Chapitre 1

Algèbre générale

Sommaire

1.1 Relation d'équivalence

1.1.1 Définitions

Relations binaires

Une relation binaire sur un ensemble E est une partie de E^2

Relations d'équivalences

Ce sont des relations binaires qui vérifient :

1. réflexivité : $\forall x \in, x\mathcal{R}x$
2. symétrique : $\forall (x,y) \in E^2, x\mathcal{R}y \Leftrightarrow y\mathcal{R}x$
3. transitivité : $\forall (x,y,z) \in E^3, x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$

Deux éléments sont en relation si et seulement si ils ont une valeur commune

Exemples

1. L'égalité
2. Les classes d'un lycée, tranches d'imposition
3. Soit $f : E \longrightarrow F$ une application :

$$xRy \Leftrightarrow f(x) = f(y)$$

Congruences

Soit $n \in \mathbb{N}^*$:

$$x \equiv y[n] \Leftrightarrow n \mid x - y$$

Relation caractéristique d'un groupe

Soit G un groupe et H un sous groupe de G, on définit la relation $\mathcal{R}$:

$$x\mathcal{R}y \Leftrightarrow x^{-1}y \in H$$

1. $x^{-1}x = e \in H : x\mathcal{R}x$
2. $x^{-1}y \in H \Leftrightarrow (yx^{-1})^{-1} \in H \Leftrightarrow xy^{-1} \in H$ donc, $xRy \Leftrightarrow y\mathcal{R}x$
3. xRy et $yRz \Rightarrow (x^{-1}y, y^{-1}z) \in H \Rightarrow x^{-1}(yy^{-1})z \in H \Rightarrow x^{-1}z \in H$

1.1.2 Classes d'équivalences, ensemble quotient

Définition

Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. Soit $x \in E$, on définit la classe de x :

$$\bar{x} = Cl(x) = \{y \in E / y\mathcal{R}x\}$$

Théorème

2 classes distinctes sont soient égales soient disjointes :

$$\forall (x,y) \in E^2, \bar{x} = \bar{y} \text{ ou } \bar{x} \cap \bar{y} = \emptyset$$

Ensemble quotient

L'ensemble des classes d'équivalences s'appelle l'ensemble quotient, noté :

$$\frac{E}{\mathcal{R}}$$

Remarque : on peut définir une relation d'équivalence sur chaque partition

Étude de cas particulier

Soit $n \in \mathbb{N}*$, on note l'ensemble quotient de la relation congruences modulo n sur $\mathbb{Z}$ est noté :

$$\frac{\mathbb{Z}}{n\mathbb{Z}}$$

On note $card(\frac{\mathbb{Z}}{n\mathbb{Z}}) = n$

Preuve : $n_0 \in \mathbb{Z}$, par division euclidienne :

$\exists !(q,r) \in \mathbb{Z} \times [\![0; n-1]\!] / n_0 = qn + r \Rightarrow n_0 \in \bar{r}$

$r, r' \in [\![0; n-1]\!], \bar{r} = \bar{r'} \Rightarrow r = \bar{r'}$

Théorème de Lagrange (HP)

Soit $(G, \cdot)$ et H un sous-groupe de G, G fini et $\mathcal{R}$ la relation d'équivalence sur G :

$$x\mathcal{R}y \Leftrightarrow x^{-1}y \in H \Leftrightarrow \exists h \in H, x^{-1}y = h \Leftrightarrow \exists h \in H, y = xh$$

Il vient : $\bar{x} = \{xh/h \in H\} = xH$
Or : $\begin{array}{ccccc} \varphi & : & H & \to & xH \\ & & x & \mapsto & xh \end{array}$
est surjective et par définition de xH est injective car x est inversible.
On a donc : $card(xH) = card(\frac{G}{\mathcal{R}})card(H)$

Il vient le corollaire suivant : si G est un groupe fini et H un sous-groupe de G, alors :

$$card(H) \mid card(G)$$

Par conséquent un groupe de cardinal premier admet deux sous-groupe : e et lui même

1.1.3 Relation compatible avec une loi

Soit (E,*) un magma et $\mathcal{R}$ une relation d'équivalence. On souhaite définir une loi * sur $\frac{E}{R}$ telle que :

$$\bar{x} * \bar{y} = \overline{x * y}$$

Pour ce faire il faut que si $\bar{x} = \bar{x'}$ et $\bar{y} = \bar{y'}$ alors $\overline{x * y} = \overline{x' * y'}$, il y a indépendance du représentant choisit

Définition

On dit que * est compatible avec R si et seulement si :

$$\forall (x, x', y, y') \in E^4, x\mathcal{R}x' \text{ et } y\mathcal{R}y' \Rightarrow x * y\mathcal{R}x' * y'$$

Dans ce cas on peut définir la loi quotient sur $\frac{E}{R}$: $\bar{x} * \bar{y} = \overline{x * y}$

Théorème

Si * possède un neutre e alors la loi quotient a pour neutre $\bar{e}$
Si x est associative (resp. commutative) alors la loi quotient l'est aussi
Si x est inversible pour * alors $\bar{x^{-1}} = \bar{x}^{-1}$
Si (E,*) est un groupe alors ($\frac{E}{\mathcal{R}}$,*) l'est aussi

Cas de $\frac{\mathbb{Z}}{n\mathbb{Z}}$

On peut munir $\frac{\mathbb{Z}}{n\mathbb{Z}}$ d'une loi de groupe notée $+$ pour :

$$\bar{x} + \bar{y} = \overline{x + y}$$
$$\bar{0} \text{ est le neutre}$$
$$-\bar{x} = \bar{-x} = \overline{n - x}$$

Exemple :

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

1.2 Structure de groupes

1.2.1 Morphismes de groupes

Définition

Soient $(G,\cdot)$ et $(G',*)$ deux groupes. On dit qu'une application φ de G dans G' est un (homo)morphisme de groupe si :

$$\forall (x,y)\in G^2, \varphi(x\cdot y)=\varphi(x)*\varphi(y)$$

Dans ce cas : $\varphi(e)=e'$ et $\forall x\in G, \varphi(x^{-1})=\varphi(x)^{-1}$

Preuve : $\varphi(e\cdot e)=\varphi(e)$ et $\varphi(e\cdot e)=\varphi(e)^2 \Rightarrow \varphi(e)=e'$
$\varphi(x\cdot x^{-1})=\varphi(x)*\varphi(x^{-1})$ et $\varphi(x\cdot x^{-1})=\varphi(e)=e' \Rightarrow \varphi(x)*\varphi(x^{-1})=e' \Rightarrow \varphi(x^{-1})=\varphi(x)^{-1}$

Exemples

1. $x\in G$ et $\begin{array}{rccc}\varphi & : & (\mathbb{Z},+) & \to & (G,\cdot)\\ & & n & \mapsto & x^n\end{array}$
   $\varphi(n_1+n_2)=x^{n_1+n_2}=x^{n_1}\cdot x^{n_2}=\varphi(n_1)\cdot\varphi(n_2)$
2. $\begin{array}{rccc}\ln & : & (\mathbb{R}_+^*,\times) & \to & (\mathbb{R},+)\\ & & x & \mapsto & \ln(x)\end{array}$
   $\ln(xy)=\ln(x)+\ln(y)$
3. $\begin{array}{rccc}\varphi & : & (\mathbb{R}_+^*,+) & \to & (\mathbb{C}^*,\times)\\ & & \theta & \mapsto & exp(i\theta)\end{array}$
4. L'identité est un morphisme de groupe
5. Le morphisme trivial qui envoie tous les éléments sur le neutre est un morphisme de groupe

Isomorphismes

Ce sont des morphismes bijectifs de $(G,\cdot)$ dans $(G',*)$. Dans ce cas l'application réciproque est aussi un morphisme de groupes. On dit que G et G' sont isomorphes, un isomorphisme transporte fidèlement la structure de G sur celle de G', ils ont les mêmes propriétés

Preuve :

$\forall (x',y')\in G'^2, f(f^{-1}(x'*y'))=x'*y'=f(f^{-1}x')*f(f^{-1}y')=f(f^{-1}(x')*f^{-1}(y'))$
f étant bijective : $f^{-1}(x'*y')=f^{-1}(x')*f^{-1}(y')$

Exemples

1. $\ln : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +)$ est bijectif, c'est un isomorphisme de groupe
2. Sa réciproque $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \times)$ est aussi un isomorphisme de groupe
3. Soit $\{e; a; b\}$ un groupe a 3 éléments, montrons que si $(G, \cdot)$ est un groupe , $\forall g \in G$ $\begin{array}{rccc} \tau & : & G & \to & G \\ & & x & \mapsto & gx \end{array}$ est bijective. Dans une table de groupe, chaque élément apparaît une et une seule fois dans chaque ligne et chaque colonne :

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

est la seule loi possible, tout les groupes à 3 éléments sont isomorphes à $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Image et Image réciproque d'un morphisme

Soit $f : G \longrightarrow G'$ un morphisme de groupe

1. Soit H un sous-groupe de G alors $f(H)$ est un sous-groupe de G'
2. Soit H' un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G
3. Lorsque H=G, $f(G)$ est un sous-groupe de G' appelé image de f noté $Im(f)$:
$$f \text{ est surjective} \Leftrightarrow Im(f) = G'$$
4. Lorsque $H' = \{e\}, f^{-1}(\{e\}) = \{x \in G / f(x) = e'\}$ est un sous-groupe de G, appelé noyau de f, noté $Ker(f)$.
$$f \text{ est injective} \Leftrightarrow Ker(f) = \{e\}$$

Preuve :

1. $e \in H \Rightarrow e' = f(e) \in H$
Soit $(x', y') \in f(H)^2 : \exists (x, y) \in H^2$,
$$\begin{aligned} x' &= f(x) \\ y' &= f(y) \end{aligned}$$
$x' \cdot (y')^{-1} = f(x) * f(y)^{-1} = f(x) * f(y^{-1}) = f(x \cdot y^{-1}) \in f(H)$
$$f(H) \text{ est un sous-groupe de G'}$$
2. $f(e) = e' \in H' \Rightarrow e \in f^{-1}(H')$, soit $(x, y) \in f^{-1}(H')^2, f(xy^{-1}) = f(x) * f(y)^{-1} \in H'$
$$f^{-1}(H') \text{ est un sous-groupe de G}$$
3. Si f est injective : $x \in Ker(f) \Rightarrow f(x) = e' \Rightarrow f(x) = f(e) \Rightarrow x = e$
$$Ker(f) = \{e\}$$
Si $Ker(f) = \{e\} : (x, y) \in G^2$
$$\begin{aligned} f(x) = f(y) &\Leftrightarrow f(x)f(y)^{-1} = e \\ &\Leftrightarrow f(xy^{-1}) = e \\ &\Leftrightarrow xy^{-1} = e \\ &\Leftrightarrow x = y \end{aligned}$$
$$f \text{ est injective}$$

Remarque

Si f est un morphisme de groupes quelconque. Soit $(x_1, x_2) \in G^2$

$$f(x_1) = f(x_2) \Leftrightarrow x_1 x_2^{-1} \in Ker(f) \Leftrightarrow x_1^{-1} x_2 \in Ker(f)$$

Si la loi de G est notée $+$:

$$f(x_1) = f(x_2) \Leftrightarrow x_1 - x_2 \in Ker(f) \Leftrightarrow x_2 = x_1 + Ker(f)$$

Décomposition canonique d'un morphisme (HP)

Soit $f : (G, \cdot) \longrightarrow (G', *)$ est un morphisme de groupes. La relation d'équivalence $\mathcal{R}$ définie sur G par :

$$\forall (x, y) \in G^2, x \mathcal{R} y \Leftrightarrow f(x) = f(y) \Leftrightarrow xy^{-1} \in Ker(f)$$

Cette relation d'équivalence est compatible avec la loi $\cdot$. On peut alors munir l'ensemble quotient, noté $\frac{G}{Ker(f)}$ d'une structure de groupe. De plus, l'application

$$\begin{array}{rccc} \overline{f} & : & \frac{G}{Ker(f)} & \to & Im(f) \\ & & \overline{x} & \mapsto & \overline{f}(\overline{x}) = f(x) \end{array}$$

est bien définie et est un isomorphisme de $\frac{G}{Ker(f)}$ sur $Im(f)$

Preuve : soit $(x, x', y, y') \in G^4 x \mathcal{R} y$ et $x' \mathcal{R} y'$ on a : $xy \mathcal{R} x'y'$
Soit $(x, x') \in G^2$, telle que $\overline{x} = \overline{x'}$ alors $f(x) = f(x')$, on peut donc définir :

$$\overline{f}(\overline{x}) = f(x) \text{ indépendamment du représentant choisi}$$

De plus soit $(x, y) \in G^2$:

$$\overline{f}(\overline{x} \cdot \overline{y}) = \overline{f}(\overline{x \cdot y}) = f(x \cdot y) = f(x) * f(y) = \overline{f}(\overline{x}) * \overline{f}(\overline{y})$$

$$\overline{f} \text{ est un morphisme de } \frac{G}{Ker(f)} \text{ dans } Im(f)$$

$\overline{f}$ est surjective, car on réduit l'ensemble d'arrivée à l'ensemble des images

$\overline{f}$ est injective car :

$$\begin{array}{rcl} \forall x \in G, \overline{x} \in Ker(\overline{f}) & \Leftrightarrow & \overline{f}(\overline{x}) = e' \\ & \Leftrightarrow & f(x) = e' \\ & \Leftrightarrow & x \in Ker(f) = \overline{e} \\ & \Leftrightarrow & \overline{x} = \overline{e} \end{array}$$

$$Ker(\overline{f}) = \{e\}$$

1.2.2 Sous-groupes, groupes engendrés par une partie

Définition

Soit (G, ·) un groupe, une partie H de G est un sous-groupe si et seulement si :

1. $H \subset G$
2. $e \in H$
3. $\forall (x,y) \in H^2, xy^{-1} \in H$

Alors H est un groupe. De plus toute intersection de sous-groupe de G est un sous-groupe de G

⚠Soit H_1, H_2 deux sous-groupes de G, tel que $H_1 \nsubseteq H_2$ et $H_2 \nsubseteq H_1$. Soit alors $x \in H_1 \setminus H_2$ et $y \in H_2 \setminus H_1$.
Si $H_1 \cup H_2$ était un sous-groupe de G, on aurait :

$$\begin{aligned} xy \in H_1 \cup H_2 &\Rightarrow xy \in H_1, xy \in H_2 \\ &\Rightarrow x = (xy)y^{-1} \in H_2 \end{aligned}$$

Ce qui est absurde

Sous-groupe engendré

Soit $(G, \cdot)$ un groupe, $\mathcal{A}$ une partie quelconque de G. On appelle sous-groupe engendré par $\mathcal{A}$ et on notre $gr(\mathcal{A})$, l'intersection de tous les sous-groupes de G contenant $\mathcal{A}$, on a :

$gr(\mathcal{A})$ est un sous-groupe de G, contenant $\mathcal{A}$
Tout sous-groupe de G contenant $\mathcal{A}$ contient $gr(\mathcal{A})$

Cette propriété caractérise $gr(\mathcal{A})$, le plus petit (au sens de l'inclusion) sous-groupe de G contenant $\mathcal{A}$. On dit que $\mathcal{A}$ est génératrice de G si et seulement si $gr(\mathcal{A}) = G$

Exemples

1. $gr(\varnothing) = \{e\}$, intersection de tous les sous-groupes de G
2. $\mathcal{A}$ est un sous-groupe de de G $\Leftrightarrow gr(\mathcal{A}) = \mathcal{A}$
3. Soit $x \in G$, $gr(\mathcal{A}) = \{x^n / n \in \mathbb{Z}\}$
   Preuve : $\begin{array}{cccc} f & : & \mathbb{Z} & \to & G \\ & & n & \mapsto & x^n \end{array}$ est un morphisme de groupe
   $\{x^n / n \in \mathbb{Z}\} = Im(f)$ est un sous-groupe de G, il contient x.
   Soit H un sous-groupe de G contenant x, la loi · étant interne alors $\forall n \in \mathbb{Z}, x^n \in H$ donc $\{x^n / n \in \mathbb{Z}\} \subset H$, d'où :

$$gr(\mathcal{A}) = \{x^n / n \in \mathbb{Z}\}$$

Remarque

Généralement on vérifie que :

$$gr(\mathcal{A}) = \{a_1^{\varepsilon_1} ... a_n^{\varepsilon_n} / n \in \mathbb{N}, (a_1, ..., a_n) \in \mathcal{A}^n, \varepsilon_k \in \{-1; 1\}$$

Dans σ_n, l'ensemble des transpositions est générateur
Dans le groupe des isométries du plan, l'ensemble des symétries orthogonales par rapport à une droite est générateur

1.2.3 Groupes monogènes, groupes cycliques

Définitions

Un groupe monogène est engendré par un seul élément :

$$G = \{x^n / n \in \mathbb{Z}\} \text{ ou } \{nx / n \in \mathbb{Z}\}$$

Un groupe cyclique est monogène et fini

Exemples

1. $(\mathbb{Z}, +) = gr\{1\}$ est monogène
2. $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +) = gr\{1\}$ est cyclique
3. Tout sous-groupe de $(\mathbb{Z}, +)$ est monogène. En effet, soit H un sous-groupe de $(\mathbb{Z}, +)$ alors $H = n\mathbb{Z} = gr\{n\}$

Théorème de structure

Soit $G = gr\{x\}$ un groupe monogène,l'application : $\begin{array}{ccccc} \varphi & : & \mathbb{Z} & \to & G \\ & & n & \mapsto & x^n \end{array}$ est un morphisme de groupe injectif.
$Ker(f)$ est un sous-groupe de $\mathbb{Z}, \exists! n \in \mathbb{N}, Ker(f) = n\mathbb{Z}$
Si n=0 alors $Ker(f) = \{0\}$, f est un isomorphisme de $(\mathbb{Z}, +)$ dans $(G, \cdot)$ infini
Si n >0 alors $\begin{array}{ccccc} \overline{\varphi} & : & \frac{\mathbb{Z}}{n\mathbb{Z}} & \to & G \\ & & \overline{k} & \mapsto & x^k \end{array}$ alors card(G) = card($\frac{\mathbb{Z}}{n\mathbb{Z}}$) = n. On définit un isomorphisme de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ dans G

Preuve : n=0 , $Ker(f) = \{0\}$ et f est bijective : c'est un isomorphisme
n>0 : $\overline{f}$ est bien définie, car si $\overline{k} = \overline{k'}$ alors $n \mid k - k' \Rightarrow k - k' \in n\mathbb{Z} = Ker(f))$
Par conséquent $f(k - k') = e = x^{k-k'} \Rightarrow x^k = x^{k'}$
Par construction $\overline{f}$ est surjective et c'est un morphisme car :

$$\begin{aligned} \forall (k, k') \in \mathbb{Z}^2, \overline{f}(\overline{k} + \overline{k'}) &= \overline{f}(\overline{k + k'}) \\ &= f(k + k') \\ &= \overline{f}(\overline{k}) \cdot \overline{f}(\overline{k'}) \end{aligned}$$

Enfin, $\forall k \in \mathbb{Z}, f(k) = e \Leftrightarrow \overline{f}(\overline{k}) = e \Leftrightarrow \overline{k} = \overline{0}$

$\overline{f}$ est bijective

Exemples

Soit $n \in \mathbb{N}^*, \mathbb{U}_n = \{e^{\frac{2ik\pi}{n}}/k \in [|0; n-1|]\} = gr\{e^{\frac{2i\pi}{n}}\}$ C'est un groupe monogène fini, il est cyclique. On peut définir le morphisme :

$$\begin{array}{rccc} \psi & : & \frac{\mathbb{Z}}{n\mathbb{Z}} & \to & \mathbb{U}_n \\ & & \bar{k} & \mapsto & e^{\frac{2ik\pi}{n}} \end{array}$$

Ordre d'un élément

1. Soit G un groupe et $x \in G$, si $gr\{x\}$ est fini de cardinal $n \in \mathbb{N}^*$, on dit que x est d'ordre fini n, noté : $\omega(x) = n$, cette notation n'est pas universelle
2. Par définition $x = min\{k \in \mathbb{N}^*/x^k = e\}$. n est caractérisé par : $Ker(f) = n\mathbb{Z}$, c'est à dire :

$$\forall k \in \mathbb{Z}, x^k = e \Leftrightarrow n|k$$

Exemples

1. $\omega(e) = 1$, e est le seul élément d'ordre 1
2. $\omega((i,j)) = 2$ car $(i,j)^2 = id$. En effet l'ordre divise 2 mais n'est pas 1 car ce n'est pas l'identité
3. Il en découle que l'ordre d'un p-cycle est p
4. Dans $(\mathcal{O}, \circ)$ une symétrie vectorielle orthogonale par rapport à une droite est d'ordre 2
5. Soit $\theta \in \mathbb{R}/\frac{\theta}{\pi} \notin \mathbb{Q}$. On considère $\mathcal{R}_\theta$:

$$\forall k \in \mathbb{Z}, (\theta)^n = \mathcal{R}_{n\theta} = id \Leftrightarrow n \in 2\pi\mathbb{Z} \Leftrightarrow \frac{\theta}{\pi} \in \mathbb{Q}$$

   Ce qui est absurde, donc cette rotation n'est pas d'ordre fini
6. Soit $n \in \mathbb{N}^*$ et $m \in \mathbb{Z}$, on recherche l'ordre de $\overline{m}$ dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$

$$\begin{array}{rcl} k \in \mathbb{Z}, k\overline{m} = \bar{0} & \Leftrightarrow & \overline{km} = \bar{0} \\ & \Leftrightarrow & n|km \\ & \Leftrightarrow & n_1(n \wedge m)|km_1(n \wedge m),\ n_1 \wedge m_1 = 1 \\ & \Leftrightarrow & n_1|km_1,\ \wedge m_1 = 1 \end{array}$$

   D'après le théorème de Gauss : $n_1|k$, ainsi :

$$\omega(\overline{m}) = n_1 = \frac{n}{n \wedge m}$$

   Il vient pour n=6 :

$$\begin{array}{c} gr\{\bar{0}\} = \bar{0} \\ gr\{\bar{1}\} = \bar{1} \\ gr\{\bar{2}\} = \{\bar{0}; \bar{2}; \bar{4}\} \\ gr\{\bar{3}\} = \{\bar{0}; \bar{3}\} \\ gr\{\bar{4}\} = \{\bar{0}; \bar{4}; \bar{2}\} \\ gr\{\bar{5}\} = \{\bar{0}; \bar{5}; \bar{4}; \bar{3}; \bar{2}; \bar{1}\} = \frac{\mathbb{Z}}{6\mathbb{Z}} \end{array}$$

7. (ENS) Soit G un groupe abélien fini, on définit l'exposant de G, $m = \bigvee_{x \in G} \omega(x)$

   $\forall x \in G, \omega(x)|m$ donc $x^m = e$. Montrer que :

   $$\exists x_0 \in G / \omega(x) = m$$

   Indication : on pourra considérer la décomposition en produit de facteurs premiers de m. Définissons tout d'abord la valuation p-adique : $\nu_p(n)$ est l'exposant de p dans la décomposition en produit de facteurs premiers de m :

   $$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$$

   On observe les propriétés suivantes :

   $$\begin{gathered} a|b \Leftrightarrow \forall p \in \mathbb{P}, \nu_p(a) \leq \nu_p(b) \\ \nu_p(a \wedge b) = min(\nu_p(a), \nu_p(b)) \\ \nu_p(a \vee b) = max(\nu_p(a), \nu_p(b)) \end{gathered}$$

   donc, $\nu_p(m) = max_{x \in G}(\nu_{p_i}(\omega(x)))$
   $\exists y_i \in G / \nu_{p_i}(\omega(y_i)) = \alpha_i$ et $\exists k_i \in \mathbb{N} / \omega(k_i) = p_i^{\alpha_i} k_i$
   Posons : $x_i = y_i^{k_i}$

   $$\begin{aligned} n \in \mathbb{N}, x_i^n = e &\Leftrightarrow y_i^{nk_i} = e \\ &\Leftrightarrow p_i^{\alpha_i} k_i | nk_i \\ &\Leftrightarrow p_i^{\alpha_i} | n \end{aligned}$$

   Par conséquent $\omega(x_i) = p_i^{\alpha_i}$. Soit $x = x_1 ... x_r$:

   $$\begin{aligned} n \in x^n = e &\Rightarrow x_1^n ... x_r^n = e \\ &\Rightarrow x_1^{np_2^{\alpha_2} ... p_r^{\alpha_r}} (x_2^n ... x_r^n)^{p_2^{\alpha_2} ... p_r^{\alpha_r}} = e \\ &\Rightarrow x_1^{np_2^{\alpha_2} ... p_r^{\alpha_r}} = e \\ &\Rightarrow p_1^{\alpha_i} | np_2^{\alpha_2} ... p_r^{\alpha_r} \\ &\Rightarrow p_1^{\alpha_i} | n, \text{théorème de Gauss} \end{aligned}$$

   De même pour les autres facteurs, d'où :

   $$m = p_1^{\alpha_1} ... p_r^{\alpha_r} | n$$

   Si m|n alors $x^n = e$ car $x^m = e$ donc $\omega(x) = m$. Ce résultats devient faux si G n'est pas abélien, par exemple : σ_3

Théorème

Soit G un groupe fini de cardinal n non nul et $x \in G$:

1. $\omega(x)|n$
2. $x^n = e$

Preuve :

1. Découle du théorème de Lagrange
2. $\omega(x)|n \Rightarrow x^n = e$
   Dans le cas où G est abélien on peut considérer :
   Soit $x_0 \in G$ l'application : $\begin{array}{rccc} \tau_{x_0} & : & G & \to & G \\ & & \overline{x} & \mapsto & x_0 x \end{array}$ est bijective :

$$a = \prod_{x \in G} x_0 x = x_0^n \prod_{x \in G} x$$

$$x_0^n = e$$

Exemple

Soit $(\mathbb{U}, \times)$ et G un sous-groupe fini de cardinal n :

$$x^n = 1 \text{ et } card(G) = n \Rightarrow G \subset \mathbb{U}_n \Rightarrow G = \mathbb{U}_n$$

En outre,les sous-groupes de $\mathbb{U}_n$, H sont des sous-groupes de $\mathbb{U}$ fini :

$$\exists d \in \mathbb{N}^*, H = \mathbb{U}_d$$
$$d|n \text{ d'après le théorème de Lagrange}$$

Les sou-groupes de $\mathbb{U}_n$ sont donc cyclique de cardinal d|n . Tout groupe cyclique a n éléments est isomorphe à $\mathbb{U}_n$: les sous-groupes d'un groupe cyclique sont cycliques.

$\forall d/d|n, \exists!$ un unique sous-groupe de cardinal ("ordre") d dans un groupe cyclique à n éléments

Dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ l'unique sous-groupe à d éléments est :

$$gr\{\overline{\frac{n}{d}}\}$$

Théorème

1. Soit x un élément d'ordre fini nm alors :

$$\omega(x^n) = m$$

2. Soit $f : G \mapsto G'$ un morphisme de groupes, on a :

$$\forall x \in G, \omega(f(x))|\omega(x)$$

   Si de plus f est injective alors $\omega(f(x)) = \omega(x)$

Preuve :

1.

$$\begin{array}{rcl} \text{Soit} k \in \mathbb{Z}, (x^n)^k & \Leftrightarrow & x^{nk} = e \\ & \Leftrightarrow & nm|nk \\ & \Leftrightarrow & m|k \end{array}$$

$$\omega(x^n) = m$$

2. $f(x^{\omega(x)}) = e' \Leftrightarrow f(x)^{\omega(x)}|e \Leftrightarrow \omega(f(x))|\omega(x)$
   Si f est injective :

$$\begin{aligned} \forall k \in \mathbb{Z}, f(x)^k = e' &= f(x^k) = e' \\ &= x^k = e \\ &= \omega(x)|k \end{aligned}$$

$$\omega(f(x)) = \omega(x)$$

Exemple

Combien y a-t-il de morphismes de $\frac{\mathbb{Z}}{6\mathbb{Z}}$ dans $\frac{\mathbb{Z}}{14\mathbb{Z}}$?
Soit f un tel morphisme : il est entièrement déterminé par $\bar{1}$:

$$\forall k \in \mathbb{Z}, f(\bar{k}) = kf(\bar{1})$$

$f(\bar{1}) \in \frac{\mathbb{Z}}{14\mathbb{Z}} \Rightarrow \omega(f(\bar{1}))|14$ et $\omega(f(\bar{1}))|\omega(\bar{1}) = 6$ Il vient :

$$\begin{gathered} \omega(f(\bar{1})) = 1 \Rightarrow f \text{ est le morphisme trivial} \\ \omega(f(\bar{1})) = 2 \Rightarrow f(\bar{1}) = \tilde{7} \\ f(\bar{k}) = \tilde{7k} \end{gathered}$$

1.2.4 Groupe produit

Définition

Soit $(G_i)_{i\in[|1;n|]}$ une famille de groupe. On définit une loi produit sur $G_1 \times ... \times G_n$:

$$\begin{gathered} \forall((x_1;...;x_n),(y_1;...;y_n)) \in (G_1 \times ... \times G_n)^2 \\ (x_1;...;x_n)\cdot(y_1;...;y_n) = (x_1y_1;...;x_ny_n) \end{gathered}$$

Théorème

Muni de cette loi, $G_1 \times ... \times G_n$ est un groupe, dit groupe produit.
Son neutre est : $(e_1;...;e_n)$ et on a : $(x_1;...;x_n)^{-1} = (x_1^{-1};...;x_n^{-1})$.
De plus si chacun des groupes G_i est abélien, alors le groupe produit l'est aussi.

Groupe de Klein

$K = \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$

	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

C'est un groupe de cardinal 4 non isomorphe à $\frac{\mathbb{Z}}{4\mathbb{Z}}$, tel que chaque élément a son propre inverse. C'est le groupe qui laisse invariant la molécule d'éthylène.

