longrightarrow (G/H, H) \\ g &\longmapsto (aH, h) \end{aligned}$$

Ceci nous permet donc de montrer le **théorème de Lagrange** qui nous donne que pour tout groupe fini G, on a:

$$|G| = |G/H||H|$$

Et comme corollaire immédiat la propriété suivante:

Le cardinal d'un sous-groupe divise le cardinal du groupe.

Sous-groupes normaux :

On cherche alors à caractériser les sous-groupes tels que la relation d'équivalence définie ci-dessous soit **compatible** avec les opération de groupe, en d'autres termes on cherche à définir un groupe quotient pour cette relation. On peut alors montrer que les sous-groupes vérifiant cette compatibilité vérifient:

$$\forall g \in G \ ; \ gH = Hg$$

En d'autres termes les classes à droite et à gauche coincident. C'est alors immédiat que **tout sous-groupe d'un groupe abélien est normal**. Par ailleurs on peut caractériser les sous-groupes normaux d'une autre façon (détaillée au chapitre sur les actions de groupe) comme les sous-groupes qui vérifient:

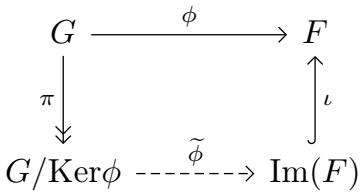
$$\forall h \in H \ , \ \forall g \in G \ ; \ ghg^{-1} \in H$$

II — Théorèmes d'isomorphismes

Une des motivations de la notion de groupe quotient est entre autres de pouvoir trouver des **isomorphismes** entre des groupes connus, dans ce chapitre, on énonce les trois grands théorèmes utilisables pour atteindre cet objectif.

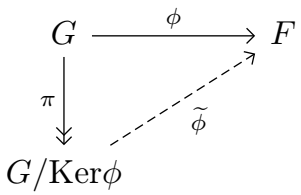
Premier théorème d'isomorphisme :

Soit $\phi : G \longrightarrow F$ un morphisme, on rapelle que tout les noyaux sont normaux et on peut alors montrer qu'il existe un unique isomorphisme $\widetilde{\phi} : G/\mathrm{Ker}\phi \longrightarrow F$ tel que le diagramme soit commutatif [1]:



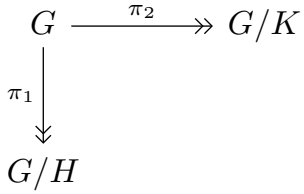
En effet, le passage au quotient rend le morphisme injectif, donc surjectif sur son image, et le diagramme commute, ie on a $\phi = \iota \circ \widetilde{\phi} \circ \pi$.

De manière plus générale, on a la **propriété universelle du quotient** pour $H \trianglelefteq G$ tel que $H \subseteq \ker(\phi)$, alors on a l'existence d'un morphisme $\widetilde{\phi}$ tel que le diagramme suivant commute:

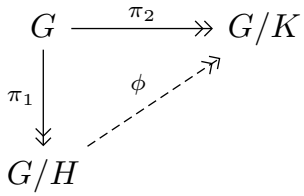


Deuxième théorème d'isomorphisme :

On considère ici deux sous groupe normaux H, K de G tel que $H \subseteq K$, alors on a les deux projections suivantes:

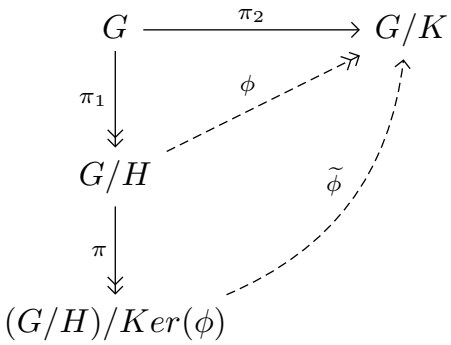


On peut alors utiliser la propriété universelle du quotient pour compléter le diagramme par un morphisme ϕ (par ailleurs surjectif):



[1] Un **diagramme commutatif** est une collection d'objets et de morphismes tels tout les chemins (de composition) partant d'un objet vers un autre donnent le meme résultat (ie sont le meme morphisme).

Enfin, on peut appliquer le premier théorème d'isomorphisme à ϕ pour obtenir le diagramme suivant:



On peut alors montrer que $\mathrm{Ker}(\phi) = K/H$ et donc qu'on a l'isomorphisme suivant:

$$(G/H)/(K/H) \cong G/K$$

Troisième théorème d'isomorphisme :

Caractère universel :

Le parti pris a été fait de mettre cette section dans le chapitre sur les groupes, mais ceci est trompeur, les trois théorèmes ci-dessus sont en fait vrais dans un cadre bien plus général, et pour des objets bien plus généraux apellés **algèbres universelles**, en particulier tout structure sur laquelle on peut définir une notion de quotient compatibles avec les opérations vérifie alors des analogues de ces théorèmes. En particulier:

- On peut quotienter un ensemble par la relation d'équivalence "avoir la même image" et obtenir alors de tels théorèmes.
- On peut quotienter un anneau par un **idéal** et obtenir alors de tels théorèmes.
- On peut quotienter un espace vectoriel (ou même un module) par un sous-espace et obtenir alors de tels théorèmes.

Applications :

II — Actions de groupe

Soit G un groupe et X un ensemble quelconque, dans ce chapitre on définit un notion fondamentale en théorie des groupes, la notion **d'action d'un groupe sur un ensemble.** En effet on appelera **action** du groupe G sur X une application de la forme:

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

En outre une action doit vérifier deux autres propriétés:

- **Le neutre n'agit pas:** $\forall x \in X \ ; \ e \cdot x = x$
- **Associativité mixte:** $\forall g_1, g_2, x \in G \times G \times X \ ; \ (g_1 g_2) \cdot x = g_1(g_2 \cdot x)$

On dira alors que G **agît** sur X et on notera alors $G \curvearrowright X$.

Morphisme structurel:

On se donne une action $G \curvearrowright X$, alors il peut être utile de considérer la currifiée[1] de cette action, ie:

$$\begin{aligned} \phi : G &\longrightarrow (X \longrightarrow X) \\ g &\longmapsto (x \longmapsto g \cdot x) \end{aligned}$$

On peut alors montrer que cette fonction prends son image dans l'ensemble des bijections sur X (dont on montrera que c'est un groupe au chapitre sur le groupe symétrique) et que c'est un **morphisme de groupe**. L'action de G induit donc un morphisme de groupe, appelé **morphisme structurel** de la forme:

$$\phi : G \longmapsto \mathfrak{S}(X)$$

En outre cette correspondante est bijective, il est donc équivalent de considérer une action d'un groupe sur un ensemble ou un morphisme structurel.

Action induite sur l'ensemble des parties :

Si G agît sur X alors G agît alors naturellement sur $\mathcal{P}(X)$ par l'action:

$$(g, P) \mapsto g \cdot P := \{g \cdot x \ ; \ x \in P\}$$

Action induite sur les sous structures:

On se pose alors deux questions naturelles:

- Une action de G sur X induit-elle nécessairement une action de G sur $Y \subseteq X$?
- Une action de G sur X induit-elle nécessairement une action de $H \leq G$ sur X ?

On peut alors montrer que la première question admet une réponse positive si et seulement si Y est **stable par l'action**.

Pour la seconde question, elle admet toujours une réponse positive et on a même le résultat général suivant gràce au morphisme structurel, on considère deux groupes G, H reliés par un morphisme ϕ, et une action de H sur X de morphisme structurel ψ, alors on a le diagramme:

$$G \xrightarrow{\ \phi\ } H \xrightarrow{\ \psi\ } X$$

Et donc $\phi \circ \psi$ définit bien un morphisme structurel de G sur $\mathfrak{S}(X)$ et donc une action. Le cas particulier des sous-groupes se déduit en considérant ϕ le morphisme d'inclusion d'un sous-groupe dans le groupe total.

[1] On rapelle que $\mathcal{F}(E \times F, G) \cong \mathcal{F}(E, \mathcal{F}(F, G))$ en tant qu'ensembles.

Orbites :

Considérons un point $a \in X$, alors on définit **l'orbite** de a sous l'action du groupe G par:

$$\mathrm{Orb}_G(a) := \{g \cdot a \ ; \ g \in G\}$$

Intuitivement, ce sont tout les points atteints par l'action de G sur le point initial a. Une propriété fondamentale des orbites est la suivante, si on considère la relation suivante:

$$x \sim y \iff y \in \mathrm{Orb}_G(x)$$

Alors c'est une **relation d'équivalence**, et on a donc toujours une **partition** de X associée à l'action de G, c'est la partition en orbites.

Stabilisateurs :

Considérons un point $a \in X$, alors on définit **le stabilisateur** de a sous l'action du groupe G par:

$$\mathrm{Stab}_G(a) := \big\{g \in G \ ; \ g(a) = a\big\}$$

Intuitivement, ce sont tout les éléments du groupe qui laissent a invariant. Une propriété fondamentale des stabilisateurs est que c'est un **sous-groupe** du groupe G. En outre si on considère le morphisme structurel ϕ de l'action, on a:

$$\mathrm{Ker}(\phi) = \bigcap_{x \in X} \mathrm{Stab}_G(x)$$

Généralisations aux parties :

On peut alors noter qu'il est aussi possible de définir les orbites et stabilisateurs de **parties**, en considérant les orbites et stabilisateurs pour l'action induite sur les parties définie plus haut.

