19 Structures algébriques et arithmétique

« In the judgement of the most competent living mathematicians, Fräulein Noether was the most significant creative mathematical genius thus far produced since the higher education of women began. In the realm of algebra, in which the most gifted mathematicians have been busy for centuries, she discovered methods which have proved of enormous importance in the development of the present-day generation of younger mathematicians. »

Albert Einstein, à propos d'Emmy Noether

Plan de cours

I | Structure de groupe

A – Groupes et sous-groupes

Définition 19.1 : Groupe

Un groupe est un couple $(G,*)$ constitué d'un ensemble G et d'une loi de composition interne $*$ tels que :

(i) la loi $*$ est associative : $\forall x,y,z\in G,\quad x*(y*z)=(x*y)*z$;

(ii) il existe un élément neutre : $\forall x\in G,\quad x*e=e*x=x$;

(iii) tout élément de G possède un inverse : $\forall x\in G,\quad \exists y\in G,\quad x*y=y*x=e$.

Quelques remarques en vrac :

- Les notations sont très variables et on privilégiera selon le contexte une notation additive $(+)$, multiplicative $(\times)$ ou bien de composition de fonctions $(\circ)$. On omettra parfois même de noter la loi, s'il n'y a aucune ambiguïté. Toujours en fonction du contexte, on parlera d'élément inverse, de symétrique ou bien d'opposé. Par convention, la notation additive est en général réservée aux groupes abéliens, c'est-à-dire aux groupes commutatifs. La notation multiplicative est la plus courante.
- L'associativité de la loi permet de se dispenser de tout parenthésage.
  Exemples de lois de composition non associatives : $(x,y)\mapsto x\wedge y$ sur $\mathbb{R}^3$, $(u,v)\mapsto u\circ v-v\circ u$ sur $\mathscr{L}(E)$.
- Lorsqu'ils existent, l'élément neutre et l'inverse d'un élément sont uniques.
- L'existence d'un inverse permet de simplifier les expressions : $ax=ay\Longrightarrow x=y$.

Exemples

- Groupes additifs : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathscr{M}_n(\mathbb{K})$. Groupes multiplicatifs : $\mathbb{Q}^*$, $\mathbb{Q}_+^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$, $\mathbb{C}^*$, $\mathbb{U}$ et $\mathrm{GL}_n(\mathbb{K})$.
- Si $\mathfrak{S}_X$ désigne l'ensemble des bijections (ou permutations) d'un ensemble X, $(\mathfrak{S}_X,\circ)$ est un groupe.

Proposition 19.2

Si $(G_1,*_1)$ et $(G_2,*_2)$ désignent deux groupes, alors $(G_1\times G_2,*)$ est un groupe, avec $*$ définie par :

$$\forall (x_1,x_2),(y_1,y_2)\in G_1\times G_2,\quad (x_1,x_2)*(y_1,y_2)=(x_1*_1y_1,x_2*_2y_2)$$

Par récurrence immédiate, tout produit fini de groupes est encore un groupe.

Définition 19.3 : Sous-groupe

Soit $(G,*)$ un groupe. On dit que $H \subset G$ est un sous-groupe de G si $(H,*)$ est un groupe.

On retiendra plutôt la caractérisation suivante.

Proposition 19.4 : Caractérisation d'un sous-groupe

Soit $(G,*)$ un groupe. $H \subset G$ est un sous-groupe de G si H est non vide et si :

$$\forall x, y \in H, \quad x * y^{-1} \in H$$

On vérifiera donc en pratique que $e \in H$, que H est stable par $*$ et enfin que pour tout $x \in H$, $x^{-1} \in H$.

Exemples

- $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$.
- L'ensemble des matrices triangulaires d'ordre n est un sous-groupe de $\mathcal{M}_n(\mathbb{K})$ (pour quelle loi ?).
- $\mathrm{O}(E)$ et $\mathrm{SO}(E)$ sont des sous-groupes de $(\mathrm{GL}(E), \circ)$.

Exercice 1

On appelle centre du groupe $(G,\star)$ l'ensemble défini par :

$$\mathrm{Z}(G) = \{a \in G \mid \forall b \in G,\ a \star b = b \star a\}$$

Montrer que $\mathrm{Z}(G)$ est un sous-groupe de G. Quel est le centre de $\mathrm{GL}_n(\mathbb{K})$?

Exercice 2

Soient E un ensemble non vide, $(\mathfrak{S}_E, \circ)$ son groupe de permutations et $x \in E$. On pose :

$$\mathrm{Stab}_x = \{\sigma \in \mathfrak{S}_E \mid \sigma(x) = x\}$$

Montrer que Stab_x est un sous-groupe de $\mathfrak{S}_E$.

Théorème 19.5 : Sous-groupes de $\mathbb{Z}$

Si G est un sous-groupe de $(\mathbb{Z},+)$, alors il existe un unique $n \in \mathbb{N}$ tel que $G = n\mathbb{Z}$.

Démonstration

Si $G = \{0\}$, le résultat est immédiat. Supposons désormais $G \neq \{0\}$.

- Si G contient $x \in \mathbb{Z}^*$, il contient également $-x$, ce qui nous assure que $G \cap \mathbb{N}^*$ est non vide. $G \cap \mathbb{N}^*$ admet donc un plus petit élément noté n.
- Comme $n \in G$ et G est un groupe, $n\mathbb{Z} \subset G$.
- Réciproquement, soit $m \in G$.
  Par division euclidienne, il existe un unique couple d'entiers (p, r) tel que :

  $$m = pn + r \text{ avec } 0 \leqslant r < n$$

  Comme $m \in G$ et $pn \in G$, $r \in G \cap \mathbb{N}$. Par définition de n, r est nécessairement nul, ce qui montre que $m \in n\mathbb{Z}$. Ainsi, $G = n\mathbb{Z}$. ■

Proposition 19.6 : Intersection de sous-groupes

Soit $(H_i)_{i\in I}$ une famille de sous-groupes de G. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

En revanche, la réunion de sous-groupes n'a aucune raison, en général, d'être un sous-groupe.

Exercice 3

Identifier le sous-groupe $p\mathbb{Z} \cap q\mathbb{Z}$ pour deux entiers p et q quelconques.

B – Morphismes de groupes

Pour comparer les groupes entre eux, nous allons faire appel aux morphismes de groupes. Ce sont les applications qui préservent la structure de groupes.

Définition 19.7 : Morphisme de groupes

On appelle morphisme du groupe $(G,*)$ dans le groupe $(G',\star)$ toute application $\phi : G \to G'$ qui vérifie :

$$\forall x, y \in G, \quad \phi(x*y) = \phi(x) \star \phi(y)$$

Exemples

Parmi les exemples les plus classiques, on peut citer :

$$\exp : (\mathbb{R},+) \to (\mathbb{R}_+^*,\times); \quad \ln : (\mathbb{R}_+^*,\times) \to (\mathbb{R},+); \quad |\cdot| : (\mathbb{C}^*,\times) \to (\mathbb{R}_+^*,\times);$$

$$\det : (\mathrm{GL}_n(\mathbb{K}),\times) \to (\mathbb{K}^*,\times); \quad \varepsilon : (\mathfrak{S}_n,\circ) \to (\{-1,1\},\times)$$

On rappelle que $\varepsilon(\sigma)$ désigne la signature d'une permutation σ de $[\![1,n]\!]$.