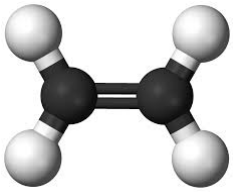


FIGURE 1.1 – Molécule d'éthylène

1.2.5 Groupes de cardinal premier

Soit $p \in \mathbb{P}$, où $\mathbb{P}$ désigne l'ensemble des nombres premiers. Tout groupe de cardinal p est cyclique et isomorphe à $\frac{\mathbb{Z}}{p\mathbb{Z}}$

Preuve : $x \in G \setminus \{e\}, \omega(x) \neq 1$ et $\omega(x)|p$, donc :

$$\omega(x) = p$$
$$G = gr\{x\}$$

1.2.6 Groupe symétrique

Définition

Pour $n \geq 2$, on note $(\sigma_n, \circ)$ le groupe symétrique, l'ensemble des permutations de $[|1;n|]$. Il est non commutatif dès que $n \geq 3$.
Soit $\sigma \in \sigma_n$ et $l \in [|1;n|]$:

$$\forall k \in \mathbb{N}, \sigma^k(l) \in [|1;n|]$$
$$\exists i < j \in [|1;n|]^2 / \sigma^i(l) = \sigma^j(l)$$
$$\text{d'où, } \sigma^{j-i}(l) = l, j - i \in [|1;n|]$$

On peut donc considérer $m = \min\{k \in \mathbb{N}^* / \sigma^k(l) = l\}$. Alors $\{l; \sigma(l); ...; \sigma^{m-1}(l)\}$ sont distincts et $\sigma^m(l)$ est appelé l'orbite de σ .

Orbites sur σ

Les orbites sur σ sont les classes d'équivalence de la relation définie sur $[|1;n|]$ par :

$$i\mathcal{R}j \Leftrightarrow \exists k \in \mathbb{Z} / j = \sigma^k(i)$$

Exemple

Soit pour $\sigma \in \sigma_{10}$: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 6 & 7 & 4 & 9 & 10 & 8 & 3 & 1 & 2 \end{pmatrix}$

Il vient :

$$\sigma = (1 \quad 5 \quad 9) \circ (2 \quad 6 \quad 10) \circ (3 \quad 7 \quad 8)$$

On en déduit les orbites :

$$\{1;5;9\}; \{2;6;10\}; \{3;7;8\}; \{4\}$$

Théorème

Pour chaque orbite de cardinal m, σ agit comme un cycle de longueur m. Rappelons qu'on note $(a_1;...;a_m)$ le cycle tel que :

$(a_1;...;a_m)(a_i) = a_{i+1}$ si $1 \leq i \leq m-1$
$(a_1;...;a_m)(a_m) = a_1$
$\forall k \notin \{a_1;...;a_n\}, (a_1;...;a_m)(k) = k$

Propriétés

1. Toute permutation peut se décomposer de manière unique à l'ordre des facteurs près en un produit de cycles à support disjoints
2. $(a_1;...;a_m) = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_2 & a_3 \end{pmatrix} \circ ... \circ \begin{pmatrix} a_{m-1} & a_m \end{pmatrix}$
3. Soit $\sigma \in \sigma_n$, $\sigma \circ (a_1;...;a_m) \circ \sigma^{-1} = (\sigma(a_1);...;\sigma(a_m))$, cette opération est la conjugaison
4. Deux m-cycles sont conjugués dans σ_n

Preuve :

1. découle du théorème des orbites
2. $\forall i \in [|1; n-1|], \begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_2 & a_3 \end{pmatrix} \circ ... \circ \begin{pmatrix} a_{m-1} & a_m \end{pmatrix} (a_i) = a_{i+1}$
   $\begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_2 & a_3 \end{pmatrix} \circ ... \circ \begin{pmatrix} a_{m-1} & a_m \end{pmatrix} (a_m) = a_1$
   $\forall k \notin \{a_1;...;a_m\}, \begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_2 & a_3 \end{pmatrix} \circ ... \circ \begin{pmatrix} a_{m-1} & a_m \end{pmatrix} (k) = k$
3. $\sigma \circ (a_1;...;a_m) \circ \sigma^{-1}(\sigma(a_i)) = \sigma \circ (a_1;...;a_m)(a_i) = \sigma(a_{i+1})$

$$\sigma \circ (a_1;...;a_m) \circ \sigma^{-1}(\sigma(a_m)) = \sigma(a_1)$$

   $\sigma \circ (a_1;...;a_m) \circ \sigma^{-1}(k) = k, k \in \mathbb{Z} \setminus \{a_1;...;a_m\}$
4. $\sigma \circ (a_1;...;a_m) \circ \sigma^{-1} = \begin{matrix} \sigma(a_1) & ... & \sigma(a_m) \end{matrix}$, il suffit de choisir σ telle que : $\sigma(a_i) = \sigma(b_i)$

Remarques

1. Pour $i \in [|1; n|], \sigma = [i+1, i+2] = \sigma^{-1}$. Il vient que l'on peut écrire toute transposition comme produit de transpositions de la forme $[k, k+1]$
2. L'ordre d'une permutation est le PPCM des longueurs des cycles qui interviennent dans la décomposition (à supports disjoints)
3. Généralement dans un groupe G, pour x_0 fixé, l'application : $\begin{matrix} f & : & G & \to & G \\ & & x & \mapsto & x_0^{-1} x x_0 \end{matrix}$ est un automorphisme
4. $\forall (x, y) \in G^2, f(xy) = x_0^{-1} xy x_0 = x_0^{-1} x x_0^{-1} x_0 y x_0 = f(x) f(y)$

   Sa réciproque est l'application : $\begin{matrix} f^{-1} & : & G & \to & G \\ & & x & \mapsto & x_0 x x_0^{-1} \end{matrix}$ On dit que f est une conjugaison, elle mesure le défaut de commutativité d'un groupe

Signature d'une permutation

Soit $\sigma \in \sigma_n$, on définit la signature :

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

1. $\varepsilon(\sigma) \in \{-1; 1\}$
2. La signature est un morphisme de groupe surjectif
3. $\mathcal{A}_n = Ker(\varepsilon) = \{\sigma \in \sigma_n / \varepsilon(\sigma) = 1\}$ est un sous-groupe de σ_n de cardinal $\frac{n!}{2}$

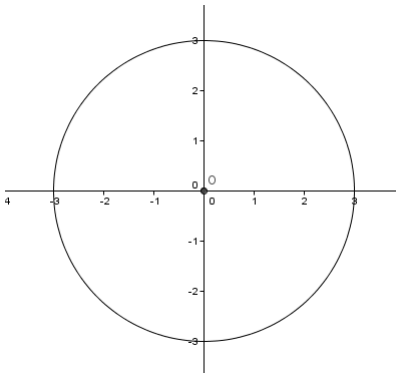
Preuve : Lemme : soit $\Delta_n = \{(i,j) \in [|1;n|]^2 / i \neq j\}$.
L'application $\begin{array}{rccc} \sigma^* & : & \Delta_n & \to & \Delta_n \\ & & (i,j) & \mapsto & (\sigma(i), \sigma(j)) \end{array}$ est bijective. En effet σ^* est bien définie car σ est injective, sa réciproque est : $\begin{array}{rccc} (\sigma^{-1})^* & : & \Delta_n & \to & \Delta_n \\ & & (i,j) & \mapsto & (\sigma^{-1}(i), \sigma^{-1}(j)) \end{array}$

1. D'après le lemme, $(\sigma(j) - \sigma(i))_{1 \leq i < j \leq n}$ décrit exactement $(j-i)_{1 \leq i < j \leq n}$ au changement de signe près (i.e inversions) : il vient,
$$\varepsilon(\sigma) = (-1)^m \text{ où m est le nombre d'inversions de } \sigma$$
2. Soit $(\sigma, \sigma') \in \sigma_n^2$:
$$\begin{aligned} \varepsilon(\sigma \circ \sigma') &= \prod_{1 \leq i < j \leq n} \frac{(\sigma \circ \sigma')(j) - (\sigma \circ \sigma')(i)}{\sigma'(j) - \sigma'(i)} \times \frac{\sigma'(j) - \sigma'(i)}{j - i} \\ &= \prod_{1 \leq i < j \leq n} \frac{(\sigma \circ \sigma')(j) - (\sigma \circ \sigma')(i)}{\sigma'(j) - \sigma'(i)} \times \prod_{1 \leq i < j \leq n} \frac{\sigma'(j) - \sigma'(i)}{j - i} \\ &= \varepsilon(\sigma') \times \prod_{1 \leq i' < j' \leq n} \frac{\sigma(j') - \sigma(i')}{j' - i'} \\ &= \varepsilon(\sigma') \times \varepsilon(\sigma) \end{aligned}$$
$\varepsilon(id) = +1$
$\tau = [i_0; j_0] \Rightarrow \varepsilon(\tau) = -1$ preuve par disjonction des cas sur i_0 et j_0
3. Par décomposition canonique $\frac{\sigma_n}{\mathcal{A}_n}$ est isomorphe à $\mathrm{Im}(\varepsilon)$, d'après le théorème de Lagrange :
$$card(\sigma_n) = card(\mathcal{A}_n) card(\tfrac{\sigma_n}{\mathcal{A}_n})$$
$$\text{d'où } card(\mathcal{A}_n) = \tfrac{n!}{2}$$
Une preuve ne faisant appel à aucun résultats hors programme consiste à étudier l'application : $\begin{array}{rccc} \tau & : & \mathcal{A}_n & \to & \frac{\sigma_n}{\mathcal{A}_n} \\ & & x & \mapsto & x_0 x x_0^{-1} \end{array}$, et montrer que c'est un morphisme bijectif

1.2.7 Groupes et géométries

On s'intéresse à l'ensemble des isométries qui laissent globalement invariante une figure plane : c'est un sous-groupe des isométries vectorielles du plan.

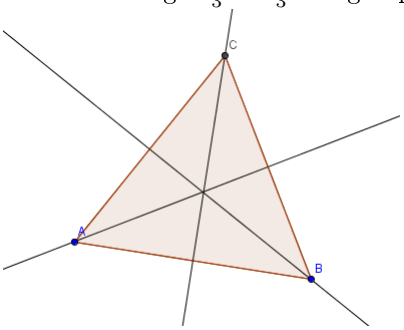
Cercle



Toutes les isométries laissent le cercle invariant

Triangle équilatéral

Une telle symétrie réalise une permutation des points A, B et C. Il y en a au plus $6! = 3$. Ainsi ces isométries sont les symétrie orthogonales par rapport aux médianes, l'identité, et les rotations d'angle $\frac{2\pi}{3}$ et $\frac{4\pi}{3}$. Ce groupe est isomorphe à σ_3. La signature joue le rôle du déterminant.



Isométries du triangle

Il est impossible de réaliser des transpositions. On a deux symétries orthogonales par rapport aux médiatrices, l'identité et la rotation d'angle π. C'est le groupe de Klein.

Isométries du polygone régulier

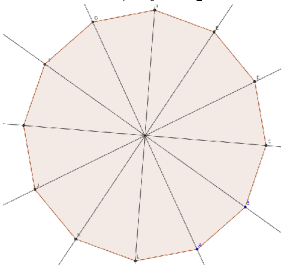
Pour les symétries, il suffit de connaître l'image de A_i de A_1, il y a donc n symétries orthogonales possibles :

Si n est pair : il y a n/2 symétries orthogonales passant par les sommets opposés et n/2 passant par les côtés opposés.
Si n est impair : il y a n symétries orthogonales issue des hauteurs

Les rotations sont déterminés par l'image de A_1 : il y en a n possibles :

$$\boxed{\mathcal{R}_\theta(A_1) = A_k \Rightarrow \theta = \frac{2\pi(k-1)}{n}}$$

On obtient un groupe de cardinal 2n, appelé diédral D_n composé de n symétries orthogonales et n rotations. Notons que l'ensemble des rotations est un sous-groupe (noyau du déterminant) de cardinal n, cyclique.



1.3 Anneaux et Corps

1.3.1 Définitions générales

Anneaux

On dit qu'un ensemble $\mathcal{A}$ muni de deux lois internes $+$ et $\times$ est un anneau si et seulement si :

1. $(\mathcal{A}, +)$ est un groupe abélien de neutre $0_\mathcal{A}$
2. La loi $\times$ est associative, de neutre $1_\mathcal{A}$
3. $\times$ est distributive sur $+$

Si de plus $\times$ est commutative alors $\mathcal{A}$ est un anneau commutatif

Corps

Si de plus $\mathcal{A}$ est un anneaux dont tout les éléments de $\mathcal{A} \setminus \{0_\mathcal{A}\}$ sont inversibles pour $\times$ alors $\mathcal{A}$ est muni d'une structure de corps : c'est un anneau intègre

Exemples

1. $(\mathbb{Z}, +, \times)$, $(\mathcal{M}_n(\mathbb{K}), +, \times)$ et $(\mathbb{K}[X], +, \times)$ sont des anneaux commutatifs
2. Soit I un ensemble , $\mathcal{F}(I, \mathbb{K})$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{K}(X)$ sont des corps
3. $\mathbb{H}$ le corps des quaternions est un corps non commutatif

Propriétés

1. 0 est absorbant pour $\times$:
$$\forall a \in \mathcal{A}, a \times 0 = 0 \times a = 0$$
2. On dit que $a \in \mathcal{A} \setminus \{0\}$ est un diviseur de 0 si et seulement si :

$$\exists b \in \mathcal{A} \setminus \{0\} / a \times b = 0 \text{ ou } b \times a = 0$$

3. Lorsqu'il n'existe pas de diviseur de 0, on dit que $\mathcal{A}$ est intègre :
$$\forall (a,b) \in \mathcal{A}^2, a \times b = 0 \Leftrightarrow a = 0 \text{ ou } b = 0$$
4. On dit que $\mathcal{A}$ est régulier à droite (resp. à gauche) si et seulement si :
$$\forall (c,b) \in \mathcal{A}^2, a \times b = a \times c \Rightarrow b = c$$
5. Groupes des inversibles : on note $\mathcal{U}$ ou $\mathcal{A}^\times$ l'ensembles des inversibles pour $\times$, qui est un groupe multiplicatif

Exemples

1. $\mathbb{Z}^\times = \{-1; +1\}$
2. $\mathbb{K}[X]^\times = \mathbb{K}_0 \setminus \{0\}$, résultat provenant de la théorie des degrés :
$$\deg(AB) = \deg(A)\deg(B) \Leftrightarrow \deg(A) = \deg(B) = 0$$
3. Les entiers de Gauss : $\mathbb{Z}[i] = \{a + ib / (a,b) \in \mathbb{Z}^2\}$. C'est le plus petit sous-anneaux de $\mathbb{C}$ contenant i.
$$\mathbb{Z}[i]^\times = \{1; -1; i; -i\}$$
4. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} / (a,b) \in \mathbb{Z}^2\}$. Démontrons une condition d'inversibilité :
$$\begin{aligned} (a+b\sqrt{2})(a'+b'\sqrt{2}) = 1 &\Leftrightarrow (a^2-2b^2)(a'^2-2b'^2) = 1 \\ &\Leftrightarrow a^2 - 2b^2 \in \{-1, 1\} \end{aligned}$$

Règles de calculs dans un anneaux

Soit $(a,b) \in \mathcal{A}^2$ / $ab = ba$:

1. $$\forall n \in \mathbb{N}, (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$
2. $$\forall n \in \mathbb{N}, a^n - b^n = (a-b) \sum_{k=1}^{n} a^{n-k} b^{k-1}$$
3. $$\forall n \in \mathbb{N}, a^{2+1} + b^{2n+1} = a^{2n+1} - (-b)^{2n+1} = (a+b) \sum_{k=1}^{2n+1} a^{2n+1-k}(-b)^{k-1}$$
4. $$1 - a^n = 1^n - a^n = (1-a) \sum_{k=0}^{n-1} a^k$$
5. Si a est nilpotent , $\exists n \in \mathbb{N} / a^n = 0$ alors $1 - a$ est inversible d'inverse
$$\sum_{k=0}^{n-1} a^k$$

1.3.2 Anneaux Quotient

Définition

Soit $\mathcal{A}$ un anneau et $\mathcal{R}$ une relation d'équivalence compatible avec $+$ et $\times$, on peut alors munir $\frac{\mathcal{A}}{\mathcal{R}}$ d'une structure d'anneau en définissant :

$$\begin{aligned} \forall (a,b) \in \mathcal{A}^2, \overline{a+b} &= \overline{a} + \overline{b} \\ \overline{a \times b} &= \overline{a} \times \overline{b} \end{aligned}$$

Cas de $\frac{\mathbb{Z}}{n\mathbb{Z}}$

La relation $\equiv$ est compatible avec $+$ et $\times$:

$$\begin{gathered} \forall (x,y,x',y') \in \mathbb{Z}^4, x \equiv y[n] \text{ et } x' \equiv y'[n] \text{ alors :} \\ x+y \equiv x'+y'[n] \text{ et } xy \equiv x'y'[n] \end{gathered}$$

On peut donc munir $\frac{\mathbb{Z}}{n\mathbb{Z}}$ d'une structure d'anneau

Morphismes d'anneaux

Soient $\mathcal{A}$ et $\mathcal{B}$ deux anneaux. On dit $\varphi : \mathcal{A} \to \mathcal{B}$ est un morphisme d'anneaux :

$$\begin{aligned} \forall (x,y) \in \mathcal{A}^2, \varphi(x+y) &= \varphi(x) + \varphi(y) \\ \varphi(x \times y) &= \varphi(x) \times \varphi(y) \end{aligned}$$

$\varphi(1_{\mathcal{A}}) = 1_{\mathcal{B}}$, bien que cette condition ne soit pas nécessaire

Exemples

L'identité et la conjugaison sont des morphismes de $\mathcal{C}$ dans $\mathcal{C}$. Ce sont les seuls qui laissent $\mathbb{R}$ et donc $\mathbb{Z}$ invariants. On ne notera que $Im(\varphi)$ est un anneau

Décomposition canonique d'un morphisme d'anneau (HP)

Soit $\varphi : \mathcal{A} \longrightarrow \mathcal{B}$ un morphisme d'anneaux. La relation d'équivalence :

$$x \mathcal{R} y \Leftrightarrow \varphi(x) = \varphi(y) \Leftrightarrow (x-y) \in Ker(\varphi)$$

est compatible avec les lois $+$ et $\times$. On note $\frac{\mathcal{A}}{Ker(\varphi)}$ l'anneau quotient correspondant :

$$\begin{array}{rccc} \overline{\varphi} & : & \frac{\mathcal{A}}{Ker(\varphi)} & \to & Im(\varphi) \\ & & \overline{x} & \mapsto & \overline{\varphi}(\overline{x}) = \varphi(x) \end{array}$$

est un isomorphisme d'anneaux

Preuve : φ étant un morphisme de groupes, $\mathcal{R}$ est compatible avec $+$. De plus, on montre de même qu'elle est compatible avec $\times$:

$$\forall (x,y,x',y') \in \mathcal{A}^4, \varphi(x) = \varphi(x') \text{ et } \varphi(y) = \varphi(y') \text{ donc}$$
$$\varphi(xy) = \varphi(x)\varphi(y) = \varphi(x')\varphi(y') = \varphi(x'y')$$

De plus $\overline{\varphi}$ est définie et est un morphisme de groupes. En outre :

$$\forall (x,y) \in \mathcal{A}^2, \overline{\varphi}(xy) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi(x)\varphi(y)}$$
$$\overline{\varphi} \text{ est bien un morphisme d'anneaux}$$

1.3.3 Anneaux produits

Définition

Soit $\mathcal{A}_i$ une famille d'anneaux, on définit sur $\mathcal{A}_1 \times ... \times \mathcal{A}_n$ les lois produits :

$$\forall ((a_1;...;a_n),(b_1;...;b_n)) \in (\mathcal{A}_1 \times ... \times \mathcal{A}_n)^2$$
$$(a_1;...;a_n) + (b_1;...;b_n) = (a_1+b_1;...;a_n+b_n)$$
$$(a_1;...;a_n) \times (b_1;...;b_n) = (a_1b_1;...;a_nb_n)$$

$\mathcal{A}_1 \times ... \times \mathcal{A}_n$ muni de ces lois est un anneau dit anneau-produit

Inversibles et neutres

Il faut que toutes les composantes soient inversibles. Dans ce cas, on inverse composante par composante. Pour les éléments neutres :

$$(1_{\mathcal{A}_1};...;1_{\mathcal{A}_n}) \text{ pour } +$$
$$(0_{\mathcal{A}_1};...;0_{\mathcal{A}_n}) \text{ pour } \times$$

⚠Cela ne marche pas pour les corps : $\mathbb{R}^2$ n'est pas un corps pour la loi produit :

$$(1;0) \times (0;1) = (0;0)$$

cet anneau n'est pas intègre, ce n'est pas un corps

1.3.4 L'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Définition

Soit $n \in \mathbb{N}^*$, on a :

1. $\forall (l,m) \in \mathbb{Z}^2, \overline{lm} = l\overline{m} = \overline{l}\overline{m}$
2. $\forall \in \mathbb{Z}$, $\overline{k}$ est inversible pour $\times$ dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ si et seulement si $\overline{k}$ est générateur pour $+$, si et seulement si $k \wedge n = 1$
3. Si $p \in \mathbb{P}$, $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps, noté $\mathbb{F}_p$
4. Sinon,
$$\frac{\mathbb{Z}}{n\mathbb{Z}}$$
n'est pas un corps, et $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times)$ n'est pas intègre

Preuve :

2

$$\begin{aligned}
\overline{k} \in \frac{\mathbb{Z}}{n\mathbb{Z}}^{\times} &\Rightarrow \exists \overline{l} \in \frac{\mathbb{Z}}{n\mathbb{Z}}, \overline{lk} = \overline{1} \\
&\Rightarrow l\overline{k} = \overline{1} \\
&\Rightarrow \forall a \in \mathbb{Z}, al\overline{k} = \overline{a} \in gr\{k\} \\
&\Rightarrow \overline{k} \text{ est générateur de}(\frac{\mathbb{Z}}{n\mathbb{Z}}, \times) \\
\text{Réciproquement }, \overline{k} \text{ est générateur de } (\frac{\mathbb{Z}}{n\mathbb{Z}}, \times) &\Rightarrow k \wedge n = 1 \\
&\Rightarrow \exists (u,v) \in \mathbb{Z}^2, ku + nv = 1 \\
&\Rightarrow \exists u \in \mathbb{Z}, \overline{k}u = \overline{1} \\
&\Rightarrow \overline{k} \text{ est inversible pour } \times \text{ dans} \frac{\mathbb{Z}}{n\mathbb{Z}}
\end{aligned}$$

3

$$\begin{aligned}
\text{Si} p \in \mathbb{P}, \forall k \in [|1; p-1|], p \wedge k = 1 &\Rightarrow \exists (u,v) \in \mathbb{Z}^2, pu + kv = 1 \\
&\Rightarrow \exists v \in \mathbb{Z}, v\overline{k} = \overline{1} \\
&\Rightarrow \overline{k} \text{ est inversible}
\end{aligned}$$

$$(\tfrac{\mathbb{Z}}{p\mathbb{Z}}, +, \times) \text{ est un corps}$$

4 Si p n'est premier, alors :

$$\exists (a,b) \in [|1; n-1|]^2, n = ab \Rightarrow \overline{ab} = \overline{n} \Rightarrow \overline{a}\overline{b} = \overline{0}$$

$\frac{\mathbb{Z}}{n\mathbb{Z}}$ n'est pas intègre, ce n'est pas un corps

Exemple : $\frac{\mathbb{Z}}{17\mathbb{Z}}$

Eléments	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Inverses	1	9	6	13	7	3	5	15	2	12	14	10	4	11	8	16

Remarque

$$x^2 = \overline{1} \Leftrightarrow (x - \overline{1})(x + \overline{1}) = \overline{0} \Leftrightarrow x \in \{\overline{1}; \overline{-1}\} \text{ par intégrité}$$

Exemple : $\frac{\mathbb{Z}}{12\mathbb{Z}}$

$\frac{\mathbb{Z}}{n\mathbb{Z}}^{\times} = \{\overline{1}; \overline{5}; \overline{7}; \overline{11}\}$ est isomorphe au groupe de Klein

Groupes des inversibles

Soit $p \in \mathbb{P}, (\mathbb{F}_p^*, \times)$ est un groupe abélien fini à $p-1$ éléments. Soit pour $\overline{x} \in \mathbb{F}_p^*, \omega(\overline{x})$ son ordre : on sait que : $\omega(\overline{x}) | p-1$. Soit

$$m = \bigvee_{\overline{x} \in \mathbb{F}_p^*} \omega(\overline{x})$$

d'après ce qui précède, $mp|1$.
Par ailleurs $\exists x_0 \in \mathbb{F}_p^*/\omega(x_0) = m$. Or :

$$\forall \overline{x} \in \mathbb{F}_p^*, \overline{x}^m = \overline{1}$$

Dans le corps commutatif $\mathbb{F}_p^*$, le polynôme $X^m - 1$ admet au plus m racines distinctes, il vient que :

$$\mathbb{F}_p^* = gr\{\overline{x_0}\}, \text{ donc } (\mathbb{F}_p^*, \times) \text{ est cyclique}$$

On montre ainsi que $\mathbb{F}_{17}^*$ est engendré par $\overline{3}$

Petit théorème de Fermat, théorème de Wilson

1. Petit théorème de Fermat : $p \in \mathbb{P}, a \in \mathbb{Z}$,
$$p \nmid a \Rightarrow a^{p-1} \equiv 1[p]$$
$$a^p \equiv a[p]$$
2. Théorème de Wilson : $p \in \mathbb{P} \Leftrightarrow (p-1)! \equiv -1[p]$

Preuve :

1. $p \nmid a, \overline{a} \in (\mathbb{F}_p^*, \times)$, ensemble à $p-1$ éléments, on sait alors que :
$$\overline{a}^{p-1} = \overline{1}$$
De même : $p|a \Rightarrow \overline{a}^p = \overline{0} \Rightarrow \overline{a}^p = \overline{a}$
2. $$n \in \mathbb{P}, \overline{(n-1)!} = \prod_{\overline{x} \in \mathbb{F}_p^*} \overline{x} \Rightarrow \overline{(n-1)!} = \overline{-1}\overline{1} = \overline{-1}$$
En effet les éléments étant deux à deux distincts de leur inverse, ils se compensent sauf pour $\overline{1}$ et $\overline{-1}$. Une autre démonstration consiste à étudier le polynôme $X^{n-1} - 1$ qui s'annule pour tout les élements de $\mathbb{F}_p^*$, ce qui permet d'obtenir le résultat souhaité en évaluant en 0. Si $n \notin \mathbb{P}$ alors $\overline{(n-1)!} = \overline{0}$

1.3.5 Indicatrice d'Euler et théorème Chinois

Théorème Chinois

Soit $(n, m) \in \mathbb{N}^* \times \mathbb{N}^*/n \wedge m = 1$, l'application :

$$\begin{array}{rccc} \varphi & : & \frac{\mathbb{Z}}{nm\mathbb{Z}} & \to & \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}} \\ & & \overline{k} & \mapsto & (\overleftarrow{k}, \overrightarrow{k}) \end{array}$$

est un isomorphisme d'anneaux

Preuve : $Ker(\varphi) = \{k \in \mathbb{Z}/\overleftarrow{k} = \overleftarrow{0} \text{ et } \overrightarrow{k} = \overrightarrow{0}\} = \{k \in \mathbb{Z}/nm|k\} = nm\mathbb{Z}$
On sait alors que l'application $\overline{\varphi}$ canoniquement associée est un isomorphisme d'anneaux, ce qui implique que : $Im(\varphi) = \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$

Remarque

C'est le caractère surjectif de $\overline{\varphi}$ qui est intéressant ; le théorème se reformule ainsi :

$$\forall (a,b) \in \mathbb{Z}^2, \exists ! k \in [|0; mn-1|], (\overleftarrow{k}, \overrightarrow{k}) = (\overleftarrow{a}, \overrightarrow{b})$$
$$a \equiv k[n] \text{ et } b \equiv k[m]$$

Corollaire

Soient $(n_1; ...; n_r) \in \mathbb{N}^r, \forall (i,j) \in [|1;r|]^2, i \neq j \Rightarrow n_i \wedge m_i = 1$, l'application :

$$\begin{array}{rccc} \varphi & : & \frac{\mathbb{Z}}{n_1...n_r\mathbb{Z}} & \to & \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{n_r\mathbb{Z}} \\ & & \overline{k}^{n_1...n_r} & \mapsto & (\overleftarrow{k}^{n_1}; ...; \overrightarrow{k}^{n_r}) \end{array}$$

est un isomorphisme d'anneaux.

Preuve : se fait par récurrence triviale sur n

Définition : indicatrice d'Euler

Soit $n \in \mathbb{N}^*$:

$$\varphi(n) = card\{1 \leq k \leq n / k \wedge n = 1\}$$

C'est également le nombre d'inversibles de l'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ et de générateur du même groupe.

Ainsi :

n	1	2	3	4	5	6
$\varphi(n)$	1	1	2	2	4	2

Théorème

1. Si $p \in \mathbb{P}, \forall \alpha \in \mathbb{N}^*, \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, donc $\varphi(p) = p - 1$
2. Si $n \wedge m = 1, \varphi(nm) = \varphi(n)\varphi(m)$
3. $$n = \prod_{i=1}^{r} p_i^{\alpha_i}, \varphi(n) = \prod_{i=1}^{r} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$$

Preuve :

1. Soit $m \in [|1; p^\alpha|]$:
   $$m \wedge p^\alpha \neq 1 \Leftrightarrow p | m \Leftrightarrow m \in \{kp / k \in [|1; p^\alpha|]\}$$
   Il y a $p^{\alpha-1}$ tel nombres, d'où : $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$
2. Découle du théorème chinois, on considérant les groupes des inversibles
3. On applique les deux résultats précédents

Théorème d'Euler - Möbius (HP)

Soit $n \in \mathbb{N}^*$, on a :

$$\boxed{n = \sum_{d|n} \varphi(d)}$$

Preuve : Dans $(\mathbb{U}_n, \times)$ chaque élément possède un ordre et un seul $d|n$, donc :

$$\mathbb{U}_n = \bigcup_{d|n} \mathcal{G}_d$$

éléments d'ordre d dans $\mathbb{U}_n$

Or $z \in \mathbb{U}_n$ est d'ordre d si et seulement si z^d et $\omega(z) = d$ si et seulement si $gr\{z\} = \mathbb{U}_d$
Or il existe $\varphi(d)$ éléments d'ordre d dans $(\mathbb{U}_d, \times)$ par isomorphisme, d'où :

$$n = card(\mathbb{U}_n) = \sum_{d|n} card(\mathcal{G}_d) = \sum_{d|n} \varphi(d)$$

Exemple

On se place dans $\mathbb{U}_6$

x	1	$-j^2$	j	-1	j^2	$-j$
$\omega(x)$	1	6	3	2	3	6

On a bien les résultats escomptés

Théorème d'Euler

Soit $n \in \mathbb{N}^*, a \in \mathbb{Z}/a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1[n]$

Preuve : $\bar{a} \in \frac{\mathbb{Z}}{n\mathbb{Z}}^{\times}$ or ce groupe est de cardinal $\varphi(n)$, donc $\bar{a}^{\varphi(n)} = \bar{1}$

Théorème RSA

Soient $p, q \in \mathbb{P}$ distincts $n = pq$ et $c, d \in \mathbb{N}, cd \equiv 1[\varphi(n)], \varphi(n) = (p-1)(q-1)$

$$\forall \bar{t} \in \frac{\mathbb{Z}}{n\mathbb{Z}}, \bar{t}^{cd} = \bar{t}$$

Preuve : Montrons que : $\forall t \in [|0; n-1|], n|t^{cd} - t \Leftrightarrow p|t^{cd} - t$ et $q|t^{cd} - t$

$p|t \Rightarrow t^{cd} \equiv t \equiv 0[p] \Rightarrow p|t^{cd} - t$

$p \wedge t = 1 \Rightarrow t^{p-1} \equiv 1[p]$
$cd \equiv 1[\varphi(n)] \Rightarrow \exists k \in \mathbb{N}/cd = 1 + k\varphi(n) = 1 + k(p-1)(q-1) \Rightarrow t^{cd} = t(t^{p-1})^{q-1} \equiv t[p]$

$$p|t^{cd} - t \text{ , de même pour q}$$

Ainsi les applications : $f : \begin{array}{ccc} \frac{\mathbb{Z}}{n\mathbb{Z}} & \to & \frac{\mathbb{Z}}{n\mathbb{Z}} \\ \bar{t} & \mapsto & \bar{t}^c \end{array}$ et $g : \begin{array}{ccc} \frac{\mathbb{Z}}{n\mathbb{Z}} & \to & \frac{\mathbb{Z}}{n\mathbb{Z}} \\ \bar{t} & \mapsto & \bar{t}^d \end{array}$ sont bijectives et réciproques l'une de l'autre. Le principe des clefs publiques consistent à publier les valeurs de n et c : tout le monde peut effectuer f(codage). Seul celui qui connait p et q (donc $\varphi(n)$) peut évaluer d et décoder

1.4 Arithmétique générale

1.4.1 Idéal

Soit $\mathcal{A}$ un anneau et une partie $I \subset \mathcal{A}$. Soit $\mathcal{R}$, la relation bianaire définie su r$\mathcal{A}$:

$$x\mathcal{R}y \Leftrightarrow x - y \in I$$

C'est une relation d'équivalence si et seulement si $(I, +)$ est un sous-groupe additif de $\mathcal{A}$. A quelle conditions sur I, $\mathcal{R}$ est-elle compatible avec $+$ et $\times$?
Soit $(x, y, x', y') \in \mathcal{A}^4 / x\mathcal{R}y$ et $x'\mathcal{R}y'$, alors :

$$\exists (a, b) \in I^2 / x' = x + a \text{ et } y' = y + b$$

$x' + y' = x + y + a + b \Rightarrow x' + y'\mathcal{R}x + y$
$x'y' = xy + ay + xb + ab$, on a :

$$x'y'\mathcal{R}xy \Leftrightarrow ay + xb + ab \in I \Leftrightarrow \forall a \in \mathcal{A}, \forall z \in I, az \in I$$

Définition

Soit $\mathcal{A}$ un anneau, on dit que $I \subset \mathcal{A}$ est un idéal de $\mathcal{A}$ si et seulement si :

1. I est un sous-groupe de $(\mathcal{A}, +)$
2. $\forall (x, a) \in I \times \mathcal{A}, xa \in I$ et $ax \in I$

Exemples

1. $\{0\}$ et $\{0\}$ sont des idéaux
2. Soit $\mathcal{A}$ commutatif : $\forall a \in \mathcal{A}, a\mathcal{A} = \{ab / b \in \mathcal{A}\}$ est un idéal, dit idéal principal engendré par a.
3. Dans $\mathbb{Z}$, les idéaux sont de la forme $n\mathbb{Z}$
4. Dans $\mathbb{Z}^2$, $(0, 1)\mathbb{Z} + (2, 0)\mathbb{Z}$ est un idéal

Propriétés

1. Toute intersection d'idéaux est un idéal. Pour une partie $\mathcal{B} \subset \mathcal{A}$ on peut définir l'idéal engendré par $\mathcal{B}$ comme l'intersection de tous les idéaux de $\mathcal{A}$ contenant $\mathcal{B}$
2. L'idéal engendré par a est $a\mathcal{A}$
3. Soit I un idéal de $\mathcal{A}$
$$I = \mathcal{A} \Leftrightarrow 1 \in I \Leftrightarrow \exists b \in \mathcal{A}^\times, b \in I$$
4. Si $\mathcal{A}$ est un corps alors ses seuls idéaux sont $\{0\}$ et $\mathcal{A}$

Preuve :
1. trivial

2. $a\mathcal{A}$ est un idéal contenant a. Si I est un idéal contenant a alors $I = a\mathcal{A}$
3. $\mathcal{A} = I \Rightarrow 1 \in I \Rightarrow \exists b \in \mathcal{A}, b \in I \Rightarrow \forall a \in \mathcal{A}, a = u(u^{-1}a) \in I, u \in \mathcal{A}^\times \Rightarrow \mathcal{A} = I$
4. Si $\mathcal{A}$ est un corps, soit I un idéal de $\mathcal{A}$ et $a \in I \setminus \{0\}$, a est inversible, d'après 3), $\mathcal{A} = I$

Remarque

Dans un anneau non commutatif, on distingue deux types d'idéaux :

Les idéaux tout courts, bilatères
Les idéaux à droite, les idéaux à gauche

Somme d'idéaux

Soit $(\mathcal{A}, +, \times)$ un anneau et (I_k) une famille d'idéaux de $\mathcal{A}$ alors :

$$I_1 + ... + I_n = \sum_{k=1}^{n} I_k = \{x_1 + ... + x_n / \forall i \in [|1; n|], x_i \in I_i\}$$

est l'idéal engendré par

$$\bigcup_{i=1}^{n} I_i$$

Preuve :

$$0 \in \sum_{k=1}^{n} I_k$$

Soit $((x_1; ...; x_n), (y_1; ...; y_n)) \in (I_1 \times ... \times I_n)^2$

$$(x_1; ...; x_n) - (y_1; ...; y_n) = (x_1 - y_1; ...; x_n - y_n) \in \sum_{k=1}^{n} I_k$$

$$a(x_1; ...; x_n) = (ax_1; ...; ax_n) \in \sum_{k=1}^{n} I_k$$

c'est donc un idéal contenant

$$\bigcup_{i=1}^{n} I_i$$

Soit par ailleurs I un idéal contenant

$$\bigcup_{i=1}^{n} I_i$$

par stabilité il vient :

$$\forall (x_1; ...; x_n) \in I_1 \times ... \times I_n, \sum_{i=1}^{n} x_i \in I \supset \sum_{k=1}^{n} I_k$$

Décomposition canonique d'un morphisme d'anneau

Soit $\varphi : \mathcal{A} \longrightarrow \mathcal{B}$ un morphisme d'anneaux :

1. $Ker(\varphi)$ est un idéal de $\mathcal{A}$ et $Im(\varphi)$ est un sous-anneau de $\mathcal{B}$
2. (HP) : $\begin{array}{rccc} \overline{\varphi} & : & \frac{\mathcal{A}}{Ker(\varphi)} & \to & Im(\varphi) \\ & & \bar{x} & \mapsto & \overline{\bar{x}} = \varphi(x) \end{array}$ est un isomorphisme d'anneaux

Preuve :

1. $Ker(\varphi)$ est un sous-groupe de $(\mathcal{A}, +)$ et $\forall (x, a) \in Ker(\varphi) \times \mathcal{A}, \varphi(xa) = \varphi(x)\varphi(a) = 0 = \varphi(x)$

$$Ker(\varphi) \text{ est un idéal de } \mathcal{A}$$

2. $\frac{\mathcal{A}}{Ker(\varphi)}$ désigne l'anneau quotient de $\mathcal{A}$ par la relation d'équivalence :

$$x\mathcal{R}y \Leftrightarrow (x - y) \in Ker(\varphi) \Leftrightarrow \varphi(x) = \varphi(y)$$

compatible avec $+$ et $\times$ car $Ker(\varphi)$ est un idéal. On a vu par ailleurs que c'est un isomorphisme de groupes. En outre :

$$\forall (x, y) \in \mathcal{A}^2, \overline{\varphi}(\bar{x}\bar{y}) = \overline{\varphi}(\overline{xy}) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi}(\bar{x})\overline{\varphi}(\bar{y})$$
$$\overline{\varphi}(\overline{1_{\mathcal{A}}}) = \varphi(\overline{1_{\mathcal{A}}}) = 1_{\mathcal{B}}$$
$$\overline{\varphi} \text{ est un morphisme d'anneau}$$

1.4.2 Divisibilité

Définitions

Soit $\mathcal{A}$ un anneau commutatif intègre

1. Soit $(a, b) \in \mathcal{A}^2$, on dit que :

$$b|a \Leftrightarrow \exists c \in \mathcal{A}/a = bc \Leftrightarrow a \in b\mathcal{A} \Leftrightarrow a\mathcal{A} \subset b\mathcal{A}$$

c'est une relation réflexive et transitive

2. Soit $(a, b) \in (\mathcal{A} \setminus \{0\})^2$ on dit que

$$a \text{ et } b \text{ sont associés } \Leftrightarrow a|b \text{ et } b|a \Leftrightarrow a\mathcal{A} = b\mathcal{A} \Leftrightarrow \exists u \in \mathcal{A}^\times/b = au$$

c'est une relation d'équivalence

3. On dit que $a \in \mathcal{A} \setminus \{0\}$ est irréductible dans $\mathcal{A}$ si et seulement si :
   (a) a n'est pas inversible
   (b) $\exists (b, c) \in \mathcal{A}^2/a = bc \Rightarrow$ l'un est inversible (l'autre est donc associé à a)

Exemples

Dans $\mathbb{Z}$, deux éléments sont associés si et seulement si $|a| = |b|$, $a \in \mathbb{Z}^*$ est irréductible si et seulement $|a| \in \mathbb{P}$

Remarques

$$a \text{ est inversible} \Leftrightarrow a\mathcal{A} = \mathcal{A}$$
$$a \text{ est irréductible} \Leftrightarrow a\mathcal{A} \subsetneq \mathcal{A} \Leftrightarrow [a\mathcal{A} \subset a_1\mathcal{A} \Rightarrow a_1\mathcal{A} = \mathcal{A} \text{ ou } a_1\mathcal{A} = a\mathcal{A}$$

1.4.3 Anneaux principaux

Définition

On dit qu'un anneau $\mathcal{A}$ commutatif et intègre est principal si tout ses idéaux sont principaux :

$$\forall I \text{ idéal de } \mathcal{A}, \exists a \in \mathcal{A} / I = a\mathcal{A}$$

Exemples

$\mathbb{Z}$ et $\mathbb{K}[X]$ sont principaux

Preuve : Soit I un idéal de $\mathbb{K}[X]$:
$\rightarrow$ si $I = \{0\}$ alors $I = 0 \cdot \mathbb{K}[X]$
$\rightarrow$ si $I \neq \{0\}$ alors P_0 est unitaire et dans I, tel que

$$\deg(P_0) = min\{deg(P) / P \in I \setminus \{0\}\}$$

Comme I est un idéal contenant P_0 : $P_0 \subset \mathbb{K}[X]$
On effectue la division euclidienne de $A \in I$ par P_0 :

$$\exists (Q, R) \in \mathbb{K}[X]^2 / A = QP_0 + R, deg(R) < deg(Q)$$
$$R = A - QP_0 \in I \Rightarrow R = 0$$
$$A = QP_0 \in P_0\mathbb{K}[X]$$

Finalement : $I = P_0\mathbb{K}[X]$

PGCD et PPCM

Soit $\mathcal{A}$ un anneau principal et $(a_1; ...; a_n) \in \mathcal{A}^n$

1. $$\delta = PGCD(a_1; ...; a_n) = \bigwedge_{i=1}^{m} \Leftrightarrow \delta\mathcal{A} = \sum_{i=1}^{n} a_i\mathcal{A} \Leftrightarrow \mathcal{A} \text{ est générateur de l'idéal } \sum_{i=1}^{n} a_i\mathcal{A}$$

   On a : $\forall d \in \mathcal{A}, \forall i \in [|1; n|], d|a_i \Leftrightarrow d|\delta$

2. $$m = PPCM(a_1; ...; a_n) = \bigvee_{i=1}^{n} a_i \Leftrightarrow m\mathcal{A} = \bigcap_{i=1}^{n} a_i\mathcal{A} \Leftrightarrow m \text{ est générateur de l'idéal } \bigvee_{i=1}^{n} a_i$$

   Dans ce cas on a : $\forall b \in \mathbb{A}, \forall i \in [|1; n|] a_i|b \Leftrightarrow m|b$

Preuve :

1.

$$\begin{aligned}\forall i \in [|1;n|] d|a_i &\Leftrightarrow \forall i \in [|1;n|] a_i\mathcal{A} \subset d\mathcal{A} \\ &\Leftrightarrow \bigcup_{i=1}^{n} a_i\mathcal{A} \subset d\mathcal{A} \\ &\Leftrightarrow d|\delta\end{aligned}$$

2.

$$\begin{aligned}\forall i \in [|1;n|] a_i|b &\Leftrightarrow \forall i \in [|1;n|] b\mathcal{A} \subset a_i\mathcal{A} \\ &\Leftrightarrow b\mathcal{A} \subset \bigcap_{i=1}^{n} a_i\mathcal{A} \\ &\Leftrightarrow m|b\end{aligned}$$

On remarque que $\wedge$ et $\vee$ sont commutatifs et associatifs.
O est neutre pour $\wedge$ et absorbant pour $\vee$
Un inversible est absorbant pour $\wedge$ et neutre pour $\vee$

Éléments premiers entre eux

Soit $(a_1;...;a_n) \in \mathcal{A}^n$,

1. ils sont premiers entre-eux dans leur ensemble si et seulement si : $\bigwedge_{i=1}^{n} a_i = 1$
2. ils sont premiers entre-eux 2 à 2 si et seulement si : $\forall i \neq j, a_i \wedge a_j = 1$
3. $(a_1;...;a_n)$ sont premiers entre eux dans leur ensemble alors ils sont premiers entre-eux deux à deux. La réciproque est fausse

Théorème de Bézout

$$\begin{aligned}\text{Soit } (a_1;...;a_n) \in \mathcal{A}^n, \bigwedge_{i=1}^{n} = 1 &\Leftrightarrow \mathcal{A} = \sum_{i=1}^{n} a_i\mathcal{A} \\ &\Leftrightarrow 1 \in \sum_{i=1}^{n} a_i\mathcal{A} \\ &\Leftrightarrow \exists (x_1;...;x_n) \in \mathcal{A}^n, \sum_{i=1}^{n} a_i x_i = 1\end{aligned}$$

Dans $\mathbb{Z}$ et $\mathbb{K}[X]$, on obtient des valeurs pour $a \wedge b = 1$ des valeurs $(x_1;x_2)$ telle que $ax_1+bx_2 = 1$ avec l'algorithme d'Euclide étendu

Caractérisation du PGCD

Soit $(a_1;...;a_n) \in \mathcal{A}^n$, $\delta = \bigwedge_{i=1}^n a_i$ alors $\exists (a'_1;...;a'_n) \in \mathcal{A}^n / \forall i \in [|1;n|]$:

$$\bigwedge_{i=1}^n a'_i = 1 \qquad a_i = \delta a'_i$$

Preuve : si $\forall i \in [|1;n|], a_i = 0 \Rightarrow \delta = 0$
$\forall i \in [|1;n|], a'_i = 0$
sinon : $\exists i_0 \in [|1;n|], a_{i_0} \neq 0 \Rightarrow \delta \neq 0$
$\forall i \in [|1;n|], \exists a'_i \in \mathcal{A} / a_i = \delta a'_i$
Or :

$$\begin{aligned}
\delta \in \sum_{i=1}^n a_i \mathcal{A} &\Rightarrow \delta = \sum_{i=1}^n a_i b_i / (b_1;...;b_n) \in \mathcal{A}^n \\
&\Rightarrow \delta = \delta(\sum_{i=1}^n a'_i b_i) \\
&\Rightarrow 1 = \sum_{i=1}^n a'_i b_i \\
&\Rightarrow \bigwedge_{i=1}^n a'_i = 1 \text{ d'après le théorème de Bézout}
\end{aligned}$$

Thérorème de Gauss

$$\boxed{a|bc \text{ et } a \wedge b = 1 \Rightarrow a|c}$$

Preuve :

$$\begin{aligned}
\exists (u,v) \in \mathcal{A}^2 / au + bv = 1 &\Rightarrow acu + bcv = c \\
&\Rightarrow a|acu \text{ et} a|bc \\
&\Rightarrow a|c
\end{aligned}$$

Cas des irréductibles

1. $a \wedge b = 1 \Rightarrow \forall (n,m) \in \mathbb{N}^2, a^n \wedge b^m = 1$
2. Soient $(p,q) \in m\mathcal{A}$ deux irréductibles non associés, on a $p \wedge q = 1$

Preuve :

1. $\exists (u,v) \in \mathcal{A}^2 / au + bv = 1$, d'après le formule du binôme (anneaux commutatif) :

$$\begin{aligned}(au+bv)^n = 1^n &\Leftrightarrow \sum_{k=0}^{n} \binom{n}{k} (au)^{n-k}(bv)^k = 1 \\ &\Leftrightarrow a^n u^n + b\sum_{k=1}^{n} \binom{n}{k} v(au)^{n-k}(bv)^{k-1} = 1 \\ &\Leftrightarrow a^n U + bV = 1 \\ &\Leftrightarrow a^n \wedge b = 1\end{aligned}$$

   On applique ensuite ce résultat à a^n et b

2. Notons $\delta = p \wedge q$, si δ est non inversible, comme p est irréductible et $\delta | p$, δ est associé à p. De même pour q, donc p et q sont associés, absurde. Ainsi $p \wedge q = 1$

Théorème de factorialité (HP)

Soit $\mathcal{A}$ un anneau principal. $\mathcal{P}$, l'ensemble des irréductibles de $\mathcal{A}$ et $\mathcal{P}_0 \subset \mathcal{P}$, $\forall p \in \mathcal{P}, \exists ! p_0 \in \mathcal{P}_0$ associé à p. On $\mathcal{U}$ l'ensemble des inversibles . On a :

$$\forall a \in \mathcal{A}^*, \exists ! u \in \mathcal{U}, \exists ! \ \nu \ : \begin{array}{ccc} \mathcal{P}_0 & \to & \mathbb{N} \\ p & \mapsto & \nu_p(a) \end{array}, a = u \prod_{p \in \mathcal{P}_0} p^{\nu_p(a)}$$

Preuve :

Existence Soit $a \in \mathcal{A}^*$, supposons que a n'est pas décomposable, e, particulier a n'est pas inversible et on peut écrire $a = bc$ où ni b ni c n'est inversible. Parmi b et c l'un des deux n'est pas décomposable, notons $a_0 = a$ et $a_1 \in \{b; c\}$ non décomposable : $a_1 | a_0 \Rightarrow a_0\mathcal{A} \subsetneq a_1\mathcal{A}$ car ils ne sont pas associés. Par récurrence, on peut construire $(a_n)_{n\in\mathbb{N}} / \forall n \in \mathbb{N}, a_n$ n'est pas décomposable et $a_n\mathcal{A} \nsubseteq a_{n+1}\mathcal{A}$.
Notons $I = \bigcup_{n\in\mathbb{N}} a_n\mathcal{A}, 0 \in I$. $\forall (x,y) \in I^2, \exists (n,m) \in \mathbb{N}^2 / x \in a_n\mathcal{A}$ et $y \in a_m\mathcal{A}$. Supposons $n \geq m$, comme $a_m\mathcal{A} \subsetneq a_n\mathcal{A}$. $(x,y) \in (a_n\mathcal{A}^2 \Rightarrow x - y \in a_n\mathcal{A} \subset I$. Soit enfin $b \in \mathcal{A}$ et $x \in I$, $\exists n \in \mathbb{N} / x \in a_n\mathcal{A}$. Ainsi I est un idéal de $\mathcal{A}$, or $\mathcal{A}$ est principal :

$$\exists \alpha \in \mathcal{A} / I = \alpha\mathcal{A}$$

En particulier :

$$\exists n_0 \in \mathbb{N} / \alpha \in a_{n_0}\mathcal{A}$$

On a

$$I = \alpha\mathcal{A} \subset a_{n_0}\mathcal{A} \subsetneq a_{n_0+1}\mathcal{A} \subset I$$

absurde

Unicité Supposons $a = u\prod_{p\in\mathcal{P}_0} p^{\nu_p(a)} = v\prod_{p\in\mathcal{P}_0} p^{\mu_p(a)}$. S'il existe $p_0 \in \mathcal{P}_0/\nu_p(a) \neq \mu_p(a)$ Il vient par intégrité :

$$up_0^{\nu_{p_0}(a)-\mu_{p_0}(a)} \prod_{p\in\mathcal{P}\setminus p_0} p^{\nu_p(a)} = v \prod_{p\in\mathcal{P}_0\setminus p_0} p^{\mu_p(a)}$$

D'après le théorème de Gauss :

$$p_0| \prod_{p\in\mathcal{P},\setminus p_0} p^{\mu_p(a)}$$

ce qui absurde car $\forall p \in \mathcal{P}_0, p_0 \wedge p = 1$, donc $\forall p \in \mathcal{P}_0, \mu_p(a) = \nu_p(a)$ par intégrité $u = v$

1.4.4 Cas de $\mathbb{K}[X]$

Soit $\mathbb{K}$ un corps commutatif, les inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls

$$P \in \mathbb{K}[X], P = aP_0/a \in \mathbb{K}, P_0 \text{ est unitaire}$$

$P \in \mathbb{K}[X]$ est irréductible $\Leftrightarrow \deg(P) \geq 1, \exists(P_1, P_2) \in \mathbb{K}[X]^2/P = P_1P_2, \{\deg(P_1); \deg(P_2)\} \neq \{0; \deg(P)\}$

Théorèmes

1. Tout polynôme de degré 1 est irréductible su $\mathbb{K}[X]$
2. Tout polynôme de degré ≥ 2 irréductible sur $\mathbb{K}$ n'a pas de racines sur $\mathbb{K}$
3. Si $\deg(P) \in \{2; 3\}$ et si P n'a pas de racines sur $\mathbb{K}$ alors il est irréductible sur $\mathbb{K}[X]$
4. Soit P irréductible sur $\mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$ $\{0\}$, $\deg(Q) < \deg(P) \Rightarrow Q \wedge P = 1$

Preuve :

1. $\deg(P) = 1$ et si $P = P_1P_2$ alors $\deg(P_1) + \deg(P_2) = 1$, alors l'un des deux est de degré nul
2. Si $\deg(P) \geq 2$, si $\alpha \in \mathbb{K}$ est racine de P, on peut écrire : $P(X) = (X-\alpha)Q(X), \deg(Q) \geq 1$ donc P n'est pas irréductible
3. Si $\deg(P) \in \{2; 3\}$ et si P n'a pas de racine sur $\mathbb{K}$, si $P = P_1P_2/\begin{cases} \deg(P_1) < \deg(P) \\ \deg(P_2) < \deg(P) \end{cases}$

   $$\{\deg(P_1); \deg(P_2)\} = \{1; 1\} \text{ ou} \{1; 2\}$$

   P_1 ou P_2 est de degré 1 donc admet une racine sur $\mathbb{K}$, contradiction.
   Cela devient faux si $\deg(P) \geq 4, (X^2+1)^2$ n'a pas de racines sur $\mathbb{R}$ mais n'est pas irréductible sur $\mathbb{R}$
4. Notons $\Delta = P \wedge Q, \Delta|P \Rightarrow \begin{cases} \deg(\Delta) = 0 \text{ ou} \\ \deg(\Delta) = \deg(P) \end{cases}$
   $\Delta|Q \Rightarrow \deg(\Delta) \leq \deg(Q) < \deg(P)$, $\deg(\Delta) = 0 \Rightarrow P \wedge Q = 1$

Exemples

$$\begin{aligned} X^3-2 &= (X-\sqrt[3]{2})(X-\sqrt[3]{2}j)(X-\sqrt[3]{2}j^2),\ \text{sur}\mathbb{C} \\ &= (X-\sqrt[3]{2})(X^2+\sqrt[3]{2}X+\sqrt[3]{4}),\ \text{sur}\mathbb{R} \\ &= X^3-2 \end{aligned}$$

X^3-2 est irréductible sur $\mathbb{Q}$, mais pas sur $\mathbb{R}$ ou $\mathbb{C}$, car $\sqrt[3]{2}$ est irrationel

Théorème d'Alembert Gauss

1. Tout polynôme non constant sur $\mathbb{C}[X]$ admet au moins une racine sur $\mathbb{C}$
2. Soit $P \in \mathbb{C}[X]$ non constant, on peut le décomposer de manière unique en :
$$P(X) = \gamma \prod_{i=1}^{n}(X-\alpha_i)$$
3. Les irréductibles sur $\mathbb{R}$ sont :
$$\mathcal{I}_{\mathbb{R}[X]} = \{aX+b/(a;b) \in \mathbb{R}^2\} \cup \{aX^2+bX+c/\Delta < 0\}$$

Relations coefficients-racines

Soit $P \in \mathbb{K}[X]$ scindé sur $\mathbb{K}$,

$$P(X) = \sum_{i=0}^{n} a_i X^i = a_n \prod_{i=1}^{n}(X-\alpha_i)$$

$$\forall k \in [|0;n-1|], a_k = a_n(-1)^{n-k}\sigma_{n-k}(\alpha_i)$$

1.5 Corps

1.5.1 Caractéristique

Définition

Soit $\mathbb{L}$ un corps, on dit que $\mathbb{K} \subset \mathbb{L}$ est un sous-corps de $\mathbb{L}$ si et seulement si :

1. 0 et $1 \in \mathbb{K}$
2. $\forall (x;y) \in \mathbb{K}^2, x-y$ et $xy \in \mathbb{K}$
3. $\forall x \in \mathbb{K}^*, x^{-1} \in \mathbb{K}$

Exemple

Soit $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{2}/(a;b;c) \in \mathbb{Q}^3\}$. C'est un sous-anneau de $\mathbb{Q}$ de dimension finie engendré par $(1; \sqrt[3]{2}; \sqrt[3]{4})$. Considérons : $\begin{array}{cccc} f & : & \mathbb{Q}[\sqrt[3]{2}] & \to & \mathbb{Q}[\sqrt[3]{2}] \\ & & x & \mapsto & x_0 x \end{array}$, il vient : $f \in \mathcal{L}(\mathbb{Q}[\sqrt[3]{2}])$ or $Ker(f) = \{0\}$, f est injective en dimension finie donc bijective :

$$\exists! x_1 \in \mathbb{Q}[\sqrt[3]{2}]/x_0 x_1 = 1 \Leftrightarrow x_1 = x_0^{-1}$$

C'est un sous-corps de $\mathbb{Q}$

Remarque : si $\mathbb{K}$ est un sous-corps de $\mathbb{L}$, alors on peut considérer que $\mathbb{L}$ est un $\mathbb{K}$ espace vectoriel

Caractéristique (HP)

Soit $\mathbb{K}$ un corps, l'application $\begin{array}{cccc} \psi & : & \mathbb{Z} & \to & \mathbb{Z} \\ & & n & \mapsto & n1_{\mathbb{K}} \end{array}$ est un morphisme d'anneaux. Son noyau est un idéal de $\mathbb{Z}$, de la forme $n_0\mathbb{Z}$: n_0 est la caractéristique de $\mathbb{K}$:
Soit $n_0 = 0$
Soit $n_0 \neq 0 \Rightarrow n_0 \in \mathbb{P}$ et $Im(\psi)$ est un sous-corps de $\mathbb{K}$ isomorphe a $\frac{\mathbb{Z}}{n_0\mathbb{Z}}$

Preuve : $n_0 \neq 0$ et si $n_0 = n_1 n_2$ on a :

$$n_0 1_{\mathbb{K}} = 0_{\mathbb{K}} \Leftrightarrow (n_1 1\mathbb{K})(n_2 1_{\mathbb{K}}) = 0_{\mathbb{K}} \Leftrightarrow n_0 | n_1 \text{ ou } n_0 | n_2$$

Il vient que $p \in \mathbb{P}$, la décomposition canonique de ψ nous assure alors que l'on a un isomorphisme d'anneaux, donc de corps car $n_0\mathbb{P}$ entre $\frac{\mathbb{Z}}{n_0\mathbb{Z}}$ et $Im(\psi)$. Ainsi la caractéristique de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est p

1.5.2 Corps fini (HP)

Soit $\mathbb{L}$ un corps fini (donc commutatif), $\mathbb{K}$ un sous-corps de $\mathbb{L}$. $\mathbb{L}$ est muni d'une structure de $\mathbb{K}$ espace vectoriel de dimension finie . Soit $(\varepsilon_1; ...; \varepsilon_n)$ une $\mathbb{K}$-base de $\mathbb{L}$, alors l'application : $\begin{array}{cccc} u & : & \mathbb{K}^n & \to & \mathbb{L} \\ & & (\lambda_1; ...; \lambda_n) & \mapsto & \sum_{i=1}^n \lambda_i \varepsilon_i \end{array}$ $u \in \mathcal{L}(\mathbb{K}^n, \mathbb{L})$ est un isomorphisme. Par bijectivité : $card(\mathbb{L}) = card(\mathbb{K})^n$ Plus précisement : $\begin{array}{cccc} \psi & : & \mathbb{Z} & \to & \mathbb{L} \\ & & k & \mapsto & k1_{\mathbb{L}} \end{array}$
$\mathbb{Z}$ étant infini et $\mathbb{L}$ fini , donc $Ker(\psi)$ est un idéal fini de $\mathbb{Z}$: $\exists p \in \mathbb{P}, Ker(\psi) = p\mathbb{Z}, p = car(\mathbb{L})$. $Im(\psi)$ est un sous-corps de $\mathbb{L}$ isomorphe à $\frac{\mathbb{Z}}{p\mathbb{Z}}$. Il vient :

$$\boxed{\exists n \in \mathbb{N}^*/card(\mathbb{L}) = card(Im(\psi))^n = p^n}$$

1.5.3 Morphisme de Frobenius (HP)

Soit $\mathbb{K}$ un corps commutatif / $car(\mathbb{K}) = p \in \mathbb{P}$, alors l'application : $\begin{array}{cccc} \psi & : & \mathbb{K} & \to & \mathbb{K} \\ & & x & \mapsto & x^p \end{array}$ est un morphisme de corps

Preuve :

1. $\psi(xy) = (xy)^p = x^p y^p = \psi(x)\psi(y)$

2. $\psi(1) = 1^p = 1$
3. $$\psi(x+y) = (x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{n}{k} x^k y^{p-k}$$

   par définition de la caractéristique : $\forall a \in \mathbb{K}, pa = 0$. En outre $p \in \mathbb{P}, 1 \leq k < p, p | k! \binom{n}{k}$ et $p \wedge k! = 1$, d'après le théorème de Gauss : $p | \binom{n}{k}$, ce qui implique :

   $$\psi(x+y) = x^p + y^p = \psi(x) + \psi(y)$$

   Dans $\mathbb{F}_p, (x + \bar{1})^p = x^p + \bar{1}^p$ on en déduit petit fermat par récurrence.

1.6 Algèbre

1.6.1 Définition

Structure d'algèbre

Soit $\mathbb{K}$ un corps et $(\mathcal{A}, +, \times)$ un ensemble muni de 2 lois interne $+$ et $\times$ et d'une loi externe : $\mathbb{K} \times \mathcal{A} \longrightarrow \mathcal{A}$. On dit $\mathcal{A}$ est une $\mathbb{K}$ algèbre si et seulement si :

1. $(\mathcal{A}, +, \times)$ est un anneau
2. $(\mathcal{A}, +, \cdot)$ est un $\mathbb{K}$ espace-vectoriel
3. $\forall (\lambda, a, b) \in \mathbb{K} \times \mathcal{A}^2, \lambda(a \times b) = (\lambda a) \times b = a \times (\lambda b)$

Exemples

1. Si $\mathbb{K} \subset \mathbb{L}$ est muni d'une structure naturelle de $\mathbb{K}$ algèbre
2. $\mathbb{K}[X]$ est une $\mathbb{K}$-algèbre commutative
3. $\mathcal{M}_n(\mathbb{K})$ est une $\mathbb{K}$-algèbre non commutative
4. Si E est un $\mathbb{K}$-espace vectoriel alors $(\mathcal{L}(E), +, \circ, \cdot)$ est une $\mathbb{K}$-algèbre
5. Soit I un ensemble quelconque $(\mathbb{K}^I, +, \times, \cdot)$ est une $\mathbb{K}$-algèbre

Sous-algèbres

Soit $\mathcal{A}$ une $\mathbb{K}$-algèbre, $\mathcal{B} \subset \mathcal{A}$ est une sous-algèbre de $\mathcal{A}$ si et seulement si :

1. $\mathcal{B}$ est un sous-anneau de $\mathcal{A}$
2. $\mathcal{B}$ est un sous-espace vectoriel
3. $0 \in \mathcal{B}$ et $1 \in \mathcal{B}$
4. $\forall (x, y, \lambda) \in \mathcal{A}^2 \times \mathbb{K}, \lambda x + y \in \mathcal{B}$ et $x \times y \in \mathcal{B}$

Toute intersection de sous-algèbres est une sous-algèbre. Soit $\times$ une partie quelconque de $\mathcal{A}$, on appelle sous-algèbre de $\mathcal{A}$ engendrée par X, l'intersection de toutes les sou-algèbres de $\mathcal{A}$ contenant X

Morphismes d'algèbres

Soit $\mathcal{A}$ et $\mathcal{A}'$ deux $\mathbb{K}$-algèbres, on appelle morphisme d'algèbre, toute application $\varphi : \mathcal{A} \to \mathcal{A}'$ qui est un morphisme d'anneaux et de $\mathbb{K}$ espaces vectoriels :

1. $\forall (x, y, \lambda) \in \mathcal{A}^2 \times \mathbb{K} \varphi(\lambda x + y) = \lambda \varphi(x) + \varphi(y)$
2. $\varphi(xy) = \varphi(x)\varphi(y)$
3. $\varphi(1) = 1$

$Ker(\varphi)$ est un idéal et un sous-espace vectoriel de $\mathcal{A}$. $Im(\varphi)$ est une sous-algèbre de $\mathcal{A}'$

1.6.2 Sous-algèbre engendrée par un élément (HP)

Soit $\mathcal{A}$ une $\mathbb{K}$ algèbre commutative et $a \in \mathcal{A}$. Soit

$$P(X) = \sum_{i=0}^{n} \alpha_i X^i \in \mathbb{K}[X]$$

On définit :

$$P(a) = \sum_{i=0}^{n} \alpha_i a^i \in \mathcal{A}$$

L'application $\begin{array}{cccc} \psi_a & : & \mathbb{K}[X] & \to & \mathcal{A} \\ & & P & \mapsto & P(a) \end{array}$ est un morphisme d'algèbres

$Im(\psi_a) = \{P(a)/P \in \mathbb{K}[X]\} = Vect_{\mathbb{K}}[a^k]_{k\in\mathbb{N}} = \mathbb{K}[a]$ est la sous-algèbre de $\mathcal{A}$ engendrée par a

$Ker(\psi_a)$ est un idéal de $\mathbb{K}[X]$: soit il est réduit à $\{0\}$, ψ_a est injective la famille $(a^k)_{k\in\mathbb{N}}$ est libre et $\mathbb{K}[a]$ est isomorphe à $\mathbb{K}[X]$, $\dim(\mathbb{K}[a]) = +\infty$

$Ker(\psi_a) \neq \{0\}$, c'est un idéal de $\mathbb{K}[X], \exists! P_0 \in \mathbb{K}[X]$ unitaire non nul tel que $Ker(\psi_a) = P_0\mathbb{K}[X]$: P_0 est le polynôme minimal de a : $\forall P \in \mathbb{K}[X], P(a) = 0 \Leftrightarrow P_0 | P$

$\deg(P_0) = n \Rightarrow (1; a; ...; a^{n-1})$ est une base de $\mathbb{K}[a]$ et $\dim_{\mathbb{K}}(\mathbb{K}[a]) = n < +\infty$

Preuve : $\psi_a(1) = 1$

$$\forall (x, y, \lambda) \in \mathcal{K}[X]^2 \times \mathbb{K}, P(X) = \sum_{k\in\mathbb{N}} \alpha_k X^k, Q(X) = \sum_{k\in\mathbb{N}} \beta_k X^k$$

$$\begin{aligned} \psi_a(\lambda P + Q) &= \sum_{k\in\mathbb{N}} (\lambda \alpha_k a^k + \beta_k a^k) \\ &= \lambda \sum_{k\in\mathbb{N}} \alpha_k a^k + \sum_{k\in\mathbb{N}} \beta_k a^k \\ &= \lambda P(a) + Q(a) \\ &= \lambda \psi_a(P) + \psi_a(Q) \end{aligned}$$

$$\psi_a(PQ) = \sum_{k\in\mathbb{N}} \gamma_k a^k / \forall k \in \mathbb{N}, \gamma_k = \sum_{i_1+i_2=k} \alpha_{i_1}\beta_{i_2} a^k$$

$$\begin{aligned}\psi_a(P)\psi_a(Q) &= (\sum_{i_1\in\mathbb{N}}\alpha_{i_1}a^{i_1})(\sum_{i_2\in\mathbb{N}}\beta_{i_2}a^{i_2})\\ &= \sum_{k\in\mathbb{N}}(\sum_{i_1+i_2=k}\alpha_{i_1}\beta_{i_2})a^k\\ &= \sum_{k\in\mathbb{N}}\gamma_k a^k\\ &= \psi_a(PQ)\end{aligned}$$

$Im(\psi_a)$ est une sous-algèbre contenant $a = X(a)$. D'autre part $\mathcal{B}$ une sous-algèbre de $\mathcal{A}$ contenant a, par stabilité pour $\times, 1 \in \mathcal{B}, \forall k \in \mathbb{N}, a^k \in \mathcal{B}$, par combinaison linéaire : $\forall P \in \mathbb{K}[X], P(a) \in \mathcal{B}$ donc $\mathbb{K}[a] \subset \mathcal{B}$

$\mathbb{K}[a]$ est la sous-algèbre engendrée par a

$Ker(\psi_a) = \{0\}$, soit $n \in \mathbb{N}, \alpha_k \in \mathbb{K}$

$$\sum_{k=0}^{n}\alpha_k a^k = 0, P(X) = \sum_{k=0}^{n}\alpha_k X^k$$

$P(a) = 0 \Rightarrow P \in Ker(\psi_a)$
$P = 0 \Rightarrow \forall k \in [|0; n|], \alpha_k = 0$

La famille (α_k) est libre

$Ker(\psi_a) \neq \{0\} \Rightarrow \exists! P_0 \in \mathbb{K}[x]$ unitaire$/Ker(\psi_a) = P_0\mathbb{K}[X]$. Soit

$$(\alpha_k)/\sum_{k=0}^{n-1}\alpha_k a^k = 0, P(X) = \sum_{k=0}^{n-1}\alpha_k X^k$$

$P(a) = 0 \Rightarrow P|P_0$, ainsi $(1; a; ...; a^{n-1})$ est libre. Par ailleurs soit $A \in \mathbb{K}[X]$, par division euclidienne par $P_0, A = QP_0 + R/\deg(R) \leq n-1$

$$A(a) = Q(a)P_0(a) + R(a) = R(a) \in Vect_{\mathbb{K}}[1, ..., a^{n-1}]$$

, donc la famille $(1; a; ...; a^{n-1})$ est génératrice de $\mathbb{K}[a]$

Cas où $\mathcal{A} = \mathbb{L}$ est un sur-corps de $\mathbb{K}$

Soit $a \in \mathbb{L}$, ou bien $\forall P \in \mathbb{K}[X]^*, P(a) \neq 0$, on dit que a est transcendant sur $\mathbb{K}$, $\dim_{\mathbb{K}}(\mathbb{K}[a]) = +\infty$
Ou bien : $\exists P \in \mathbb{K}[X]^*, P(a) = 0$, on dit que a est algébrique sur $\mathbb{K}$
Dans ce cas, soit P_0 son polynôme minimal :

a est irréductible sur $\mathbb{K} \Rightarrow P_0$ irréductible sur $\mathbb{K} \Rightarrow \mathbb{K}[a]$ est un corps

Par ailleurs, Q irréductible unitaire sur $\mathbb{K}$ annulateur de a, alors $Q = P_0$

Preuve : Supposons que $\exists (P_1, P_2) \in \mathbb{K}[X]/P_0 = P_1P_2$

$$\begin{aligned}P_0(a) = P_1(a)P_2(a) &\Rightarrow P_1(a)P_2(a) = 0\\ &\Rightarrow P_1(a) = 0 \text{ ou} P_2(a) = 0, \mathbb{L} \text{ est un corps}\\ &\Rightarrow P_0|P_1 \text{ ou} P_0|P_2\end{aligned}$$

$i \in \{1;2\}/P_0|P_i$ ils sont associés, P_0 est irréductible sur $\mathbb{K}$. D'autre part, soit $x_0 \in \mathbb{K}[a]^*$ et : $\begin{array}{ccccc} f & : & \mathbb{K}[a] & \to & \mathbb{K}[a] \\ & & x & \mapsto & x_0 x \end{array}$ $f \in \mathcal{L}(\mathbb{K}[a])$, injective car $Ker(f) = \{0\}$ Comme $\dim_{\mathbb{K}}(\mathbb{K}[a]) < +\infty, f$ est bijective : $\exists x \in \mathbb{K}[a]/x_0 x = 1, x = x_0^{-1} \in \mathbb{K}[a]$
Une autre méthode consiste à utiliser le théorème de Bézout et le fait que deux polynômes irréductibles qui se divisent sont associés.
Le degré d'algébricité est défini comme étant $n = \deg(P_0) = \dim_{\mathbb{K}}(\mathbb{K}[a])$

Exemples

1. $X^2 - 2$ est irréductible qur $\mathbb{Q}[X]$, il annule $\sqrt{2}$, qui est donc algébrique de degré 2 sur $\mathbb{Q}[X]$
2. Tout les rationnels sont algébrique de degré 1 sur $\mathbb{Q}$: $X - a/a \in \mathbb{Q}7$
3. $)X^3 - 2$ est irréductible sur $\mathbb{Q}[X]$ et annule $\sqrt[3]{2}$, qui est donc algébrique de degré 3 : $(a,b,c) \in \mathbb{Q}^3, a + b\sqrt[3]{2}c\sqrt[3]{4} = 0$, soit $P(X) = a + bX + cX^2 \in \mathbb{Q}[X], P(\sqrt[3]{2}) = 0$
   En considérant $I = \{A \in \mathbb{Q}[X]/A(\sqrt[3]{2}) = 0, \exists! P_0 \text{ unitaire}/I = P_0\mathbb{Q}[X]$, or $X^3 - 2 \in I$ irréductible donc :
   $$X^3 - 2|P \Rightarrow P = 0 \Rightarrow a = b = c = 0$$
4. e et π sont transcendants

1.6.3 Théorème de Liouville (HP)

Soit $\alpha \in \mathbb{R}$ algébrique sur $\mathbb{Q}$ de degré supérieur ou égal à 2. Soit$P_0 \in \mathbb{Q}[X]$ irréductible unitaire sur $\mathbb{Q}$ son polynôme minimal. En multipliant par le PPCM des dénominateurs des coefficients de P_0, on obtient $P_1 \in \mathbb{Z}[X]$ irréductible sur $\mathbb{Q} \setminus \{P_1(\alpha)\} = 0$. $\deg(P_1) = \deg(P_0) = d \geq 2$
Soit $\frac{p}{q} \in \mathbb{Q}, P_1(\frac{p}{q}) \neq 0$ car P_1 est irréductible sur $\mathbb{Q}$ de degré ≥ 2.
Alors : $q^d P_1(\frac{p}{q}) \in \mathbb{Z}^*$ et $|q^\alpha P_1(\frac{p}{q})| \geq 1$, il vient :

$$\frac{1}{q^\alpha} \leq |P_1(\frac{p}{q})| = |P_1(\frac{p}{q}) - P_1(\alpha)|$$

Supposons $\frac{p}{q} \in [\alpha - 1; \alpha + 1]$, notons $M = \sup_{x \in [\alpha-1;\alpha+1]} |P'(x)| > 0$. Si $P_1' = 0$ sur $[\alpha - 1; \alpha + 1]$, P_1 est constant, impossible. Dans ce cas

$$\frac{d}{q} \leq M|\frac{p}{q} - \alpha| \Rightarrow |\frac{p}{q} - \alpha| \geq \frac{1}{Mq^d}$$

Si $|\frac{p}{q} - \alpha| > 1 \geq \frac{1}{q^d}$, en posant $c = \min(1; \frac{1}{M}$, on a :

$$\boxed{\text{a est algébrique de degré d } \Rightarrow \exists c > 0/\forall \frac{p}{q} \in \mathbb{Q}, |\alpha - \frac{p}{q}| \geq \frac{c}{p^d}}$$

Cas de $\sqrt{2}$

Soit $\frac{p}{q} \in \mathbb{Q}$, avec $q \in \mathbb{N}^*$
$|\sqrt{2} - \frac{p}{q}| = \frac{1}{q}|q\sqrt{2} - p| = \frac{1}{q}\frac{|2q^2 - p^2|}{q\sqrt{2}+p} = \frac{1}{q|q\sqrt{2}+p|}$
Or , $|q\sqrt{2} + p| = |p - q\sqrt{2} + 2q\sqrt{2}| \leq |p - q\sqrt{2}| + 2q\sqrt{2} = q|\frac{p}{q} - \sqrt{2}| + 2q\sqrt{2}$
$|\frac{p}{q} - \sqrt{2}| \leq 1 \Rightarrow |q\sqrt{2} + p| \leq (2\sqrt{2} + 1)q \Rightarrow |\sqrt{2} - \frac{p}{q}| \geq \frac{1}{q^2(2\sqrt{2}+1)}$
$\sqrt{2}$ est mal approché par des rationnels

Corollaire

Soit $x \in \mathbb{R}, \exists A > 0$ et $\exists (q_n) \in \mathbb{N}^{\mathbb{N}} \forall n \in \mathbb{N}, q_n \geq 2$ et $\exists (p_n) \in \mathbb{Z}^{\mathbb{N}}$

$$0 < |x - \frac{p_n}{q_n}| \leq \frac{A}{q_n^n}$$

alors x est transcendant

Preuve : si $x \in \mathbb{Q}, x = \frac{p}{q}/(p,q) \in \mathbb{Z} \times \mathbb{N}^*$
$\forall n \in \mathbb{N}, 0 < |q_n p - q p_n| \leq \frac{Aq}{q_n^{n-1}} \leq \frac{Aq}{2^{n-1}}$
Alors $q_n p - q p_n \in \mathbb{Z}^*, 1 \leq |q_n p - q p_n| \leq \frac{Aq}{2^{n-1}}$, ce qui est absurde lorsque n tend vers $+\infty$
Si x était algébrique, d'après le théorème de Liouville :

$$\exists c > 0 / \forall \frac{p}{q} \in \mathbb{Q}, |\alpha - \frac{p}{q}| \geq \frac{c}{p^d}$$

$\frac{c}{(q_n)^d} \leq |x - \frac{p_n}{q_n}| \leq \frac{A}{(q_n)^n} \Rightarrow 0 < c \leq \frac{A}{q_n^{n-d}} \leq \frac{A}{2^{n-d}} \underset{n \to +\infty}{\longrightarrow} 0$
ce qui est absurde donc x est transcendant

Exemple

$$x = \sum_{n=1}^{+\infty} \frac{1}{10^{n!}} = 0,1100010...$$

cette série converge car elle est majorée par la série à termes positifs géométrique de raison 0.1 .
Soit : $\frac{p_n}{10^{n!}} = \sum_{k=1}^{n} \frac{1}{10^{k!}}$

$$\begin{aligned} |x - \frac{p_n}{10^{n!}}| = \sum_{k=n+1}^{+\infty} \frac{1}{10^{k!}} &\leq \sum_{k=1}^{n} \frac{1}{10^k} = \frac{1}{10^{(n+1)!}} \sum_{k=0}^{+\infty} \frac{1}{10^k} \\ &\leq \frac{10}{9 \times 10^{(n+1)!}} \\ &\leq \frac{10}{9 \times (10^{n!})^n} \end{aligned}$$

x est transcendant

1.7 Compléments

1.7.1 Sous-groupes additifs de $\mathbb{R}$

Soit G un sous-groupe de $(\mathbb{R}, +)$ avec $G \neq \{0\}$. Soit $\alpha = \inf(G \cap \mathbb{R}_+^*$:

$\alpha > 0$: $\alpha \in G$ et $G = \alpha\mathbb{Z}$ est monogène
$\alpha = 0$: G est dense dans $\mathbb{R}$

Preuve : cf cours de MPSI

1.7.2 Applications

Théorème

Soit $a \in \mathbb{R} \setminus \mathbb{Q}$ alors $\mathbb{Z} + a\mathbb{Z}$ est dense dans $\mathbb{R}$

Preuve : $G = \mathbb{Z} + a\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$ engendré par a et 1. S'il existait $\alpha \in \mathbb{R}_+^*$ tel que $G = \alpha\mathbb{Z}$ alors $\exists (n, m) \in (\mathbb{Z}^*)^2 / 1 = n\alpha$ et $a = m\alpha$, d'où $a = \frac{m}{n} \in \mathbb{Q}$ absurde

Corollaire

Soit $a \in \mathbb{R} \setminus \mathbb{Q}$ alors $\mathbb{Z} + a\mathbb{N}$ est dense dans $\mathbb{R}$ est encore dense dans $\mathbb{R}$

Exemples

1. Si $\frac{a}{\pi} \in \mathbb{R} \setminus \mathbb{Q}, \mathbb{Z} + \frac{a}{2\pi}\mathbb{N}$ est dense dans $\mathbb{R}$, donc $2\pi\mathbb{Z} + a\mathbb{N}$ est dense dans $\mathbb{R}$
2. Par continuité de sin et exp, il vient que $\{sin(na)/n \in \mathbb{N}\}$ est dense dans $[-1; 1]$ et $\{\exp(ina)/n \in \mathbb{N}\}$ est dense dans $\mathbb{U}$

1.7.3 Polynômes de Tchebychev

Définitions, propriétés

Soit $n \in \mathbb{N}, \forall \theta \in \mathbb{R}, \cos(n\theta) = Re((e^{i\theta})^n) = Re((\cos(\theta) + i\sin(\theta))^n)$

$$\cos(n\theta) = \sum_{0 \leq 2k \leq n} \binom{n}{2k} (i\sin(\theta))^{2k} (\cos(\theta))^{n-2k}$$

On pose :

$$T_n(X) = \sum_{k=0}^{E(\frac{n}{2})} \binom{n}{2k} (X^2 - 1)^k X^{n-2k}$$

C'est l'unique polynôme de $\mathbb{C}[X]$ vérifiant

$$\forall \theta \in \mathbb{R}, T_n(\cos(\theta)) = \cos(n\theta)$$

On a les propriétés suivantes :

1. $\deg(T_n) = n$
2. $\gamma(T_n) = 2^{n-1}$
3. $T_n \in \mathbb{Z}[X]$
4. T_n a la même parité que n
5. $\forall x \in [-1; 1], T_n(x) = \arccos(n\cos(x))$
6. Les polynômes de Tchebychev vérifient la relation de récurrence :

$$\forall n \in \mathbb{N}, T_{n+2} = 2XT_{n+1} - T_n$$

   avec $T_0 = 1$ et $T_1 = X$
7. $T_n \circ T_m = T_m \circ T_n = T_{nm}$

Polynômes de Tchebychev de seconde espèces

En dérivant, $T_n(\cos(\theta)) = \cos(n\theta)$:

$$\sin(\theta)T_n'(\cos(\theta)) = -n\sin(n\theta) \Rightarrow \sin(n\theta) = \frac{\sin(\theta)}{n}T_n'(\cos(\theta))$$

Si n est impair, T_n est impair, donc T_n' est pair et

$$\sin(n\theta) = U_n(\sin(\theta)) \in \mathbb{Z}[X]$$

Si n est pair, T_n' est impair, donc :

$$\sin(n\theta) = \cos(\theta)V_n(\sin(\theta))$$

Des calculs analogues à ceux réalisé pour les polynômes de premières espèces montrent que :

$$U_n(x) = \sum_{k=0}^{E(\frac{n}{2})} (-1)^k \binom{n-k}{k} (2x)^{n-2k}$$

Les racines du polynôme U_n sont de la forme : $\alpha_k^{(n)} = \cos(\frac{k\pi}{n+1})$
Les polynômes de Tchebychev de seconde espèce vérifient l'équation différentielle suivante :

$$(1-X^2)U_n''(X) - 3XU_n'(X) + n(n+2)U_n(X) = 0$$

En dérivant, on obtient les relations suivantes :

$$n^2\cos(n\theta) = \cos(\theta)T_n'(\cos(\theta)) = \sin(\theta)^2 T_n''(\cos(\theta))$$

On obtient une équation différentielle vérifiée par les polynômes de Tchebychev :

$$(X^2-1)T_n'' + XT_n' - n^2T_n = 0$$

En posant :

$$T_n = \sum_{k=0}^{n} a_{k,n}X^k$$

Il vient :

$$\sum_{k=0}^{n-2}((k(k-1)+k-n^2)a_{k,n} - (k+1)(k+2)a_{k+2,n})X^k + ((n-1)(n-2)+n-1-n^2)a_{n-1,n}X^{n-1} + (n(n-1)+n-n^2)a_{n,n}X^n$$

d'où $a_{n,n} = 2^{n-1}$ et $a_{n-1,n} = 0$, par parité. Par récurrence descendante :

$$\forall k \in [|0; E(\frac{n-1}{2})|], a_{n-(2k+1),n} = 0$$

$$\forall k \in [|0; E(\frac{n}{2})|], a_{n-2k,n} = \frac{(n-2k+1)...(n-1)n \times 2^{n-1}}{((n-2k)^2-n^2)...((n-2)^2-n^2)}$$

$$a_{k,n} = \frac{(k+1)(k+2)}{k^2-n^2}a_{k+2,n} \Rightarrow a_{n-2k,n} = \frac{(-1)^k n!2^{n-1}(n-k-1)!}{(n-2k)!2^{2k}k!(n-1)!}$$

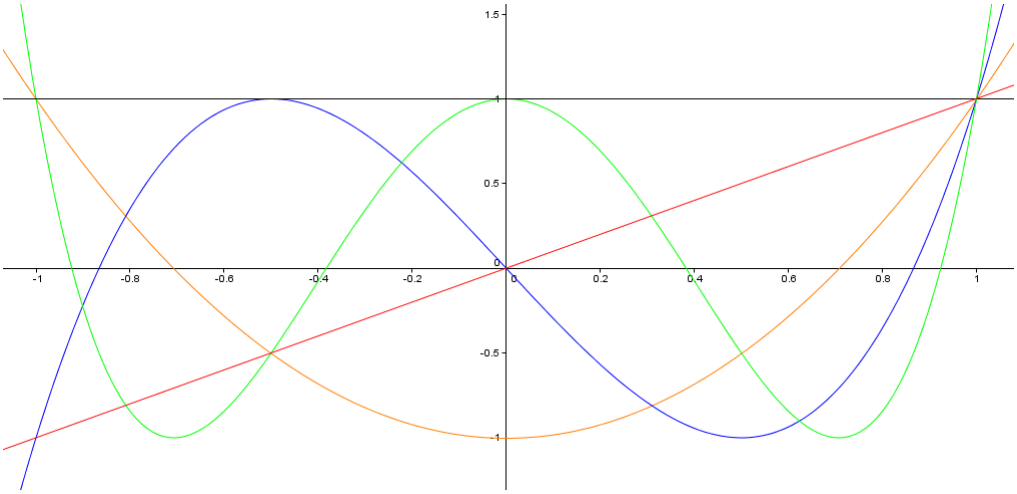


FIGURE 1.2 – Polynômes de Tchebychev de première espèce

Propriétés analytiques

$$T_n(X) = 2^{n-1}\prod_{k=0}^{n-1}(X - x_k) \text{ avec } x_k = \cos(\frac{(2k+1)\pi}{2n}) \in]-1;1[$$

$\forall x \in [-1;1], |T_n(x)| \leq 1$
$T_n(x) = 1 \Leftrightarrow \exists k \in \mathbb{Z}, x = \cos(\frac{2k\pi}{n})$
$T_n(x) = -1 \Leftrightarrow \exists k \in \mathbb{Z}, x = \cos(\frac{2k+1}{n}\pi)$

Théorème

Soit $P \in \mathbb{R}_n[X] / \deg(P) = n, \gamma(P) = 2^{n-1}$

$$\sup_{x\in[-1;1]} |P(x)| = 1 \Leftrightarrow P = T_n$$

On pose $y_p = \cos(\frac{p\pi}{n}, T_n(y_p) = (-1)^p$, si $||P||_\infty < 1$ alors $\forall x \in [-1;1], |P(x)| < 1$, car le sup est atteint : $\deg(P - T_n) \leq n - 1$

$$\forall p \in [|0; n-1|], (P - T_n)(y_p)(P - T_n)(y_{p+1}) = (P(y_p) - (-1)^p)(P(y_{p+1} - (-1)^{p+1}) < 0$$

$P - T_n$ s'annule sur chaque $]y_p; y_{p+1}[, p \in [|0; n-1|]$, donc au moins n fois : nécessairement, $P - T_n = 0$, ce qui est impossible car $||T_n||_\infty = 1$
Si $||P||_\infty = 1, \forall x \in [-1;1], |P(x)| \leq 1, \forall p \in [|0; n-1|], (P - T_n)(y_p)(P - T_n)(y_{p+1}) \leq 0, P - T_n$ s'annule au moins une fois sur $[y_p; y_{p+1}]$
Si $P - T_n$ s'annule en y_{p+1} avec $p \leq n-2$ et y_p avec $p \geq 1$, points intérieurs à $[-1;1]$ et $P'(y_p) = T_n'(y_p) = 0$, extrêma intérieur. En dénombrant les multiplicités, $P - T_n$ s'annule au moins n fois : $P - T_n = 0 \Rightarrow P = T_n$

1.7.4 Produit de convolution

Définition

Soient f et g deux fonctions réelles ou complexes, on note $f * g$ leur produit de convolution :

$$(f * g)(x) = \int_{-\infty}^{+\infty} f(x-t)g(t)dt = \int_{-\infty}^{+\infty} f(t)g(x-t)dt$$

Pour des suites (u_n) et (v_n) réelles ou complexes, on définit leur produit de convolution :

$$(u * v)_n = \sum_{m=-\infty}^{+\infty} u_{n-m}v_m = \sum_{m=-\infty}^{+\infty} u_m v_{n-m}$$

Propriétés

Les produits de convolution continu ou discret vérifient les propriétés suivantes :

1. Commutativité
2. Distributivité du produit de convolution sur l'addition
3. Associativité
4. Compatibilité avec les translations : on définit $(\tau_h f)(x) = f(x-h)$

$$((\tau_h f) * g)(x) = \int_{-\infty}^{+\infty} f(x-t-h)g(t)dt = (\tau_h(f*g))(x)$$

5. Intégration :

$$\int_{-\infty}^{+\infty} (f*g)(t)dt = (\int_{-\infty}^{+\infty} f(t)dt)(\int_{-\infty}^{+\infty} g(t)dt)$$

6. Dérivation : si f et g sont deux fonctions complexes dérivables,

$$(f*g)' = f' * g = f * g'$$

7. Si f et g sont paires alors $(f*g)$ est paire