Vocabulaire :

On peut alors nommer les actions de groupes qui vérifient certaines propriétés relatives aux ensembles définis plus haut, on appelle alors:

- Action **transitive** une action qui n'admet qu'une seule orbite.
- Action **libre** une action dont tout les stablisateurs sont triviaux.
- Action **fidèle** une action dont le noyau du morphisme structurel est trivial[1].

On dira aussi qu'une action transitive et libre est **simplement transitive**, et on peut caractériser cette action par le fait que pour tout paire d'éléments $x, y \in E$, il existe un **unique** élement de g qui relie x à y.

Action par automorphismes intérieurs:

On peut alors aussi étudier l'action du groupe G sur **lui-même**, on obtient alors un nouveau moyen d'étude du groupe G, en particulier, on a deux actions remarquables:

- **L'action par translation:** $\forall g, h \in G, g \cdot h = gh$
- **L'action par conugaison:** $\forall g, h \in G, g \cdot h = ghg^{-1}$

Ceci permet une reformulation plus élégante du concept de sous-groupe normal, en effet un sous-groupe est normal si et seulement si il est **stable par l'action de conjugaison**.

[1] On a alors d'aprés la caractérisation du noyau ci-dessus que toute action **libre** est **fidèle**.

Centralisateur:

Le stabilisateur d'un élément g pour la relation de conjugaison est alors appelé **centralisateur** et noté $Z(g)$, et c'est l'ensemble des éléments qui commutent avec g.

On peut définir le centralisateur d'une partie, noté $Z(H)$ qui est l'intersection de tout les centralisateurs de ses éléments, ie l'ensemble des éléments du groupe qui commutent avec tout les éléments de H, ie on a:

$$Z(H) := \{g \in G \ ; \ \forall h \in P \ , \ gh = hg\}$$

En particulier pour tout groupe G, on appelle **centre** du groupe et on note $Z(G)$, l'ensemble des éléments qui commutent avec tout les autres éléments.

Normalisateur:

En affaiblissant la définition ci dessus, on peut définir le **normalisateur** d'une partie H, noté $N(H)$, et c'est le stabilisateur de l'action par la conjugaison sur les **parties**, ie:

$$N(H) := \{g \in G \ ; \ gH = Hg\}$$

Relation orbites stabilisateurs:

On peut alors montrer que si on fixe $x \in X$, alors il existe une bijection entre $G/\text{Stab}(x) \longrightarrow \text{Orb}(x)$ et en particulier, on a alors la relation fondamentale suivante dite **relation orbites-stabilisateurs**:

$$|G| = \big|\text{Orb}(x)\big| \, \big|\text{Stab}(x)\big|$$

Et donc en particulier, le cardinal d'une orbite (ou d'un stabilisateur) **divise l'ordre de** G.

Formules des classes:

On peut alors utiliser le fait que X se partitionne en orbites pour obtenir une expression du cardinal de X apellée **formule des classes** où n désigne le nombre d'orbites:

$$|X| = \sum_{i=1}^{n} \big|\text{Orb}(x_i)\big| = \sum_{i=1}^{n} \frac{|G|}{\big|\text{Stab}(x_i)\big|}$$

Un des intérêts de cette formule est par exemple qu'elle permet de connaître le nombre d'orbites d'une action ou de montrer l'existence de points fixes (ie de points dont l'orbite est de cardinal 1), en effet on considère les diviseurs de l'ordre du groupe $(d_1, \ldots, d_k)$ et $(a_1, \ldots, a_k)$ le nombre d'orbites de cette taille, on obtient alors une equation de la forme suivante, qui peut souvent s'étudier facilement dans les cas simples avec peu de diviseurs:

$$|X| = \sum a_k d_k$$

Formules de Burnside:

Une autre formule important liée aux actions de groupe est **la formule de Burnside** qui permet de dénombrer les orbites de l'action, et en particulier, on peut alors **compter des éléments modulo une action de groupe**, on a la formule suivante:

$$n = \frac{1}{|G|} \sum_{g \in G} |\text{Fix(g)}|$$

Où $\text{Fix(g)} := \{x \in X \ ; \ g \cdot x = x\}$ est l'ensemble des points fixés par g. Cette formule est fondamentale en combinatoire, par exemple imaginons que nous souhaitions compter le nombre de colliers **différents** de 5 perles à deux couleurs. Alors ici "différents" signifie que un des colliers dénombré est égal à un autre aprés une rotation ou une reflexion, on considèrera ce collier comme le même que le premier.

L'idée principale est donc bien de compter des éléments modulo l'action sur l'ensemble, ie en identifiant deux éléments dans la même orbite.