Exercice 4

Montrer que $\theta \mapsto \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$ est un morphisme de $(\mathbb{R},+)$ dans $(\mathrm{SO}_2(\mathbb{R}),\times)$.

Exercice 5

Soient e l'élément neutre d'un groupe G, e' celui d'un groupe G' et ϕ un morphisme de G dans G'.
Vérifier que $\phi(e) = e'$ et que pour tout $x \in G$, $\phi(x)^{-1} = \phi(x^{-1})$.

Les deux propositions qui suivent sont assez utiles pour montrer qu'un ensemble possède une structure de groupe.

Proposition 19.8 : Images directe et réciproque d'un sous-groupe

Soit ϕ un morphisme du groupe $(G,*)$ dans le groupe $(G',\star)$.

(i) Si H est un sous-groupe de G, $\phi(H)$ est un sous-groupe de G'.

(ii) Si H' est un sous-groupe de G', $\phi^{-1}(H')$ est un sous-groupe de G.

Démonstration

Montrons la première propriété. Notons e l'élément neutre de G (donc de H) et e' celui de G'.

- $\phi(e) = e'$ donc $e' \in \phi(H)$.
- Pour tous $x', y' \in \phi(H)$, il existe $x, y \in G$ tels que $x' = \phi(x)$ et $y' = \phi(y)$. D'où,

$$x' \star (y')^{-1} = \phi(x) \star \phi(y)^{-1} = \phi(x) \star \phi(y^{-1}) = \phi(x * y^{-1})$$

Ainsi, $x' \star (y')^{-1} \in \phi(H)$.

La démonstration est analogue dans le cas de l'image réciproque. ■

On en déduit que $\mathrm{Im}(\phi) = \phi(G)$ et $\mathrm{Ker}(\phi) = \phi^{-1}(\{e'\})$ sont respectivement des sous-groupes de G' et G.

Définition 19.9 : Noyau et image d'un morphisme

Soit ϕ un morphisme du groupe $(G,*)$ dans le groupe $(G',\star)$.

- On appelle image de ϕ et on note $\mathrm{Im}(\phi)$ le sous-groupe $\phi(G) = \{\phi(x), x \in G\}$.
- On appelle noyau de ϕ et on note $\mathrm{Ker}(\phi)$ le sous-groupe $\phi^{-1}(\{e'\}) = \{x \in G, \phi(x) = e'\}$.

Exemple

$\mathrm{SO}_n(\mathbb{R})$ est un groupe en tant que noyau de $\det : \mathrm{O}_n(\mathbb{R}) \to \{-1,1\}$.

Proposition 19.10

Un morphisme ϕ est injectif si et seulement si $\mathrm{Ker}(\phi) = \{e\}$.

Démonstration

$\Longrightarrow$ Supposons ϕ injective et soit $x \in \mathrm{Ker}(\phi)$. $\phi(x) = e' = \phi(e)$ donc $x = e$. Ainsi, $\mathrm{Ker}(\phi) = \{e\}$.

$\Longleftarrow$ Supposons que $\mathrm{Ker}(\phi) = \{e\}$ et soient $x, y \in G$ tel que $\phi(x) = \phi(y)$.

$$\phi(x) \star \phi(y)^{-1} = e' \quad \text{donc} \quad \phi(x * y^{-1}) = e'$$

D'où $x * y^{-1} = e$, soit $x = y$. ϕ est bien injective. ■

Définition 19.11

Soit ϕ un morphisme du groupe $(G,*)$ dans le groupe $(G',\star)$.

- Si ϕ est bijectif, ϕ est qualifié d'isomorphisme.
- Si ϕ est bijectif et $G = G'$, alors ϕ est qualifié d'automorphisme.

La réciproque ϕ^{-1} d'un isomorphisme ϕ est lui-même... un isomorphisme!

Établir que deux groupes sont isomorphes revient à montrer qu'ils possèdent la même structure, c'est-à-dire que l'un est la parfaite copie de l'autre via l'isomorphisme ϕ.

Exemples

exp est un isomorphisme de $(\mathbb{R},+)$ dans $(\mathbb{R}_+^*,\times)$, ln est l'isomorphisme réciproque.

Attention, si deux groupes finis possèdent le même nombre d'éléments, ils ne sont pas pour autant isomorphes.

Exemple

Voici la table des deux seuls [1] groupes à 4 éléments. Autrement dit, tout groupe à 4 éléments est isomorphe à l'un de ces deux groupes. En guise d'illustration, on pensera aux groupes $\mathbb{U}_4$ et $\mathbb{U}_2^2$.

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

Groupe $\mathbb{Z}/4\mathbb{Z}$

$\star$	x	y	z	t
x	x	y	z	t
y	y	x	t	z
z	z	t	x	y
t	t	z	y	x

Groupe de Klein

Ces deux groupes abéliens ne peuvent être isomorphes. En effet, supposons qu'il existe un isomorphisme ϕ entre les deux. On aurait $\phi(a) = x$ et $\phi(c) = \phi(b * b) = \phi(b)^2 = x$. Donc $\phi(a) = \phi(c)$: contradiction!

Exercice 6

Montrer que les groupes $\mathbb{U}$ et $\mathrm{SO}_2(\mathbb{R})$ sont isomorphes.

Exercice 7 – Automorphismes intérieurs

Soient $(G,*)$ un groupe et $g \in G$. On considère l'application $\phi_g : x \mapsto g * x * g^{-1}$ définie sur G.

- Montrer que ϕ_g est un automorphisme de G.
- Montrer que $g \mapsto \phi_g$ est un morphisme de $(G,*)$ dans $(\mathfrak{S},\circ)$ où $\mathfrak{S}$ est l'ensemble des permutations de G. Quel est son noyau?

1. à isomorphisme près, nous y reviendrons!

C – Groupe $(\mathbb{Z}/n\mathbb{Z},+)$

Dans tout ce paragraphe, n désigne un entier naturel non nul. Rappelons que si $a,b\in\mathbb{Z}$,

$$a\equiv b\,[n] \iff n\mid(a-b) \iff a-b\in n\mathbb{Z}$$

Théorème / Définition 19.12

La congruence modulo n est une relation d'équivalence.
On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence de $\mathbb{Z}$ pour cette relation.

Pour $a\in\mathbb{Z}$, on note souvent $\overline{a}$ la classe d'équivalence associée à la relation de congruence modulo n. L'entier a est appelé représentant de cette classe. Cette classe est un ensemble contenant l'entier a et tous les entiers congrus à a modulo n :

$$\overline{a}=\{a+kn\mid k\in\mathbb{Z}\}=a+n\mathbb{Z}$$

En particulier, $\overline{0}=\{\ldots,-2n,-n,0,n,2n,\ldots\}=n\mathbb{Z}$.
Le principe de division euclidienne nous assure que :

$$\mathbb{Z}/n\mathbb{Z}=\left\{\overline{0},\overline{1},\ldots,\overline{n-1}\right\}$$

$\mathbb{Z}/n\mathbb{Z}$ est aussi parfois noté $\mathbb{Z}_n$.

Proposition 19.13

Si $\overline{a_1}=\overline{a_2}$ et $\overline{b_1}=\overline{b_2}$, alors :

$$\overline{a_1+b_1}=\overline{a_2+b_2} \quad\text{et}\quad \overline{a_1\times b_1}=\overline{a_2\times b_2}$$

Démonstration

Si $a_1\equiv a_2\,[n]$ et $b_1\equiv b_2\,[n]$, alors $a_1+b_1\equiv a_2+b_2\,[n]$. De même, $a_1b_1\equiv a_2b_2\,[n]$. ■

Cela signifie que lorsque l'on travaille modulo n, on peut choisir n'importe quel représentant de la classe pour mener les calculs. Forts de ce résultat, nous pouvons définir une addition (mais aussi une multiplication) sur les éléments de $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire des opérations qui portent directement sur les classes d'équivalence :

$$\forall(a,b)\in\mathbb{Z}^2,\quad \overline{a}+\overline{b}=\overline{a+b} \quad\text{et}\quad \overline{a}\times\overline{b}=\overline{ab}$$

($+$: addition dans $\mathbb{Z}/n\mathbb{Z}$; $+$: addition dans $\mathbb{Z}$)

Théorème 19.14

Pour tout $n\in\mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe abélien.

Démonstration

Pour $n\in\mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z},+)$ vérifie les propriétés suivantes :

- commutativité : $\forall a,b\in\mathbb{Z},\ \overline{a}+\overline{b}=\overline{a+b}=\overline{b+a}=\overline{b}+\overline{a}$
- associativité : $\forall a,b,c\in\mathbb{Z},\ \left(\overline{a}+\overline{b}\right)+\overline{c}=\overline{a+b}+\overline{c}=\overline{a+b+c}=\overline{a}+\overline{b+c}=\overline{a}+\left(\overline{b}+\overline{c}\right)$
- existence d'un élément neutre : $\forall a\in\mathbb{Z},\ \overline{a}+\overline{0}=\overline{a+0}=\overline{a}$
- inversibilité des éléments : $\forall a\in\mathbb{Z},\ \overline{a}+\overline{-a}=\overline{a-a}=\overline{0}$

Ainsi, $\overline{-3}=\overline{8}$ est l'inverse de $\overline{3}$ pour la loi $+$ dans $\mathbb{Z}/11\mathbb{Z}$.

L'application $a\mapsto\overline{a}$ est un morphisme surjectif[2] de $(\mathbb{Z},+)$ dans $(\mathbb{Z}/n\mathbb{Z},+)$. Cette application a pour noyau $n\mathbb{Z}$.

Nous montrerons que $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est en fait un anneau.

2. ce qui revient finalement à montrer en des termes à peine différents que $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe.

D – Sous-groupes engendrés, groupes monogènes et groupes cycliques

Définition 19.15

Soit A une partie d'un groupe $(G,*)$. Le sous-groupe engendré par A est l'intersection de tous les sous-groupes de G contenant A.

C'est bien un sous-groupe de G ; c'est même le plus petit contenant A, au sens de l'inclusion.

(i) si $A=\{a\}$ avec a un élément de G, en notant $\langle a\rangle$ le sous-groupe engendré,

$$\langle a\rangle=\left\{a^k \mid k\in\mathbb{Z}\right\} \quad \text{(notation multiplicative)} \quad \text{ou bien} \quad \langle a\rangle=\{ka \mid k\in\mathbb{Z}\} \quad \text{(notation additive)}$$

En effet, tout sous-groupe de G contenant a contient nécessairement les puissances de a et par ailleurs, l'ensemble des puissances de a est bien un sous-groupe de G.

On notera que $\phi_a : \left|\begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & a^k \end{array}\right.$ est un morphisme de groupes dont l'image est $\langle a\rangle$.

(ii) si $A=\{a_1,\dots,a_n\}$ est une partie d'un groupe abélien G, en notant $\langle a_1,\dots,a_n\rangle$ le sous-groupe engendré,

$$\langle a_1,\dots,a_n\rangle=\left\{a_1^{\alpha_1}\cdots a_n^{\alpha_n} \mid (\alpha_1,\dots,\alpha_n)\in\mathbb{Z}^n\right\}$$

Sans commutativité de $a_1,\dots,a_n$, cette égalité devient fausse. Par exemple, en général, $ab^2a^2\neq a^3b^2$.

(iii) Si A est une partie quelconque de G, en notant $\langle A\rangle$ le sous-groupe engendré,

$$x\in\langle A\rangle \iff \exists r\in\mathbb{N},\quad \exists(x_1,\dots,x_r)\in A^r,\quad \exists(\alpha_1,\dots,\alpha_r)\in\mathbb{Z}^r,\quad x=x_1^{\alpha_1}\cdots x_r^{\alpha_r}$$

Exemples

- $(\mathbb{Z},+)$ est engendré par 1 (mais aussi par -1) ; $(\mathbb{U}_n,\times)$ est engendré par $e^{2i\pi/n}$;
- $(\mathrm{GL}_n(\mathbb{K}),\times)$ est engendré par les transvections et les dilatations ;
- $(\mathrm{O}_2(\mathbb{R}),\times)$ est engendré par les réflexions ;
- $(\mathfrak{S}_n,\circ)$ est engendré par les transpositions.

Définition 19.16

Un groupe $(G,*)$ est dit :

- monogène s'il est engendré par un élément : $G=\langle a\rangle=\{a^k, k\in\mathbb{Z}\}$;
- cyclique s'il est monogène et fini.

On notera qu'un groupe monogène est nécessairement abélien.

Exemple

$(\mathbb{U}_n,\times)$ est cyclique.

Théorème 19.17

Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est cyclique. De plus, $\mathbb{Z}/n\mathbb{Z}=\langle\overline{k}\rangle$ si et seulement si k est premier avec n.

On commencera par déterminer les sous-groupes engendrés par $\overline{k}$ dans $\mathbb{Z}/4\mathbb{Z}$ pour $k\in\{0,1,2,3\}$.

Démonstration

$\mathbb{Z}/n\mathbb{Z}$ est un groupe fini et, de façon directe, $\mathbb{Z}/n\mathbb{Z}=\langle\overline{1}\rangle$.
Cherchons maintenant les autres générateurs de $\mathbb{Z}/n\mathbb{Z}$ en considérant $k\in\mathbb{Z}$.

$$\langle\overline{k}\rangle=\mathbb{Z}/n\mathbb{Z}=\langle\overline{1}\rangle \iff \exists a\in\mathbb{Z},\quad a\overline{k}=\overline{1} \iff \exists a\in\mathbb{Z},\quad \overline{ak}=\overline{1} \iff \exists(a,b)\in\mathbb{Z}^2,\quad ak+bn=1$$

D'après le théorème de Bézout, k engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k\wedge n=1$. ■

Le groupe $(\mathbb{Z},+)$ est monogène et le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est même quant à lui cyclique. Ce ne sont pas de simples exemples parmi d'autres, tous les groupes monogènes s'y ramènent comme le montre le théorème suivant.

Théorème 19.18 : Classification des groupes monogènes

- Tout groupe monogène infini est isomorphe à $(\mathbb{Z},+)$.
- Tout groupe monogène fini (c'est-à-dire cyclique) de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.

Démonstration

Soit $G=\langle a\rangle$ un groupe monogène. On considère le morphisme de groupes surjectif $\phi_a : \left|\begin{array}{ccc}\mathbb{Z} & \longrightarrow & \langle a\rangle \\ k & \longmapsto & a^k\end{array}\right.$
$\mathrm{Ker}(\phi_a)$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$. Deux possibilités :

- Si $n=0$, $\mathrm{Ker}(\phi_a)=\{0\}$ donc ϕ_a est injective. G est alors isomorphe à $\mathbb{Z}$.
- Supposons maintenant $n\neq 0$. Pour tout entier relatif p, il existe $(q,r)\in\mathbb{Z}\times\{0,\dots,n-1\}$ tel que $p=nq+r$.
  Comme $a^n=e$, $a^p=a^{nq}a^r=a^r$. Ainsi, $\mathrm{Im}(\phi_a)=\langle a\rangle=\{e,a,\dots,a^{n-1}\}$.
  Cet ensemble possède bien n éléments distincts. En effet, il n'y a pas de « doublon » puisque :

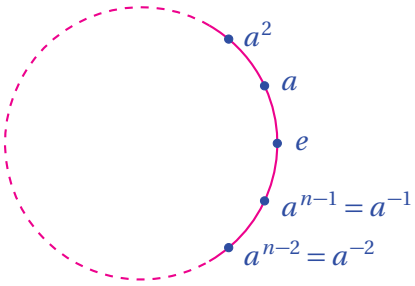
$$a^k=a^{k'} \iff a^{k-k'}=e \iff k-k'\in n\mathbb{Z} \iff \overline{k}=\overline{k'}$$

Autrement dit, le morphisme $\varphi : \left|\begin{array}{ccc}\mathbb{Z}/n\mathbb{Z} & \longrightarrow & \langle a\rangle \\ \overline{k} & \longmapsto & a^k\end{array}\right.$ est un isomorphisme de groupes.

Exemple

Le groupe $(\mathbb{U}_n,\times)$ est donc, en tant que groupe cyclique de cardinal n, isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.

Représentation d'un groupe monogène infini



Représentation d'un groupe monogène fini

E – Ordre d'un élément dans un groupe

D'après le théorème précédent, le groupe monogène $\langle a\rangle$ est soit isomorphe à $\mathbb{Z}$ soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un certain entier naturel n non nul. Ce qui amène à la définition suivante.

Définition 19.19

Soient $(G,*)$ un groupe et a un élément de G.

- On dit que a est d'ordre fini s'il existe $n\in\mathbb{N}^*$ tel que $\langle a\rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
- On appelle alors ordre de a l'entier naturel n.

En notant n l'ordre de a, $\langle a\rangle=\{e,a,\dots,a^{n-1}\}$. L'ordre de a est le plus petit entier p non nul tel que $a^p=e$.

Exemple

Le nombre complexe j est d'ordre 3 et $\langle j\rangle=\{1,j,j^2\}$.

Exercice 8

- Quel est l'ordre de $\overline{2}$ et $\overline{3}$ dans $(\mathbb{Z}/5\mathbb{Z},+)$?
- Quel est l'ordre de j dans $(\mathbb{C}^*,\times)$? À quelle condition $z\in\mathbb{C}^*$ est-il d'ordre fini ?
- À quelle condition les rotations de $\mathbb{R}^2$ sont-elles d'ordre fini ?

Proposition 19.20

Si a est d'ordre fini n, alors, pour tout p dans $\mathbb{Z}$: $\quad a^p = e \quad \Longleftrightarrow \quad n|p$.

Démonstration

C'est encore et toujours une question de division euclidienne. En effet, si l'on suppose $a^p = e$, on peut alors écrire $p = qn + r$ avec $0 \leqslant r < n$ et donc, $a^p = a^{qn}a^r = a^r = e$. Si $r \in \{1, \dots, n-1\}$, cela contrevient à la définition de n. Nécessairement $r = 0$, donc $n|p$. La réciproque est immédiate. ■

Exercice 9

Trouver les éléments de $(\mathbb{Z}/4\mathbb{Z}, +)$ et de $((\mathbb{Z}/2\mathbb{Z})^2, +)$ d'ordre 2. Ces deux groupes sont-ils isomorphes ?

Théorème 19.21

L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.

On appelle parfois ordre du groupe son cardinal, lorsque celui-ci est fini.

Démonstration

La démonstration n'est exigible que pour G commutatif ; une preuve générale sera présentée en TD.

Soit a un élément du groupe $(G, *)$ supposé fini, de cardinal n, et pour la cause, abélien.

- L'élément a est nécessairement d'ordre fini. S'il ne l'était pas, les éléments de $\langle a \rangle$ seraient nécessairement deux à deux distincts et a engendrerait alors un sous-groupe de G de cardinal infini, impossible. Nous noterons par la suite d l'ordre de a.
- Il est facile de vérifier que l'application $\phi_a : \begin{array}{|l} G \longrightarrow G \\ g \longmapsto a * g \end{array}$ est une bijection [3]. D'où :

$$\prod_{g \in G} g = \prod_{g \in G} \phi_a(g) = \prod_{g \in G} (a * g) = a^n \prod_{g \in G} g$$

(G abélien)

Par simplification, $a^n = e$ donc $d|n$. ■

Exercice 10

Vérifier cette propriété dans $(\mathbb{Z}/6\mathbb{Z}, +)$.

Attention, il n'existe pas toujours d'élément dont l'ordre est égal à n'importe quel diviseur de n.

II | Structures d'anneau et de corps

A – Anneaux et corps

Définition 19.22 : Anneau

Un anneau est un triplet $(A, +, \times)$ constitué d'un ensemble et de deux lois de composition interne tels que :

(i) $(A, +)$ est un groupe commutatif ;

(ii) la loi $\times$ est associative, admet un élément neutre et est distributive sur $+$:

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

Quelques remarques en vrac :

- On note en général 0_A l'élément neutre pour l'addition, 1_A l'élément neutre pour la multiplication.
- L'anneau est dit *commutatif* lorsque la loi $\times$ est commutative.
- Un anneau commutatif est dit *intègre* s'il est non nul et si : $\quad \forall (x, y) \in A^2, \quad x \times y = 0_A \Longrightarrow x = 0_A$ ou $y = 0_A$.

Un anneau intègre n'admet donc pas d'autre diviseur de 0 que lui-même.

3. On pensera à expliciter la bijection réciproque.

Exemples

Parmi les exemples les plus classiques d'anneaux, on peut citer :

$$(\mathbb{Z},+,\times),\quad (\mathbb{K},+,\times),\quad (\mathbb{K}[X],+,\times),\quad (\mathscr{M}_n(\mathbb{K}),+,\times),\quad (\mathscr{L}(E),+,\circ)\quad \text{et}\quad \left(\ell^1(\mathbb{N}),+,\times\right)$$

La structure d'anneau permet de retrouver des résultats déjà établis dans $\mathbb{K}$ ou $\mathscr{M}_n(\mathbb{K})$: si x et y commutent,

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k};\quad x^n-y^n=(x-y)\sum_{k=0}^{n-1}x^k y^{n-1-k}\quad \text{et}\quad (1_A-x)\sum_{k=0}^{n}x^k=1_A-x^{n+1}$$

Proposition 19.23

Si A_1 et A_2 désignent deux anneaux alors $(A_1\times A_2,+,\times)$ est un anneau pour les lois définies par :

$$\forall (x_1,x_2),(y_1,y_2)\in A_1\times A_2,\quad (x_1,x_2)+(y_1,y_2)=(x_1+y_1,x_2+y_2)\quad \text{et}\quad (x_1,x_2)\times(y_1,y_2)=(x_1y_1,x_2y_2)$$

Par récurrence immédiate, tout produit fini d'anneaux est encore un anneau.

Définition 19.24 : Sous-anneau

Soit $(A,+,\times)$ un anneau. On dit que $B\subset A$ est un sous-anneau de A si $(B,+,\times)$ est un anneau contenant 1_A.

Proposition 19.25 : Caractérisation d'un sous-anneau

Soit $(A,+,\times)$ un anneau. $B\subset A$ est un sous-anneau de A si et seulement si $1_A\in B$ et :

$$\forall x,y\in B,\quad x-y\in B\quad \text{et}\quad x\times y\in B$$

Exemples

- $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$.
- L'ensemble des matrices diagonales d'ordre n est un sous-anneau commutatif de $\mathscr{M}_n(\mathbb{K})$.
- $\mathbb{Z}[i]=\mathbb{Z}+i\mathbb{Z}=\{a+ib\mid (a,b)\in\mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$.

Définition 19.26

Soit $(A,+,\times)$ un anneau.

- On dit qu'un élément $x\in A$ est inversible s'il est inversible pour la loi $\times$.
- On note parfois A^* l'ensemble des éléments de A inversibles.

Exemples

- L'ensemble des inversibles de $\mathbb{Z}$ est $\{-1,1\}$.
- $\mathscr{M}_n(\mathbb{K})^*=\mathrm{GL}_n(\mathbb{K})$.

Définition 19.27 : Corps

Un corps est un anneau commutatif non nul pour lequel tout élément non nul admet un inverse pour la loi $\times$.

Dans le cadre du programme, les corps sont supposés commutatifs. Un corps est un anneau intègre.

Définition 19.28 : Sous-corps

Soit $(\mathbb{K},+,\times)$ un corps. On dit que $\mathbb{K}'\subset\mathbb{K}$ est un sous-corps de $\mathbb{K}$ si $(\mathbb{K}',+,\times)$ est un corps.

Proposition 19.29 : Caractérisation d'un sous-corps

Soit $(\mathbb{K},+,\times)$ un corps. $\mathbb{K}'\subset\mathbb{K}$ est un sous-corps de $\mathbb{K}$ si et seulement si :

$$\forall x,y\in\mathbb{K}'\times\mathbb{K}'^*,\quad x-y\in\mathbb{K}'\quad \text{et}\quad x\times y^{-1}\in\mathbb{K}'$$

Exemples

$(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ et $(\mathbb{K}(X),+,\times)$ sont des corps. $\mathbb{Q}$ et $\mathbb{R}$ sont des sous-corps de $\mathbb{C}$.

B – Morphismes d'anneaux

Définition 19.30 : Morphisme d'anneaux

Soient A et B deux anneaux. On appelle morphisme de A dans B toute application $\phi : A \to B$ qui vérifie :

(i) $\forall x, y \in A,\ \phi(x+y) = \phi(x) + \phi(y)$ (ii) $\forall x, y \in A,\ \phi(x \times y) = \phi(x) \times \phi(y)$ (iii) $\phi(1_A) = 1_B$

Le point (i) assure qu'un morphisme d'anneaux est un morphisme de groupes. Si $\phi(0_A) = 0_B$ découle de la définition, ce n'est pas le cas de l'égalité $\phi(1_A) = 1_B$.

Si ϕ est de plus bijectif, on le qualifie d'isomorphisme d'anneaux.

Exercice 11

Montrer que pour tout élément x inversible de A, $\phi(x)$ est inversible dans B et $\phi(x)^{-1} = \phi\left(x^{-1}\right)$.

Définition 19.31 : Noyau et image d'un morphisme

Soit ϕ un morphisme de l'anneau A dans l'anneau B.

- On appelle image de ϕ et on note $\mathrm{Im}(\phi)$ l'ensemble $\phi(A) = \{\phi(x), x \in A\}$.
- On appelle noyau de ϕ et on note $\mathrm{Ker}(\phi)$ l'ensemble $\phi^{-1}(\{0_B\}) = \{x \in A, \phi(x) = 0_B\}$.

Proposition 19.32

L'image d'un morphisme d'anneaux est un anneau.

En revanche le noyau d'un morphisme d'anneaux de A dans B n'est pas, en général, un sous-anneau de A.

Exercice 12

Soit $\phi : A \to B$ un isomorphisme d'anneaux. Montrer que ϕ^{-1} est un isomorphisme puis que x est inversible dans A si et seulement si $\phi(x)$ est inversible dans B.

C – Idéaux d'un anneau commutatif

1 – Généralités

Soit $\phi : A \to B$ un morphisme d'anneaux. Si $\mathrm{Ker}(\phi)$ n'est pas en général un sous-anneau de A, en revanche, $\mathrm{Ker}(\phi)$ est un sous-groupe de $(A,+)$ qui vérifie de plus :

$$\forall x \in \mathrm{Ker}(\phi), \quad \forall a \in A, \quad xa \in \mathrm{Ker}(\phi) \quad \text{et} \quad ax \in \mathrm{Ker}(\phi)$$

En effet, en conservant les notations, $\phi(ax) = \phi(a) \times \phi(x) = 0_B$ et $\phi(xa) = \phi(x) \times \phi(a) = 0_B$.

On dit alors que $\mathrm{Ker}(\phi)$ est un idéal (bilatère) de A, ce qui amène la définition suivante.

Définition 19.33 : Idéal d'un anneau commutatif

Soit $(A,+,\times)$ un anneau commutatif. On appelle idéal de A toute partie I de A tel que :

(i) $(I,+)$ est un sous-groupe de $(A,+)$;

(ii) I est stable par multiplication par tout élément de A : $\forall x \in I, \quad \forall a \in A, \quad xa \in I$.

On dit parfois que I est absorbant pour la loi $\times$.

En particulier, nous avons prouvé que le noyau d'un morphisme d'anneaux est un idéal.

Exemples

- $2\mathbb{Z}$ est un idéal de l'anneau $\mathbb{Z}$ et, plus généralement, $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.
- L'ensemble des suites réelles qui convergent vers 0 est un idéal de l'anneau des suites réelles convergentes.

Théorème / Définition 19.34 : Idéal principal

Soit x un élément d'un anneau commutatif A. $xA = \{xa \mid a \in A\}$ est le plus petit idéal de A contenant x. On l'appelle idéal principal engendré par x et on le note parfois (x).

On rappelle que l'on note $a|b$ pour a, b éléments d'un anneau commutatif s'il existe $c \in A$ tel que $b = c \times a$. Alors,

$$x \mid y \iff yA \subset xA \iff (y) \subset (x)$$

Proposition 19.35 : Opérations sur les idéaux

Soient I_1 et I_2 deux idéaux d'un anneau commutatif A. Alors,

- $I_1 \cap I_2$ est un idéal de A ;
- $I_1 + I_2 = \{x_1 + x_2 \mid (x_1, x_2) \in I_1 \times I_2\}$ est un idéal de A.

2 – Arithmétique dans $\mathbb{Z}$

Théorème 19.36

Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, où $n \in \mathbb{N}$.

Démonstration

Un idéal de $\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ donc de la forme $n\mathbb{Z}$. Réciproquement, on montre que $n\mathbb{Z}$ est stable par multiplication : c'est bien un idéal de $\mathbb{Z}$. Les idéaux de $\mathbb{Z}$ sont donc tous principaux. ■

Rappelons que $n\mathbb{Z} = m\mathbb{Z}$ si et seulement si $n = \pm m$.

Pour $a, b \in \mathbb{Z}$, $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de $\mathbb{Z}$ donc il existe un unique $c \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$.
De même, $a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$ donc il existe un unique $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Définition 19.37

Soient $a, b \in \mathbb{Z}$.

- On appelle plus grand diviseur commun de a et b l'unique entier naturel d tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On le note $\text{pgcd}(a, b)$ ou $a \wedge b$.
- On appelle plus petit commun multiple de a et b l'unique entier naturel c tel que $a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$. On le note $\text{ppcm}(a, b)$ ou $a \vee b$.

Il reste à vérifier que le PGCD et le PPCM ainsi définis sont bien les mêmes que ceux entrevus par le passé.

Théorème 19.38 : Théorème de Bézout

Soient $a, b \in \mathbb{Z}$.

- Il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b$.
  Une telle relation est appelée relation de Bézout de a et b.
- a et b sont premiers entre eux si et seulement s'il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

Démonstration

La première propriété découle directement de la deuxième. Justifions celle-ci.

$\boxed{\Longrightarrow}$ Supposons que $a \wedge b = 1$. Alors $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$, donc 1 s'écrit sous la forme $au + bv$ avec $u, v \in \mathbb{Z}$.

$\boxed{\Longleftarrow}$ Supposons que $1 = au + bv$. En multipliant par $n \in \mathbb{Z}$, on obtient $n = a(nu) + b(nv)$ donc $\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$.
Comme l'inclusion inverse est immédiate, on a $\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ et donc $a \wedge b = 1$. ■

L'algorithme d'Euclide est une méthode efficace pour déterminer le pgcd de deux entiers. Il repose sur le résultat suivant : si a et b sont deux entiers relatifs non nuls et si $a = bq + r$ où q est le quotient et r le reste de la division euclidienne de a par b, $a \wedge b = b \wedge r$.

Théorème 19.39 : Lemme de Gauss

Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Démonstration

Retranscrivons les hypothèses : $bc\mathbb{Z} \subset a\mathbb{Z}$ et $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$. En multipliant par c, il vient $c\mathbb{Z} \subset a\mathbb{Z}$. ■

Une conséquence directe : si p est premier et $p \mid ab$, alors $p \mid a$ ou $p \mid b$; c'est le lemme dit d'Euclide.
En revanche, méfiance, si a et b ne sont pas premiers entre eux, on peut avoir $a \mid bc$ sans que a divise c.

D – L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Théorème 19.40

Le triplet $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau.

Démonstration

Nous avons déjà prouvé que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien. L'élément $\overline{1}$ est neutre pour la multiplication.
Il ne reste qu'à montrer que la loi $\times$ est associative et distributive, ce qui est chose aisée. ■

Exercice 13

Donner les tables de multiplication de $\mathbb{Z}/4\mathbb{Z}$ et de $\mathbb{Z}/5\mathbb{Z}$.
Quels sont leurs éléments inversibles ? Sont-ce des anneaux intègres ?

Proposition 19.41

L'élément $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.

Démonstration

Grâce au théorème de Bézout,

$$\exists a \in \mathbb{Z},\quad \overline{a} \times \overline{k} = \overline{ak} = \overline{1} \quad\Longleftrightarrow\quad \exists (a,b) \in \mathbb{Z}^2,\quad ak + bn = 1 \quad\Longleftrightarrow\quad n \wedge k = 1$$ ■

La preuve nous fournit une méthode pour trouver l'inverse d'un élément de $\mathbb{Z}/n\mathbb{Z}$.

Exemple

Cherchons l'inverse de 11 dans $\mathbb{Z}/42\mathbb{Z}$. Pour cela, appliquons l'algorithme d'Euclide étendu afin de trouver une relation de Bézout. 11 étant premier, il est premier avec 42, et :

$$\begin{aligned} 42 &= 11 \times 3 + 9 & 1 &= 9 - 2 \times 4 \\ 11 &= 9 \times 1 + 2 & &= 9 - (11 - 9 \times 1) \times 4 \\ 9 &= 2 \times 4 + 1 & &= 9 \times 5 - 11 \times 4 \\ 2 &= 1 \times 2 + 0 & &= (42 - 11 \times 3) \times 5 - 11 \times 4 \\ \text{d'où } 42 \wedge 11 &= 2 \wedge 1 = 1 & &= 42 \times 5 - 11 \times 19 \end{aligned}$$

Ainsi, $42 \times 5 - 11 \times 19 = 1$, c'est-à-dire $11 \times (-19) \equiv 1\ [42]$. Donc l'inverse de $\overline{11}$ est $\overline{-19} = \overline{23}$.

Théorème 19.42

Soit $n \in \mathbb{N}^*$. Les assertions suivantes sont équivalentes :

(i) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

(ii) $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.

(iii) n est premier.

Démonstration

(i)$\Longrightarrow$(ii) : tout corps est intègre.

(ii)$\Longrightarrow$(iii) : procédons par contraposition. Supposons que n n'est pas premier. Il existe donc $a, b \in \mathbb{N}^*$ tels que $n = ab$ avec $a, b \in [\![2, n-1]\!]$. Donc $\overline{a} \times \overline{b} = \overline{0}$ sans que $\overline{a}$ ni $\overline{b}$ ne soient nuls.

(iii)$\Longrightarrow$(i) : si n est premier, tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles, à l'exception de $\overline{0}$. ■

Lorsque p est premier, on note traditionnellement $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

Théorème 19.43 : Lemme chinois

Si m et n sont deux entiers premiers entre eux,

$$\mathbb{Z}/mn\mathbb{Z} \text{ est isomorphe à } \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

Démonstration

Pour $m \wedge n = 1$, construisons un isomorphisme d'anneaux naturel entre $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
Pour cela, on va note $\overline{x}$, $\hat{x}$ et $\tilde{x}$ les classes d'équivalence respectives de x. Soit maintenant l'application :

$$\phi : \left| \begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{x} & \longmapsto & (\hat{x}, \tilde{x}) \end{array} \right.$$

Cette application est bien définie dans le sens où $(\hat{x}, \tilde{x})$ ne dépend pas du choix du représentant de $\overline{x}$. En effet, $\widehat{x + knm} = \hat{x}$ et $\widetilde{x + knm} = \tilde{x}$ pour tout $k \in \mathbb{Z}$. De plus,

- ϕ est un morphisme de groupes puisque pour tous $x, y \in \mathbb{Z}$,

$$\phi(\overline{x} + \overline{y}) = \phi(\overline{x+y}) = (\widehat{x+y}, \widetilde{x+y}) = (\hat{x} + \hat{y}, \tilde{x} + \tilde{y}) = \phi(\overline{x}) + \phi(\overline{y})$$

- On vérifie de même que pour tous $x, y \in \mathbb{Z}$, $\phi(\overline{x} \times \overline{y}) = \phi(\overline{x}) \times \phi(\overline{y})$.
- Ajoutons que $\phi(\overline{1}) = (\hat{1}, \tilde{1})$.
- Last but not least, les deux anneaux de départ et d'arrivée ont même cardinal et :

$$x \in \mathrm{Ker}(\phi) \iff \hat{x} = \hat{0} \quad \text{et} \quad \tilde{x} = \tilde{0} \iff n \mid x \quad \text{et} \quad m \mid x$$

n et m étant supposés premiers entre eux, $nm \mid x$ donc $\mathrm{Ker}(\phi) = \{\overline{0}\}$. ϕ est bien un isomorphisme. ■

Plus prosaïquement, le théorème chinois affirme que pour $n \wedge m = 1$, l'ensemble des solutions du système

$$\begin{cases} x \equiv a\ [n] \\ x \equiv b\ [m] \end{cases}$$

est $x_0 + mn\mathbb{Z}$, x_0 étant l'unique antécédent par ϕ du couple (a, b) dans $\mathbb{Z}/mn\mathbb{Z}$.
On montre par récurrence que si la factorisation première de n est $p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$,

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \left(\frac{\mathbb{Z}}{p_1^{\alpha_1}\mathbb{Z}}\right) \times \cdots \times \left(\frac{\mathbb{Z}}{p_r^{\alpha_r}\mathbb{Z}}\right)$$

La résolution d'équations dans $\mathbb{Z}/n\mathbb{Z}$ se ramène de la sorte à une résolution dans des anneaux plus simples.

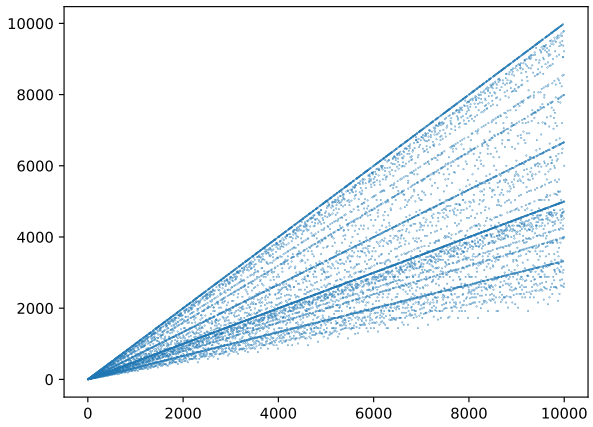
Définition 19.44 : Indicatrice d'Euler

Pour $n \in \mathbb{N}^*$, on pose $\varphi(n) = \mathrm{card}\{k \in [\![1, n]\!] \mid k \wedge n = 1\}$. La fonction φ est appelée indicatrice d'Euler.

$\varphi(n)$ représente donc le nombre d'entiers inférieurs à n et premiers avec n. Mais c'est également :

- le nombre d'éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ (on note parfois l'ensemble des inversibles $(\mathbb{Z}/n\mathbb{Z})^*$).
- le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, c'est donc aussi celui de $(\mathbb{U}_n, \times)$.

Naturellement, $\varphi(1) = 1$ et pour tout entier premier p, $\varphi(p) = p - 1$.



Représentation de l'indicatrice d'Euler

$\varphi(n)$	0	1	2	3	4	5	6	7	8	9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Les 99 premières valeurs de φ

Exercice 14 – Formule sommatoire

Montrer que pour tout $n \in \mathbb{N}^*$, $n = \sum_{d|n} \varphi(d)$.

Proposition 19.45

Soient $m, n \in \mathbb{N}^*$. Si $m \wedge n = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$.

Démonstration

Tout repose sur le lemme chinois. En effet, si $m \wedge n = 1$, alors $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes. Ils possèdent donc le même nombre d'éléments inversibles. Or les inversibles de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont les couples (a, b) où a et b sont des éléments inversibles de $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$. Ainsi, $\varphi(mn) = \varphi(m)\varphi(n)$. ■

Proposition 19.46

Pour tout $n \in \mathbb{N}^*$, $\varphi(n) = n \cdot \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \frac{1}{p}\right)$.

Démonstration

- Soient p un entier premier et $\alpha \in \mathbb{N}^*$. $\varphi(p) = p - 1$.
- Quels sont maintenant les entiers compris entre 1 et p^α non premiers avec p^α ? Ce sont exactement les nombres qui admettent p comme diviseur, c'est-à-dire les multiples de p (compris entre 1 et p^α). Il y en a précisément $p^{\alpha-1}$. Ainsi, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
- Soit $n = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$ la factorisation première de n. Les entiers $p_i^{\alpha_i}$ étant premiers entre eux,

$$\varphi(n) = \varphi(p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}) = \cdots = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r})$$
$$= \prod_{i=1}^{r} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r} \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Ainsi, $\varphi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$. ■

Comment expliquer l'alignement de certains points sur le graphe de φ ? C'est très simple :

- $\varphi(p) = p - 1$ donc les points de coordonnées $(p, p-1)$ appartiennent à la droite d'équation $y = x - 1$.
- $\varphi(p^\alpha) = p^\alpha \left(1 - \frac{1}{p}\right)$ donc les points d'abscisse p^α appartiennent aux droites d'équations $y = (1 - \frac{1}{p})x$, etc.

Lemme 19.47

Soit $n \in \mathbb{N}^*$. L'ensemble des éléments inversibles $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe pour la loi $\times$.

Proposition 19.48 : Théorème d'Euler

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N} \setminus \{0,1\}$. Si $a \wedge n = 1$, alors :

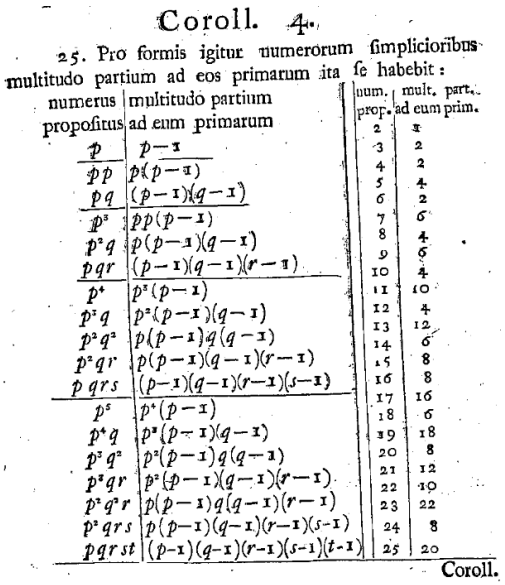
$$a^{\varphi(n)} \equiv 1\,[n]$$

Démonstration

$\varphi(n)$ n'est rien d'autre que le cardinal du groupe des inversibles $((\mathbb{Z}/n\mathbb{Z})^*, \times)$. Si $a \wedge n = 1$, $\overline{a}$ est un élément de ce groupe, donc :

$$\overline{a}^{\varphi(n)} = \overline{1} \iff a^{\varphi(n)} \equiv 1\,[n]$$

■



Coroll. 4.

25. Pro formis igitur numerorum simplicioribus multitudo partium ad eos primarum ita se habebit :

numerus propositus	multitudo partium ad eum primarum	num. prop.	mult. part. ad eum prim.
p	$p-1$	2	1
pp	$p(p-1)$	3	2
pq	$(p-1)(q-1)$	4	2
p^3	$pp(p-1)$	5	4
p^2q	$p(p-1)(q-1)$	6	2
pqr	$(p-1)(q-1)(r-1)$	7	6
p^4	$p^3(p-1)$	8	4
p^3q	$p^2(p-1)(q-1)$	9	6
p^2q^2	$p(p-1)q(q-1)$	10	4
p^2qr	$p(p-1)(q-1)(r-1)$	11	10
$pqrs$	$(p-1)(q-1)(r-1)(s-1)$	12	4
p^5	$p^4(p-1)$	13	12
p^4q	$p^3(p-1)(q-1)$	14	6
p^3q^2	$p^2(p-1)q(q-1)$	15	8
p^3qr	$p^2(p-1)(q-1)(r-1)$	16	8
p^2qrs	$p(p-1)(q-1)(r-1)(s-1)$	17	16
$pqrst$	$(p-1)(q-1)(r-1)(s-1)(t-1)$	18	6
		19	18
		20	8
		21	12
		22	10
		23	22
		24	8
		25	20

Coroll.

Theorema arithmetica nova methodo demonstrata, Leonhard Euler, 1763

On retrouve directement le petit théorème de Fermat au programme de MPSI.

Corollaire 19.49 : Petit théorème de Fermat

Soient p un entier premier et $a \in \mathbb{Z}$. Alors,

$$a^p \equiv a\,[p]$$

Si de plus p ne divise pas a, $a^{p-1} \equiv 1\,[p]$.

E – Anneaux de polynômes à une indéterminée

Dans ce paragraphe, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

1 – Division euclidienne et idéaux de $\mathbb{K}[X]$

Théorème 19.50 : Division euclidienne

Soient $A, B \in \mathbb{K}[X]$ où $B \neq \tilde{0}$. Il existe alors un unique couple $(Q,R) \in \mathbb{K}[X]$ tel que :

$$A = BQ + R \quad \text{et pour lequel} \quad \deg(R) < \deg(B)$$

Théorème 19.51

Les idéaux de $\mathbb{K}[X]$ sont les ensembles $(P) = P \cdot \mathbb{K}[X] = \{P \cdot Q \mid Q \in \mathbb{K}[X]\}$ pour $P \in \mathbb{K}[X]$.

Les idéaux de $\mathbb{K}[X]$ sont donc tous principaux.

Démonstration

Soit I un idéal de $\mathbb{K}[X]$. $(\tilde{0})$ est un idéal de $\mathbb{K}[X]$. Intéressons-nous désormais au cas où $I \neq \{\tilde{0}\}$.

- Soit P un polynôme non nul de I de degré minimal. Remarquons que $(P) \subset I$.
- Soit $A \in I$. Effectuons la division euclidienne de A par P. On trouve :

$$A = BP + R \quad \text{avec} \quad \deg(R) < \deg(P)$$

Comme I est un idéal, $BP \in I$. De plus, $(I,+)$ étant un groupe, $R = A - BP \in I$. Par minimalité du degré de P, il vient $R = \tilde{0}$, et donc $A = BP$. Les éléments de I sont donc exactement les multiples de P. ■

On montre que $(P)=(Q)$ si et seulement si $Q=\alpha P$, avec $\alpha\in\mathbb{K}^*$. Tout idéal de $\mathbb{K}[X]$ distinct de $\{\tilde{0}\}$ est donc engendré par un unique polynôme unitaire. Ce dernier est alors qualifié de polynôme minimal.

Exemple – Polynôme minimal d'un endomorphisme

Soient E un espace vectoriel de dimension finie et $u\in\mathscr{L}(E)$ non nul. $\{P\in\mathbb{K}[X]\mid P(u)=0_{\mathscr{L}(E)}\}\subset\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$. On montre qu'il n'est pas réduit à $\{\tilde{0}\}$. Il existe donc un unique polynôme unitaire qui engendre cet idéal, c'est le polynôme minimal de u !

$$(\pi_u)=\{P\in\mathbb{K}[X]\mid P(u)=0_{\mathscr{L}(E)}\}$$

2 – PGCD, PPCM et autres questions de divisibilité

De même que l'on a défini PGCD et PPCM pour les entiers relatifs au moyen des idéaux, nous pouvons définir PGCD et PPCM d'un couple ou d'une famille de polynômes. Si A et B sont deux polynômes,

$$(A)+(B)=\{AU+BV\mid(U,V)\in\mathbb{K}[X]^2\}\text{ est un idéal de }\mathbb{K}[X]$$

Cet idéal est donc engendré par un unique polynôme unitaire, appelé PGCD du couple (A,B).

Définition 19.52

Soient $A,B\in\mathbb{K}[X]$.

- On appelle plus grand diviseur commun de A et B l'unique polynôme unitaire ou nul qui engendre l'idéal $\{AU+BV\mid(U,V)\in\mathbb{K}[X]^2\}$. On le note $\text{pgcd}(A,B)$ ou $A\wedge B$.
- On appelle plus petit commun multiple de A et B l'unique polynôme unitaire ou nul qui engendre l'idéal $(A)\cap(B)$. On le note $\text{ppcm}(A,B)$ ou $A\vee B$.

On montre alors que pour tout polynôme $D\in\mathbb{K}[X]$,

$$D\mid A\quad\text{et}\quad D\mid B\iff D\mid A\wedge B$$

$A\wedge B$ est donc l'unique polynôme (unitaire) de plus haut degré qui divise à la fois A et B.

On étend la définition du PGCD à celle d'une famille de polynômes non nuls. $P_1\wedge\cdots\wedge P_n$ est l'unique polynôme unitaire vérifiant :

$$(P_1\wedge\cdots\wedge P_n)=\{P_1U_1+\cdots+P_nU_n\mid(U_1,\ldots,U_n)\in\mathbb{K}[X]^n\}$$

Enfin, deux polynômes sont premiers entre eux si $A\wedge B=1$. Cela signifie que leurs seuls diviseurs communs sont les polynômes constants.

Théorème 19.53 : Théorème de Bézout

Soient $A,B\in\mathbb{K}[X]$.

- Il existe un couple $(U,V)\in\mathbb{K}[X]^2$ tel que $AU+BV=A\wedge B$.
- A et B sont premiers entre eux si et seulement s'il existe un couple $(U,V)\in\mathbb{K}[X]^2$ tel que $AU+BV=1$.

Théorème 19.54 : Lemme de Gauss

Soient $A,B,C\in\mathbb{K}[X]$. