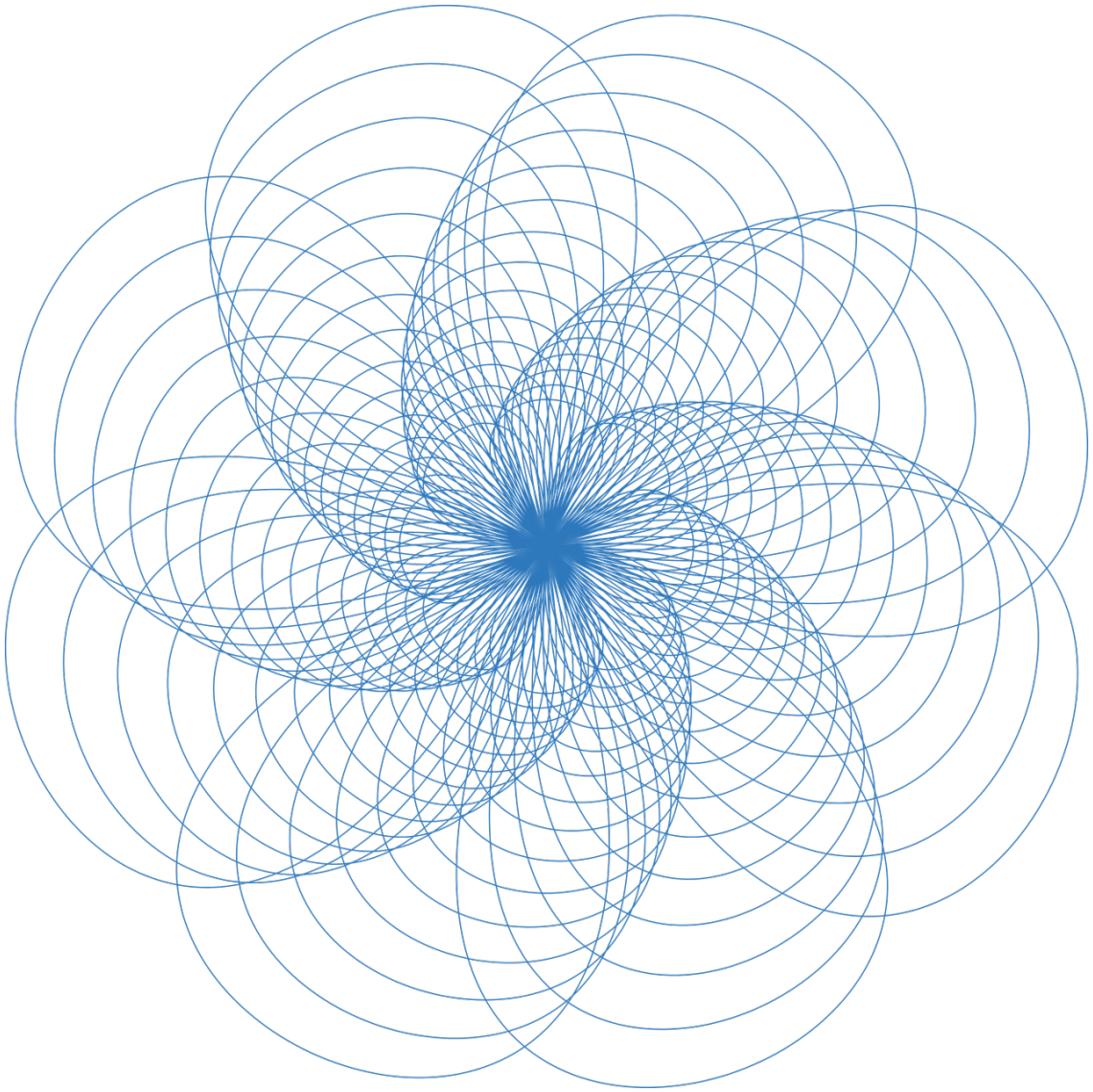
Mathématiques

Licence



Université Jean-François Champollion
Année 2022 - 2025

Table des matières

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

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

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

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

Soit $a \in E$, alors on peut aussi rencontrer dans les structures usuelles des éléments remarquables qui peuvent exister ou non:

- On dira que $e \in E$ est un **élément neutre** pour la loi si $\forall a \in E \ ; \ a \star e = e \star a = a$
- On dira que $a^{-1} \in E$ est **l'inverse** de a pour la loi si $a^{-1} \star a = a \star a^{-1} = e$

Ces éléments, si ils existent, sont alors **uniques**.

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.

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 montre alors facilement que **l'intersection** de deux sous-structures est aussi une sous-structure mais que l'union de deux sous-structures n'est en général pas une sous-structure.