Compter ces colliers revient donc à compter les orbites de l'action par symétries d'un groupe sur l'ensemble de tout les colliers possibles. Et la formule de Burnside nous permet donc d'effectuer ce calcul.

II — Groupes Symétriques

On appelle **groupe symétrique** et on note $\mathfrak{S}_n$ le groupe des **permutations** de l'ensemble $[\![1\ ;\ n]\!]$ muni de la composition des applications.

On remarque alors aisément que l'ordre de $\mathfrak{S}_n$ est $n!$.

Soit $\sigma \in \mathfrak{S}_n$ une permutation de $[\![1\ ;\ n]\!]$, alors c'est une fonction bijective sur cet ensemble. En particulier, sachant que l'ensemble est fini, c'est une fonction définie par cas qu'on note alors par commodité horizontalement dans un tableau:

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

Support :

On appelle alors **support** d'une permutation le complémentaire des points fixes de σ, ie on a:

$$\mathrm{Supp}(\sigma) := \{i \in \mathbb{N}\ ;\ \sigma(i) \neq i\}$$

Une des propriétés fondamentale qu'on peut déduire de cette définition est que **deux permutations à supports disjoints commutent**.

Cycles :

On appelle **k-cycle** une permutation σ telle qu'il existe $k \geq 2$ et k éléments deux à deux distincts $a_1, \dots, a_k$ tels que:

$$\begin{cases} \forall i \in [\![1\ ;\ k-1]\!]\ ;\ \sigma(a_i) = \sigma(a_{i+1}) \\ \forall i \notin [\![1\ ;\ k]\!]\ ;\ \sigma(a_i) = \sigma(a_i) \\ \sigma(a_k) = \sigma(a_1) \end{cases}$$

Un k-cycle laisse fixe tout les éléments sauf pour une certaine famille (a_i) pour laquelle chaque élément est envoyé sur le suivant.

On peut alors noter un tel cycle par la notation suivante qui décrit tout les éléments affectés par la permutation:

$$\sigma = (a_1, \dots, a_n)$$

Le cas particulier des 2-cycles est intéressant, en effet un 2-cycle **échange deux valeurs** de $[\![1\ ;\ n]\!]$, ils sont d'une importance particulière et on les appelle **transpositions**.

Exemple: La permutation suivante est un 3-cycle:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (1\ 2\ 3)$$

Si σ est un k-cycle et que a n'est pas un point fixe, alors on en déduit[1] que le support de σ est donné par:

$$\mathrm{Supp}(\sigma) = \{a, \sigma(a), \sigma^2(a), \dots, \sigma^{k-1}(a)\}$$

Ordre :

On peut alors démontrer une propriété fondamentale de l'ordre des cycles:

Un k-cycle est d'ordre k.

En effet si on considère le sous-groupe engendré par un tel cycle, on remarque que pour tout élément $a \in [\![1\ ;\ n]\!]$ $\sigma^k(a) = a$, donc $\sigma^k = \mathrm{Id}$.

[1] En effet par exemple $\sigma(a)$ est la valeur suivante dans le cycle, et le cycle parcourt tout les points non-fixes par construction

Théorèmes de décomposition :

Une des problématiques principales à propos des groupes symétriques est la question de la **décomposition d'une permutation** en cycles. On peut en effet montrer que **toute permutation se décompose en produit de cycles à support disjoints**.

Pour ceci, on utilise le fait que toute permutation induit une **partition en orbites** de $[\![1\ ;\ n]\!]$, ces orbites correspondront alors au supports des cycles dans la décomposition.

Par la suite, on peut alors constater directement que pour tout k-cycle $\sigma = (a_1\ \ \dots\ \ a_k)$, on a:

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

Enfin, on conclura de ces deux propositions que **toute permutation se décompose en produit de transpositions**, ou en d'autres termes si on note $\mathfrak{T}_n$ l'ensemble des transpositions:

$$\langle \mathfrak{T}_n \rangle = \mathfrak{S}_n$$

Conjugaison et permuations :

On considère alors l'action de $\mathfrak{S}_n$ sur lui-même par conjugaison, on peut alors montrer que pour toute permutation σ, on a:

$$\sigma(a_1, \dots, a_n)\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_n))$$

En particulier, on a alors que deux cycles sont conjugués si et seulement si ils ont la même longueur, et si on définit le **type d'une permutation** par le n-uplet **non ordonné** $[l_1, \dots, l_k]$ des longueurs des cycles dans sa décomposition en cycles, on a alors une caractérisation des classes de conjugaisons:

Deux permutations sont conjuguées si et seulement si elles ont même type.

Signature :

A REFAIRE.

II — Groupes Cycliques

On appelle **groupe cyclique** un groupe G engendré par un unique élément qu'on notera g. Le but de ce chapitre est de classifier ces groupes et d'identifier leurs caractéristiques.

Classification :

Dans cette section, on utilisera le morphisme surjectif suivant:

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow G \\ n &\longmapsto g^n \end{aligned}$$

On raisonne sur la finitude de G et on peut alors caractériser tout les groupes cycliques trés simplement, en effet:

- Si G est infini, le morphisme ϕ est **injectif** et on a l'isomorphisme $G \cong \mathbb{Z}$
- Si G est fini, on utilise le **premier théorème d'isomorphisme** et on a l'isomorphisme $G \cong \mathbb{Z}/n\mathbb{Z}$

Il n'y a donc qu'un seul groupe cyclique d'ordre n (resp. d'ordre infini), celui des classes de congruences modulo n (resp. celui des entiers).

Le groupe $\mathbb{Z}/n\mathbb{Z}$:

On remarque alors l'importance du groupe $\mathbb{Z}/n\mathbb{Z}$, c'est le prototype de groupe cyclique fini. On peut alors montrer que ces groupes correspondent à l'ensemble des **restes par la division euclidienne par** n et l'égalité dans ces groupes corresponds à ce qu'on appelle la **congruence**.

Exemple: Dans $\mathbb{Z}/6\mathbb{Z}$, on a $2 = 8 = 14 \dots$ en effet ces nombres ont le même reste par la division euclidienne par 6.

Générateurs de $\mathbb{Z}/n\mathbb{Z}$:

On sait que la classe de 1 ou -1 engendre le groupe $\mathbb{Z}/n\mathbb{Z}$ comme image de générateurs de $\mathbb{Z}$, on se pose la question si il existe d'autres générateurs. En effet c'est le cas, en particulier si $p \wedge n = 1$, d'aprés la relation de Bézout, on peut montrer que sommer p un certain nombre de fois permettra d'obtenir 1 et donc d'engendrer le groupe.

Il y a donc $\phi(n)$ générateurs de $\mathbb{Z}/n\mathbb{Z}$ où ϕ est **l'indicatrice d'Euler**.

Théorème chinois :

Un des grands théorèmes sur les groupes cycliques est le suivant, si on considère $p_1, \dots, p_k \in \mathbb{N}$ des nombres premiers entre eux, et qu'on note n leur produit, alors on peut montrer facilement qu'on a l'isomorphisme suivant:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_k\mathbb{Z}$$

En particulier si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ décompé en facteurs premiers, alors on a:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$$

C'est la **décomposition primaire d'un groupe cyclique**. Elle s'interprète en comprenant par exemple que la donnée du reste par 6 d'un entier est exactement equivalente à la donnée de son reste par 3 et 2.

II — Anneaux

Soit A un ensemble **non-vide** muni de deux lois de composition internes associatives notées $+, \times$ telles que:

- $(A, +)$ soit un groupe commutatif.
- La loi $\times$ est associative.
- La loi $\times$ est distributive sur la loi $+$.
- Il existe **un élément neutre** pour la loi $\times$.

Alors le triplet $(A, +, \times)$ est appellé **anneau**. Si la loi multiplicative est **commutative**, on dira alors que c'est un anneau commutatif.

Exemples :

On peut alors considérer plusieurs anneaux remarquables:

- Les **entiers relatifs** muni des opérations usuelles.
- Les **fonctions continues** muni de la somme et du produit.
- Les **polynomes**[1] muni de la somme et du produit.
- Les **matrices**[1] muni de la somme et du produit.

Propriétés Algébriques:

Pour deux éléments $a, b \in A$ qui commutent, on a **la formule du binome de Newton**:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Sous-anneaux :

Les sous-structures dans le cas des groupes sont naturellement les **sous-anneaux**. Un cas remarquable est celui du **sous-anneau engendré** par H qu'on note:

$$\langle H \rangle := \left\{ \sum_{k=1}^{n} \pm h_1^{k_1} h_2^{k_2} \dots h_n^{k_n} \ ; \ n \in \mathbb{N} \ , \ h_i \in H \ , \ k_i \in \mathbb{N} \right\}$$

C'est l'ensemble des produits et sommes d'éléments de H et de leurs inverses pour la loi de groupe.

Une propriété fondamentale est que $\langle H \rangle$ est un **opérateur de cloture** par la loi du groupe, ie c'est une application **idempotente, croissante et extensive**.

Idéaux:

On appelle **idéal** tout sous groupe additif de A qui soit stable par multiplication (à droite et à gauche) par n'importe quel élément de l'anneau.

Les idéaux jouent alors le meme role que les sous-groupes normaux, ie on peut quotienter par ceux-ci.

On peut alors montrer les propriétés suivantes:

- La préimage d'un idéal par un morphisme est un idéal[2].
- L'intesection d'une famille d'idéaux est un idéal.

[1] A coefficients dans un anneau
[1] A coefficients dans un anneau
[2] Donc en particulier, les noyaux de morphismes sont toujours des idéaux.

Inversibles :

On dit qu'un élément $x \in A^*$ est **inversible** à droite[2] si et seulement si il existe $y \in A$ tel que:

$$xy = 1$$

Si un élément est inversible bilatère, on dira alors simplement qu'il est inversible. L'ensemble des inversibles d'un anneau forme un groupe pour la loi multiplicative qu'on note $\mathbb{U}(A)$.

Diviseurs de zéro :

On dit qu'un élément $x \in A^*$ est **un diviseur de zéro** à droite[3] si et seulement si il existe $y \in A^*$ tel que:

$$yx = 0$$

Exemple: Dans l'anneau $\mathcal{M}_2(\mathbb{R})$, la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ est un diviseur de zéro car $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} = 0$

Nilpotents :

On dit qu'un élément $a \in A$ est **nilpotent** si et seulement si il existe $n \in \mathbb{N}$ tel que:

$$a^n = 0$$

En particulier les nilpotents sont donc des diviseurs de zéro.

Exemple: Dans l'anneau $\mathcal{M}_2(\mathbb{R})$, la matrice $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ est nilpotente car $A^2 = 0$

Caractéristique :

On définit la caractéristique d'un anneau non-nul par:

$$\text{char}(A) := \min\left\{ n \in \mathbb{N} \,;\, \underbrace{1 + \ldots + 1}_{n \text{ sommandes}} = 0 \right\}$$

Une autre formulation serait simplement que:

La caractéristique d'un anneau est l'ordre (additif) de l'unité multiplicative.

Anneaux intègres :

On appelle **anneau intègre** tout anneau A non-nul **commutatif** et **sans diviseurs de zéro**. En particulier, dans un anneau intègre, on a alors la propriété qu'un produit est nul si et seulement si **l'un des facteurs est nul**.

Anneaux à PGCD :

Anneaux Factoriels :

Anneaux Principaux :

Anneaux Euclidiens :

On appelle **anneau Euclidiens** tout anneau A principal qui possède une **division euclidienne**. Dans un tel anneau, on peut alors faire **de l'arithmétique** comme dans l'anneau des entiers naturels.

[2] On définit de meme les inversibles à gauche
[3] On définit de meme les diviseurs de zéro à gauche

Schéma heuristique des structures d'anneaux :

Pour mieux visualiser la hierarchie des différents types d'anneaux, on peut représenter la structure logique sous la forme de la suite d'implications suivantes:

$$\textbf{Euclidien} \implies \textbf{Principal} \implies \textbf{Factoriel} \implies \textbf{PGCD} \implies \textbf{Intégre} \implies \textbf{Commutatif}$$

II — Corps

Soit A un anneau dont tout les éléments sauf 0 sont inversibles. Alors on dit que A est **un corps**.

Exemples :

On peut alors considérer plusieurs corps remarquables:

- Les **réels** muni des opérations usuelles.
- Les **quaternions**[1] muni des opérations usuelles.
- Les **corps finis** $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ pour p premier.
- Les **nombres constructibles** à la règle et au compas.

[1] C'est un exemple de corps non commutatif

II — Corps des Complexes

On définit le nombre imaginaire i dont le carré vaut -1, et on construit alors $\mathbb{C}$ comme l'extension du corps[1] $\mathbb{R}$ avec les deux lois usuelles, ie on définit:

$$\mathbb{C} := \mathbb{R}[i] = \left\{ a + ib \ ; \ a, b \in \mathbb{R} \right\}$$

On peut alors montrer que c'est un ensemble stable pour les lois usuelles et qu'il vérifie toutes les propriétés qui font de lui un **corps**.
Chaque nombre complexe se définit alors comme des sommes ou produits de réels et du nombre imaginaire et on appelle alors cette expression la **forme algébrique** d'un nombre complexe et on appelle a **la partie réelle** et b **la partie imaginaire** de ce nombre.

Géométriquement, on peut identifier les nombres complexes à des points du plan, en effet, $a + ib$ peut se comprendre comme une combinaison linéaire d'un nombre de l'axe réel, et d'un nombre de l'axe imaginaire.

Module :

On appelle **module** de $z \in \mathbb{C}$ le **prolongement** de la fonction valeur absolue à $\mathbb{C}$, c'est donc une **norme** et on la définit telle que :

$$|z| = \sqrt{a^2 + b^2} = \sqrt{z\overline{z}}$$

Dans la suite, on notera ϱ le module de z pour faciliter la lecture.

Forme trigonométrique :

L'interprétation géométrique permet alors de montrer par passage en coordonées polaires qu'il existe un unique angle θ (modulo 2π) qu'on appelle **argument** de z tel que:

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

Forme exponentielle :

De même on définit alors **la forme exponentielle** de z l'expression:

$$z = \varrho e^{i\theta} := \varrho(\cos\theta + i\sin\theta)$$

On peut alors étendre les propriétés usuelles de l'exponentielle à $\mathbb{C}$ et on en déduit:

$$\begin{aligned} \arg(zz') &\underset{2\pi}{\equiv} \arg(z) + \arg(z') \\ \arg(\frac{z}{z'}) &\underset{2\pi}{\equiv} \arg(z) - \arg(z') \end{aligned}$$

Conjugué :

On appelle conjugaison **l'involution** qui à z associe son **conjugué**, noté $\overline{z}$ tel que:

$$\overline{z} := a - bi = \varrho(\cos\theta - i\sin\theta) = \varrho e^{-i\theta}$$

C'est une application **additive** et **multiplicative**, on montre alors les formules suivantes :

$$\Re(z) := \frac{z + \overline{z}}{2} \qquad\qquad \mathrm{Im}(z) := \frac{z - \overline{z}}{2i}$$

En utilisant ces formules pour z sous forme exponentielle, on a alors les **formules d'Euler** qui sont très importantes car elle permettent de **linéariser** des expression trigonométriques.

[1] La motivation principale de l'introduction de i et de cette construction est que $\mathbb{C}$ est algébriquement clos, ie tout les polynomes de degré n de $\mathbb{C}[X]$ ont n racines.

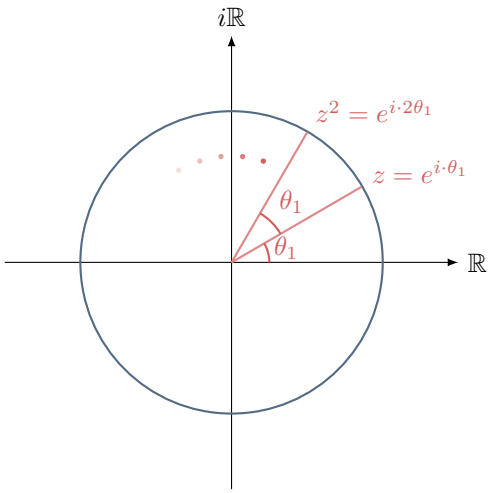
Formule de Moivre :

Un propriété importante des formes trigonométriques et exponentielles apellée **formule de Moivre**[1] est:

$$(e^{i\theta})^n = e^{n(i\theta)}$$
$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$$

Les différentes puissances d'un nombre complexe (de module 1) s'interprétent alors comme des points situés à equidistance sur un cercle.

Graphiquement:



Racines n-ièmes :

Soit $n \in \mathbb{N}$, une partie importante des problèmes impliquant des nombres complexes proviennent d'équations d'inconnue Z de la forme:

$$Z^n = z$$

On peut montrer que l'ensemble des solutions de ce type de problème est:

$$S = \left\{ \sqrt[n]{\varrho} e^{i\frac{\theta+2k\pi}{n}} \ ; \ k \in \{0, 1, \ldots, n-1\} \right\}$$

Cas particulier : Si on a une racine n-ième Z_0 de Z et qu'on connaît les racines n-ièmes de l'unité, alors on peut obtenir toutes les racines n-ièmes de Z grâce à:

$$\left\{ Z \in \mathbb{C} \ ; \ Z^n = z \right\} = \left\{ Z_0 u \ ; \ u \in \mathbb{U}_n \right\}$$

Le nombre complexe j :

On note j la première racine troisième de l'unité. Le nombre j est singulier, car il vérifie:

$$j^2 = j^{-1} = \overline{j}$$

Graphiquement, on peut observer que les affixes des nombres 1, j et $\overline{j}$ forment un triangle équilatéral inscrit dans le cercle trigonométrique.

[1] Ici, on a choisi de considérer $z \in \mathbb{U}$ mais ces propriétés sont vraies pour **tout nombre complexe**, il suffit alors d'appliquer la puissance au module.

II — Anneau des Polynômes

Définition :

Soit K un corps, et $n \in \mathbb{N}$, on appelle **polynômes** à coefficients dans K en l'indéterminée X les éléments de l'ensemble:

$$K[X] := \left\{ \sum_{i=0}^{n} a_i X^i \ ; \ a_i \in K \right\}$$

Degré et Valuation :

Soit $P, Q, R \in K[X]$.
On définit tout d'abord une propriété fondamentale appelée **degré** de P telle que $\deg(P)$ est le plus grand coefficient non nul de P. On a alors les propriétés du degré ci-dessous:

$$\deg(P+Q) \leq \max(\deg(P), \deg(Q))$$
$$\deg(PQ) = \deg(P) + \deg(Q)$$

La valuation est définie de manière analogue comme le plus petit coefficient non nul de P.

Opérations :

On considère ci-dessous que $\deg(P) = n$ et $\deg(Q) = m$ et on note a_i, b_i les coefficients de P (resp. Q).

On adjoint à cet ensemble une loi d'addition qui est simplement effectuée terme à termes.
On adjoint à cet ensemble une loi de multiplication se définit explicitement comme suit:

$$PQ := \sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_i X^k$$

Muni de ces deux opérations, on donne à cet ensemble une structure **d'anneau**[1].

On ajoute aussi une opération appelée **dérivation formelle** d'un polynôme qui s'effectue comme la dérivation analytique usuelle.

Divisibilité :

On définit tout d'abord une **division euclidienne** de deux polynômes qui se comporte comme la division euclidienne usuelle, à la différence que la condition d'arrêt porte sur le **degré du reste** qui doit être inférieur à celui du diviseur.

Soit $U, V \in R[X]^2$, on peut aussi définir une relation de **divisibilité** entre deux polynômes, cette relation est **transitive et réflexive** et on a aussi:

$$D|A \wedge D|B \implies D|UA + VB$$

Racines et Factorisation :

On dit que α est une **racine** de P si $P(\alpha) = 0$.
On montre alors le théorème fondamental ci-dessous:

$$P(\alpha) = 0 \iff (X - \alpha)|P$$

[1] Intègre car les coefficients viennent d'un corps.

On appelle **multiplicité d'une racine** α l'entier m tel que:

$$\Big[(X-\alpha)^m | P\Big] \wedge \Big[(X-\alpha)^{m+1} \nmid P\Big]$$

Si on note P^m la dérivée n-ième de P, on a aussi:

$$P^m(\alpha) = 0 \ \wedge \ P^{m+1}(\alpha) \neq 0$$

On en déduit que pour une racine α de multiplicité m, on peut **factoriser** P par $(X-\alpha)^m$.

Si on considère maintenant plusieurs racines **distinctes** $a_0, a_1, \ldots, a_{n-1}, a_n$ de multiplicité respectivement $m_0, m_1, \ldots, m_{n-1}, m_n$, on peut montrer la propriété suivante:

$$\Big[\prod_{i=0}^{n}(X-\alpha_i)^{m_i}\Big] \Big| P \qquad \text{(On peut factoriser par le produit des } (X-\alpha_i)^{m_i}\text{)}$$

Décomposition :

On appelle décomposition d'un polynôme P une factorisation **irréductible** de P, cette décomposition dépend du corps considéré, en effet si on considère $\mathbb{C}[X]$, on peut montrer le **théorème fondamental de l'Algèbre** ci-dessous:

> Tout polynôme de degré n admet n racines dans $\mathbb{C}$.

Par suite, on peut montrer que tout les polynômes de $\mathbb{C}[X]$ sont **scindés**[1].
Par contre dans $\mathbb{R}[X]$, il existe évidemment des polynômes de degré 2 irréductibles.

Soit $z \in \mathbb{C}$, il existe une propriété très utile pour décomposer un polynôme **à coefficients réel** qui est:

$$P(z) = 0 \implies P(\overline{z}) = 0$$

Fonctions symétriques des racines :

On définit le k-ième **polynôme symétrique** à n indéterminées comme la somme des produits à k facteurs de ses indéterminées, et on le note σ_k.

Par exemple pour un polynôme en trois indéterminées a, b, c, on a successivement:

$\sigma_1 = a + b + c$ (Somme des produits à 1 facteur)
$\sigma_2 = ab + ac + bc$ (Somme des produits à 2 facteurs)
$\sigma_3 = abc$ (Somme des produits à 3 facteurs)

De manière générale on a:

$$\sigma_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < \ldots < i_k \leq n} x_{i_1} x_{i_2} \ldots x_{i_k}$$

Soit $P \in K[X]$ un polynôme de degré n, on note $x_1, x_2, \ldots, x_{n-1}, x_n$ ses n racines et $a_1, a_2, \ldots, a_{n-1}, a_n$ ses n coefficients.
Alors, pour tout $k \in [\![0\ ;\ n]\!]$, on a le **théorème**:

$$\sigma_k(x_1, x_2, \ldots, x_{n-1}, x_n) = (-1)^k \frac{a_{n-k}}{a_n}$$

Ce théorème permet d'obtenir une relation **coefficient-racines**.

Exemple:
- Pour $k = 1$, on trouve que la somme des racines de P vaut $-\frac{a_{n-1}}{a_n}$
- Pour $k = 2$, on trouve que la somme des doubles produits des racines de P vaut $\frac{a_{n-2}}{a_n}$
- .....

[1] C'est à dire que tout les polynômes irréductibles de $\mathbb{C}[X]$ sont de degré 1.