[1] **Si la structure impose leur existence**
[2] **Si la structure impose leur existence**

Sous-structure engendrée :

On se donne une partie A de E, on peut alors définir la **sous-structure engendrée** par A. Si on considère $(V_i)_{i\in I}$ la famille des sous-structures de E qui contiennent A, alors on pose:

$$\langle A\rangle = \bigcap_{i\in I} V_i$$

C'est alors clair que c'est la plus petite sous-structure (pour l'inclusion) qui contienne A et on peut alors la caractériser par la propriété suivante:

C'est l'ensemble des combinaisons finies obtenues par applications des lois sur des éléments de A.

Morphismes :

Soit $(E,\star)$ et $(F,\cdot)$ deux ensembles munis de la meme structure[1] et $\varphi : M \to N$, alors φ est appelé **morphisme**, si il vérifie:

$$\forall x, y \in E\ ;\ \varphi(x\star y) = \varphi(x)\cdot\varphi(y)$$

Les morphismes préservent dans une certaine mesure la structure opératoire.

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.

La recherche d'isomorphismes est un thême principal en algèbre des structures, en effet, trouver un isomorphisme entre une structure simple et une structure complexe permet de mieux comprendre cette dernière par l'intermédiaire du morphisme.

Propriétés des morphismes :

Pour une structure donnée, on peut montrer que la composée de morphismes et l'inverse d'un morphisme bijectif est un morphisme. En outre on peut caractériser la structure des images directes et réciproques par un morphisme:

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

Par ailleurs si $F = \langle f_1,\dots,f_n\rangle$ est un sous groupe de E et que ϕ est un morphisme, on a que:

$$\phi(H) = \langle \phi(h_1),\dots,\phi(h_n)\rangle$$

En d'autres termes, **l'image des générateurs engendre l'image**.

Structures Quotients :

On considère maintenant un ensemble quotient $E/_\sim$ tel que E soit muni d'une structure, on cherche alors une condition sur la relation d'équivalence pour que **la structure soit conservée au passage au quotient**. On peut alors montrer que c'est le cas si et seulement si $\sim$ est **compatible** avec les lois, ie que pour toute loi $\star$, on ait:

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

Alors la **surjection canonique** est un morphisme $\pi : E \to E/\sim$ qui a chaque élément associe sa classe d'équivalence pour la relation.

[1] Si les structures présentent plusieurs lois, alors les morphismes doivent vérifier la compatibilité pour **toutes les lois**. Aussi dans le cas particulier de structures qui requièrent l'existence d'un élément neutre, l'image de l'élement neutre de la structure de départ doit être celui de celle d'arrivée.

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:

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

On montre facilement que c'est un sous-groupe (normal) et on peut alors montrer qu'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. On peut alors caractérisé **le sous-groupe engendré** par H (défini au premier chapitre) par:

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

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 que **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:

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

La propriété fondamentale de ces groupes, qui utilise le premier résultat du chapitre suivant est que les sous groupes normaux de G sont exactement les **noyaux** de morphismes de domaine G.

Somme et sommes directes :

Si G est **commutatif**, et que $(H_i)_{i \in I}$ est une famille de sous-groupes, on peut aussi construire une autre structure fondamentale appelée somme de sous-groupes par:

$$\sum_I H_i := \left\{ \sum_I h_i \ ; \ h_i \in H_i \right\}$$

Alors c'est un sous-groupe normal si les sous-groupes termes sont normaux. En outre, si tout élément de cet ensemble se décompose de manière **unique**, ce qui corresponds à dire que e se décompose de manière unique[1], on dira que la somme est **directe** et on notera:

$$\sum_I H_i = \bigoplus_I H_i$$

Si de plus $G = \sum_I H_i$, on dira généralement que les H_i sont **supplémentaires** dans G.

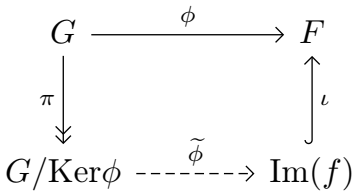
[1] En particulier si $n = 2$, on montre directement qu'une condition nécessaire et suffisante pour que la somme soit directe est que $F \cap G = \{0_E\}$

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.

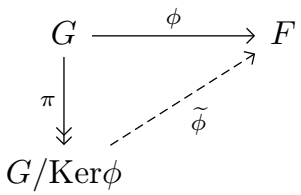
Premier théorème d'isomorphisme :

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]:



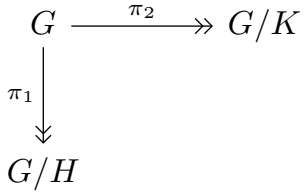
En effet, le passage au quotient rend le morphisme injectif, donc surjectif sur son image, et le diagramme commute, ie on a $\phi = \iota \circ \widetilde{\phi} \circ \pi$.

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:

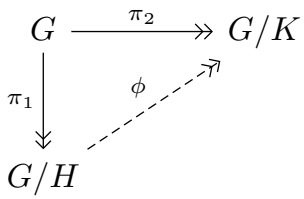


Deuxième théorème d'isomorphisme :

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

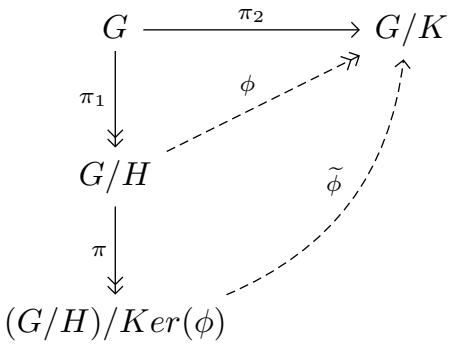


On peut alors utiliser la propriété universelle du quotient pour compléter le diagramme par un morphisme ϕ (par ailleurs surjectif):



[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 $\text{Ker}(\phi) = K/H$ 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.

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:

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

On remarque que ce groupe est doté d'une action naturelle sur $[\![1\ ;\ n]\!]$ donnée par $\sigma \cdot k = \sigma(k)$.

Support :

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

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

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

Cycles :

On appelle **k-cycle**[1] une permutation σ telle qu'il existe $k \geq 2$ et k éléments deux à deux distincts $a_1, \dots, a_k$ tels que:

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

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

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

Exemple: La permutation suivante est un 3-cycle:

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

Cycles et orbites :

Si σ est un k-cycle et que a n'est pas un point fixe, alors on en déduit que la donnée du support de σ est équivalente à la donnée de l'orbite de celle-ci (plus précisément du sous groupe engendré par celle-ci) pour son action naturelle, ie:

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

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] Si $k = 2$, on appellera un tel k-cycle une **transposition**.

Théorème de décomposition en cycles :

Une des problématiques principales à propos des groupes symétriques est la question de la décomposition d'une permutation en permutation plus simples. On peut tout d'abord 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. Il reste à choisir un représentant de chaque orbite et la décomposition en cycles est acquise.

Théorème de décomposition en transpositions :

Par la suite, on peut alors constater directement que pour tout k-cycle $\sigma = (a_1 \ \ldots \ a_k)$, on a une décomposition canonique en produit de transpositions:

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

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:

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

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** $[l_1, \ldots, l_k]$ 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 :

On considère une permutation σ de type $[l_1, \ldots, l_k]$, alors chacun de ses cycles se décompose en **le** produit de $l_i - 1$ transpositions défini ci-dessus. Il est alors naturel de définir alors la fonction suivante:

$$m(\sigma) = \sum_{i \leq k} (l_i - 1)$$

C'est le total du nombre de transpositions dans la décomposition en transpositions définie plus haut. On peut alors définir la **signature** d'une permutation par:

$$\varepsilon(\sigma) = (-1)^{m(\sigma)}$$

On montre alors facilement que cette fonction est un **morphisme de groupe** de $\mathfrak{S}_n \longrightarrow (\{-1, 1\}, \times)$ et que trivialement la signature d'une transposition est -1.

- Si $\varepsilon(\sigma) = 1$, on dira que cette permutation est **paire**.
- Si $\varepsilon(\sigma) = -1$, on dira que cette permutation est **impaire**.

L'ensemble des permutations de signature paire est alors un groupe (c'est le noyau de ε), qu'on appelle **groupe alterné** et qu'on note $\mathfrak{A}_n$.

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.

On considère tout d'abord le groupe quotient $\mathbb{Z}/n\mathbb{Z}$, on peut alors remarque que les éléments de ce groupe sont exactement **les classes de restes possibles par la division euclidienne par** n. On notera l'égalité dans ce contexte $a = b \pmod{n}$ en comprenant que ceci signife que $a + n\mathbb{Z} = b + n\mathbb{Z}$

Classification :

Dans cette section on retourne dans le case d'un groupe cyclique général G et on définit 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).

On remarque alors l'importance du groupe quotient $\mathbb{Z}/n\mathbb{Z}$, c'est le prototype de groupe cyclique fini.

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

On sait donc que ce groupe est **cyclique** d'ordre n, en particulier il est engendré par 1, mais aussi par toutes les classes dont le représentant est premier avec n, en effet si a est un tel élément alors d'aprés le théorème de Bézout, on a:

$$\exists u, v \in \mathbb{Z} \; ; \; au + bn = 1$$

Donc en particulier $a + \ldots + a = 1 \pmod{n}$ et par la suite, a engendre tout le groupe. Il y a donc $\varphi(n)$ générateurs de ce groupe.

Théorème chinois :

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

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

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

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

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. On peux définir une notion de **divisibilité** dans un anneau par la définition naturelle:

$$x \mid y \iff \exists a \in A \ ; \ ax = y$$

On définit aussi de nouveau types d'élément remarquable spécifiques au cas des anneaux:

- On dit qu'un élément $x \in A$ est **un inversible**[1] si il existe y tel que $xy = 1$.
- On dit qu'un élément $x \in A$ est **un diviseur de zéro**[2] si il existe y tel que $xy = 0$.
- On dit qu'un élément $x \in A$ est **un nilpotent** si il existe $n \in \mathbb{N}$ tel que $x^n = 0$.

On dira qu'un anneau sans diviseurs de zéro est **intègre**, et dans ce cas on a la propriété suivante trés puissante:

$$\forall x, y \in A \ ; \ xy = 0 \implies x = 0 \text{ ou } y = 0$$

Exemples :

On peut alors considérer plusieurs anneaux remarquables:

- Les **entiers relatifs** muni des opérations usuelles forment un anneau intègre.
- Les **polynomes** muni de la somme et du produit forment un anneau intègre.
- Les **fonctions continues** muni de la somme et du produit forment un anneau.
- Les **matrices** muni de la somme et du produit forment un anneau.

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 les même hypothèses on a aussi la formule de factorisation:

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1})$$

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:

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

On peut alors imaginer généraliser la notion de sous-groupe normal, ie une sous-structure qui permet que le quotient A/I soit un anneau, mais il se trouve qu'alors la notion de sous-anneau engendré n'est pas la bonne notion.

[1] Ici c'est un inversible **à droite**, on définit de même les inversible **à gauche**.
[2] Ici c'est un diviseur de zéro **à droite**, on définit de même les diviseurs de zéro **à gauche**.

Idéal :

En effet, on se donne un anneau A et un sous-groupe I de A, alors on veut pouvoir définir la multiplication de deux classes telle que celle-ci vérifie la propriété de morphisme de la projection canonique ie:

$$\pi(ab) = \pi(a)\pi(b)$$

Pour ceci, étant données deux classes $a + H$ et $b + H$, alors nécessairement on doit avoir:

$$(a + H)(b + H) = ab + Hb + aH + H = ab + H$$

Ceci nous donne alors la condition supplémentaire sur I pour que ce quotient soit bien défini, on dira alors que I est un **idéal** de A si et seulement si:

$$\forall (a, x) \in A \times I \ ; \ ax \in I$$

En d'autres termes, un idéal est un sous-anneau **stable par multiplication externe** par des éléments de l'anneau. Ceci nous donne alors directement la propriété souhaitée sur les classes et la bonne définition de l'anneau quotient.

Propriétés des idéaux :

Comme les sous-groupes normaux, les idéaux vérifient des propriétés naturelles:

- Toute intersection d'idéaux est un idéal.
- Toute somme d'idéaux est un idéal.
- Tout noyau de morphisme d'anneau est un idéal.
- Tout idéal est un noyau de morphisme d'anneau.

On définit alors **l'idéal engendré** par une partie X qu'on note (X) comme le plus petit idéal qui contient X, en outre si $X = \{x_1, \ldots, x_n\}$, ie si c'est une partie finie, on peut le caractériser par:

$$(X) := \left\{ a_1 x_1 + \ldots + a_n x_n \ ; \ (a_i) \in A \right\}$$

Ce sont en fait exactement les **polynômes** en les éléments de X et à coefficients dans $\mathbb{A}$. Si un idéal est engendré par un uniquement élément, on dira qu'il est **principal**, c'est l'analogue dans les anneaux des sous-groupes cycliques.

Caractéristique :

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

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

Une autre formulation serait simplement que la caractéristique d'un anneau est l'ordre (additif) de l'unité multiplicative. Cette notion est fondamentale car elle permet en fait moralement de détecter des **sous-structures cycliques**. En particulier -> Exemples

II — Arithmétique dans les anneaux

On considère donc la relation de divisiblité dans un anneau $\mathbb{A}$ qu'on considérera intégre et commutatif. Alors le lien naturel entre la divisibilité et la structure naturel d'idéal et donné par la propriété suivante:

$$a \,|\, b \iff (b) \subseteq (a)$$

Les idéaux représentent en fait moralement l'analogue abstrait des multiples.

Elements associés :

On dit que deux éléments $a, b \in \mathbb{A}$ sont **associés** si et seulement si ils vérifient:

$$a \,|\, b \text{ et } b \,|\, a$$

On peut alors montrer que dans ce cas on a égalité des idéaux:

$$(a) = (b)$$

En outre deux éléments sont associés si et seulement si ils sont **égaux à un inversible prés**. Ceci généralise le fait que dans $\mathbb{Z}$, on a $a\mathbb{Z} = b\mathbb{Z} \iff a = \pm b$

Elements irréductibles:

Dans un anneau, on dira qu'un élément x non-nul est **réductible** si et seulement si:

$$\begin{cases} x \text{ n'est } \textbf{pas inversible} \\ \forall a, b \in \mathbb{A} \text{ tel que } x = ab \,;\; a \in \mathcal{U}(A) \text{ ou } b \in \mathcal{U}(\mathbb{A}) \end{cases}$$

En d'autres termes, un élément est irréductible si et seulement si il ne peut pas se factoriser en produit de non-inversibles. De manière analogue, un élément est réductible si une telle factorisation existe.

PGCD et PPCM:

On considère une famille $(a_i)_{i\in I}$ d'éléments de $\mathbb{A}$, on définit les éléments suivants:

- Cette famille admet un **plus grand commun diviseur** qu'on note $\bigwedge_I a_i$ si et seulement si il existe un élément $d \in \mathbb{A}$ vérifiant:
  - **Diviseur commun:** $\forall i \in I \,;\; d \,|\, a_i$
  - **Minimalité:** $\forall d' \in A \,;\; \forall i \in I \,;\; d \,|\, a_i \implies d' \,|\, d$
- Cette famille admet un **plus petit commun multiple** qu'on note $\bigvee_I a_i$ si et seulement si il existe un élément $m \in \mathbb{A}$ vérifiant:
  - **Multiple commun:** $\forall i \in I \,;\; a_i \,|\, m$
  - **Maximalité:** $\forall m' \in A \,;\; \forall i \in I \,;\; a_i \,|\, m \implies m \,|\, m'$

Ces éléments n'existent pas a priori dans un anneau général. Néanmoins quand ils existent on peut montrer qu'ils ne sont en général pas unique, en effet, si d, d' sont des pgcd de $(a_i)_{i\in I}$, alors d et d' sont **associés**, ie **égaux à un inversible prés**.

Elements premiers entre eux:

Pour une famille donnée $(a_i)_{i\in I}$, on dira que ces éléments sont **premiers entre eux** si et seulement si ils admettent un pgcd et que:

$$\bigwedge_I a_i \in \mathcal{U}(\mathbb{A})$$

C'est une généralisation directe de la définition dans $\mathbb{Z}$.

Idéaux premiers et maximaux:

Il existe alors deux types d'idéaux trés importants qui sont définis par la richesse de la structure qu'ils engendrent sur le quotient:

- Si A/I est **intègre**, on dira que I est **premier**.
- Si A/I est **un corps**, on dira que I est **maximal**.

En particulier, on a trivialement que tout idéal maximal est premier. Les anneaux premiers sont un parallèle direct avec les nombres premiers, en effet on peut montrer que I est premier si et seulement si:

$$\forall ab \in I \ ; \ a \in I \text{ ou } b \in I$$

Qui n'est pas sans rapeller le lemme d'Euclide qui dit que si un nombre premier divise un produit, alors il divise l'un des facteurs. On dira alors qu'un élément $a \in \mathbb{A}$ est premier si et seulement si (a) est premier.

Idéaux premiers et maximaux:

II — Arithmétique dans les anneaux

II — Corps

Soit A un anneau dont tout les éléments non-nuls sont inversibles. Alors on dit que A est **un corps** et on le note en général $\mathbb{K}$. Voici quelques exempels de corps remarquables:

- Les **réels** muni des opérations usuelles.
- Les **complexes** 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.

Idéaux maximaux:

Etant donné un anneau intègre et commutatif, on peut vouloir définir, de manière analogue aux idéaux premiers, les idéaux tels que A/I est un corps. On apelle de tels idéaux **idéaux maximaux** et ils vérifient:

$$\forall J \leq \mathbb{A}\ ;\ I \subseteq J \implies J = A \text{ ou } J = I$$

En fait ce sont exactement les idéaux maximaux pour l'inclusion. Cette définition, ainsi que le fait que les $p\mathbb{Z}$ sont facilement maximaux, permet de montrer que $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ sont bien des corps.

Morphismes de corps:

Un morphisme de corps est alors simplement un morphisme d'anneaux. Néanmoins dans ce cas particulier, on peut noter la proposition suivante:

Tout les morphismes de corps sont injectifs.

En particulier ceci nous indique que l'étude des relations entre les corps se ramène à des études d'inclusion abstraites, car si deux corps sont reliés par un morphisme, alors l'un est nécessairement plongé dans l'autre, ou plutôt, l'un est nécessairement une extension de l'autre, ce qui motive la partie suivante.

Extension de corps:

Etant donné deux corps de $\mathbb{K}, \mathbb{F}$, on dira que $\mathbb{F}$ est une **extension** de $\mathbb{K}$ si et seulement si $\mathbb{K} \subseteq \mathbb{F}$ ou plus généralement, si il existe un morphisme de corps (injectif donc) de $\mathbb{K}$ dans $\mathbb{F}$.

Degré d'une extension:

Si $\mathbb{F}$ est une extension de corps de $\mathbb{K}$, alors on peut voir $\mathbb{F}$ comme un $\mathbb{K}$-espace vectoriel. On peut donc calculer sa dimesion que l'on appelle alors **degré de l'extension**, on le note $[\mathbb{F}\ ;\ \mathbb{K}]$

- Si il est fini on dira que l'extension est **finie**.
- Si il est égal à 1 on dira que l'extension est **simple**.
- Si il est égal à 2 on dira que l'extension est **quadratique**.
- ...

Exemple: Si on considère l'extension de $\mathbb{Q}$ donnée par $\mathbb{Q}[\sqrt{2}]$, alors $(1, \sqrt{2})$ est une **base** de $\mathbb{Q}[\sqrt{2}]$, et donc $\dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}]) = 2$ et l'extension est **quadratique**.

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

Propriétés du degré:

Si $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ une suite d'extensions de corps, alors on a la propriété suivante dite de multiplicativité du degré:

$$[\mathbb{L} \,;\, \mathbb{F}] = [\mathbb{L} \,;\, \mathbb{K}][\mathbb{K} \,;\, \mathbb{F}]$$

En particulier, le degré des deux sous-extensions divise celui de l'extension.

Elements algébriques et transcendants:

Etant donnés deux corps $\mathbb{K}, \mathbb{F}$, la théorie des corps se développe alors autour du concept d'élement algébrique et d'élément transcendant, pour tout $\alpha \in \mathcal{F}$, on définit le morphisme suivant:

$$\begin{aligned} \Phi_\alpha : \mathbb{K}[X] &\longrightarrow \mathbb{K}[\alpha] \subseteq \mathbb{F} \\ P &\longmapsto P(\alpha) \end{aligned}$$

C'est le morphisme d'évaluation pour les polynômes de $\mathbb{K}[X]$ dont on a étendu le domaine d'arrivée.

- On dira que α est **transcendant** sur $\mathbb{K}$ si et seulement si ce morphisme est injectif.
- On dira que α est **algébrique** sur $\mathbb{K}$ sinon.

Exemples:

- Si on considère l'inclusion $\mathbb{Q} \subseteq \mathbb{R}$, alors l'élément $\sqrt{2}$ est algébrique sur $\mathbb{Q}$.
- Si on considère l'inclusion $\mathbb{Q} \subseteq \mathbb{Q}[X]$, alors l'élément X est transcendant sur $\mathbb{Q}$.
- On peut montrer que π est transcendant sur $\mathbb{Q}$.

Polynôme minimal d'un élément:

On sait alors que $\mathbb{K}[X]$ est toujours principal, donc si un élément est **algébrique**, alors son noyau est **principal**, ie on a:

$$\ker(\Phi_\alpha) = (P_\alpha)$$

On appelle alors **polynôme minimal** de α l'élément unitaire qui engendre cet idéal. On appelle alors **degré** de α dans $\mathbb{K}$ le degré de ce polynôme. Si α est algébrique, l'intérêt de ce polynôme est alors le suivant, par le premier théorème d'isomorphisme:

$$\mathbb{K}[X]/(\Phi_\alpha) \cong \mathbb{K}[\alpha] \cong \mathbb{K}(\alpha)$$

En outre dans ce cas, $\mathbb{K}[\alpha]$ est un **corps**.

Base d'une extension algébrique:

Si α est algébrique, et que $n = \deg(\Phi_\alpha)$, alors on peut montrer la proposition suivante:

$$(1, \alpha, \ldots, \alpha^{n-1}) \textbf{ est une base de } \mathbb{K}[\alpha]$$

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:

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

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:

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

Forme exponentielle :

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

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

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

$$\begin{aligned} \arg(zz') &= \arg(z) + \arg(z') \pmod{2\pi} \\ \arg\left(\frac{z}{z'}\right) &= \arg(z) - \arg(z') \pmod{2\pi} \end{aligned}$$

Conjugué :

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

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

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.

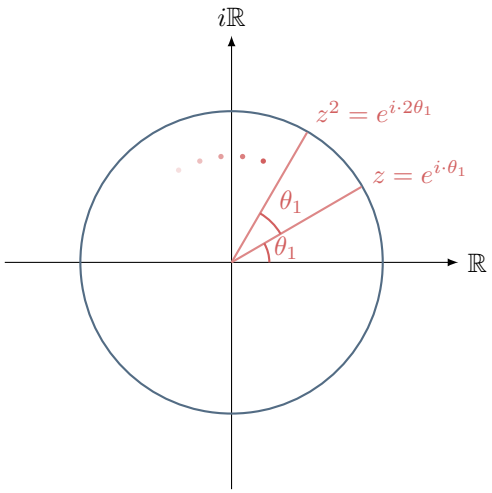
Formule de Moivre :

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:

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

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

Soit $\mathbb{A}$ un anneau commutatif, on construit l'ensemble des **polynômes** à coefficients dans $\mathbb{A}$ comme l'ensemble des suites **nulles à partir d'un certain rang** d'éléments de $\mathbb{A}$, on peut alors munir cet ensemble des opérations naturelles suivantes:

- Une **addition** effectuée termes à termes.
- Une **multiplication par un scalaire** effectuée termes à termes.
- Une **multiplication polynomiale** définie par distributivité comme:

$$PQ = (p_0q_0, p_1q_0 + p_0q_1, \ldots) = \left(\sum_{k=0}^{n} P_kQ_{n-k}\right)_{n\in\mathbb{N}}$$

C'est bien une suite nulle à partir d'un certain rang et elle correspondra alors à la distributivité usuelle[1].

On note alors $X := (0, 1, 0, \ldots)$ et on appelle cette suite **indeterminée**, on remarque alors que:

$$\forall n, m \in \mathbb{N}\ ;\ X^nX^m = X^{n+m}$$

Et par suite que tout polynôme peut s'écrire comme combinaison linéaire de cette indeterminée, ce qui nous donne finalement l'expression canonique d'un polynôme et donc la définition canonique de l'ensemble des polynômes en l'indeterminée X donnée par:

$$\mathbb{A}[X] := \left\{\sum_{n\in\mathbb{N}} a_kX^k\ ;\ (a_k) \in \mathbb{A}^{\mathbb{N}}\right\}$$

Où la suite (a_n) est nulle à partir d'un certain rang.

Structure :

Ces opérations et la structure d'anneau commutatif des coefficients donnent alors une structure **d'anneau commutatif** à l'ensemble $\mathbb{A}[X]$, en outre on pourra aussi vérifier aprés avoir lu le chapitre correspondant que c'est un **espace vectoriel** de dimension infinie, et dont une base est donnée par:

$$(1, X, X^2, \ldots)$$

Finalement, si $\mathbb{A}$ est intégre (par exemple dans le cas usuel où c'est un corps), l'anneau $\mathbb{A}[X]$ l'est aussi.

Evaluation :

Soit R un anneau quelconque qui contient $\mathbb{A}$, et $x \in R$ alors on peut montrer qu'il existe une application fondamentale, dite application **d'évaluation** donné par:

$$\begin{aligned}\phi : \mathbb{A}[X] \times R &\longrightarrow R\\ (P, x) &\longmapsto P(x) = \sum a_kx^k\end{aligned}$$

En effet, si on fixe un élément $x \in R$, alors on a simplement $\forall P \in \mathbb{A}[X]\ ;\ \phi(P, x) = P(x)$ qui est simplement le polynôme inital dont on a substitué l'indeterminée par un élément de l'anneau. En particulier si $R = \mathbb{A}[X]$, on a directement l'identification $P = P(X)$.

[1] C'est un cas particulier de produit de convolution discret, voir le chapitre sur la convolution.

Dans la suite on se restreint au cas $\mathbb{A} = \mathbb{K}$ des polynômes à coefficients dans un corps. Cette contrainte supplémentaire nous permettra de développer une arithmétique plus riche des polynômes.

Degré et Valuation :

Soit $P, Q \in \mathbb{K}[X]$, on peut alors définir tout une propriété fondamentale appelée **degré** de P qui découle directement de la construction des polynômes:

$$\deg(P) := \max\{k \in \mathbb{N} \ ; \ a_k \neq 0\}$$

On a alors les propriétés opératoires du degré ci-dessous:

- **Degré de la somme:** $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$
- **Degré du produit:** $\deg(PQ) = \deg(P) + \deg(Q)$

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

Divisibilité :

On peut naturellement définir une notion de **divisibilité** dans l'anneau $\mathbb{A}[X]$ qui vérifie toute les propriétés usuelles, mais la notion de degré nous permet aussi de définir 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**.

Plus précisément, on a le théorème suivant pour tout couple $A, B \in \mathbb{K}[X]$:

$$\exists!(Q, R) \in \mathbb{K}[X] \ ; \ A = BQ + R \text{ avec } \deg(R) < \deg(B)$$

La démonstration de ce théorème se fait de manière analogue à celui de $\mathbb{Z}$, ie en exhibant l'algorithme de division. Ce théorème donne alors à $\mathbb{K}[X]$ une structure **d'anneau Euclidien**, dont découle les conséquences suivantes:

- **Anneau de Bezout:** La relation de Bezout est vraie pour les polynômes.
- **Anneau principal:** Les idéaux sont principaux.
- **Anneau factoriel:** Il existe une décomposition en facteurs premiers.

Racines:

Soit $\alpha \in \mathbb{K}$ et $P \in \mathbb{K}[X]$, alors on peut montrer le théorème fondamental ci-dessous:

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

On dira alors que α est **racine** de P si une de ces conditions est vérifiée.

Multiplicité:

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

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

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 $m_0, m_1, \ldots, m_{n-1}, m_n$, le lemme de Gauss nous permet de montrer qu'alors:

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

Caractérisation de la multiplicité:

Si on note P^m la dérivée n-ième de P, on peut caractériser le fait que α soit de multiplicité m par:

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

Facteurs premiers :

On appelle **facteurs premiers** de $\mathbb{K}[X]$ les polynômes (non-constants) qui n'admettent pas de **diviseurs stricts** (non-constants), ces éléments dépendents du corps considéré, en effet par exemple:

- **Dans** $\mathbb{R}[X]$**:** X^2+1 est premier.
- **Dans** $\mathbb{C}[X]$**:** $X^2+1=(X-i)(X+i)$ n'est pas premier.

On dira qu'un polynôme est **scindé** sur $\mathbb{K}[X]$ si ses facteurs sont tous de degré 1.

Décomposition :

Un des grans thèmes de l'étude des polynômes est alors la recherche de la décomposition de ceux-ci en facteurs premiers, par exemple:

- Si on considère l'anneau $\mathbb{C}[X]$, on peut alors montrer le **théorème fondamental de l'Algèbre**:

  Tout polynôme non-constant admet une racine.

  Et donc en particulier par récurrence tout les polynômes de $\mathbb{C}[X]$ sont **scindés**.
- Si on considère l'anneau $\mathbb{R}[X]$, il existe donc des polynômes de degré 2 irréductibles. Mais on sait alors qu'il ceux ci ont des racines complexes, et par évaluation on trouve la propriété intéressante suivante:

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

- Si on considère l'anneau $\mathbb{F}_2[X]$, on peut par exemple remarquer la factorisation: $X^2+1=(X+1)^2$

Polynômes en plusieurs indeterminées :

On peut alors généraliser la construction des polynômes en une indeterminée X en un anneau de polynômes en plusieurs indeterminées $\mathbb{A}[X_1,\dots,X_n]$ qu'on définit par récurrence par:

$$\mathbb{A}[X_1,\dots,X_n]=\left(\mathbb{A}[X_1,\dots,X_{n-1}]\right)[X_n]$$

C'est aussi un **anneau commutatif**, aussi intègre si $\mathbb{A}$ l'est et ses éléments sont alors de la forme:

$$\mathbb{A}[X_1,\dots,X_n]:=\left\{\sum_{i_1,\dots,i_n\in\mathbb{N}} a_{i_1,\dots,i_n}X_1^{i_1}\dots X_n^{i_n}\right\}$$

Où la somme est finie, ie où l'ensemble des coefficients $(a_{i_1,\dots,i_n})_{i_1,\dots,i_n\in\mathbb{N}}$ est une famille finie. Quelques exemples:

- **Dans** $\mathbb{R}[X,Y]$**:** $P=2X^2+3XY-Y$
- **Dans** $\mathbb{C}[X,Y,Z]$**:** $P=iX^2Y^2+2iX-5Z$

Relations coefficients racines :

On peut trouver une relation entre les coefficients et les racines d'un polynôme qui peut souvent nous permettre de nous ramener à la résolution d'un système et potentiellement trouver les racines, en effet on suppose la décomposition acquise alors on a:

$$P=\sum_{k=0}^{n}a_kX^k=a_n(X-\alpha_1)\dots(X-\alpha_n)$$

En développant on trouve alors des relations pour la somme, la somme des doubles produits, la somme des triples produits, etc, et le produit des racines:

- **La somme des racines:** $\sum_{1\leq i\leq n}\alpha_i=(-1)^1\frac{a_{n-1}}{a_n}$
- **La somme des k-produits des racines:** $\sum_{1\leq i_1<\dots<i_k\leq n}\alpha_{i_1}\dots\alpha_{i_k}=(-1)^k\frac{a_{n-k}}{a_n}$
- **Le produit des racines:** $\alpha_1\dots\alpha_n=(-1)^n\frac{a_0}{a_n}$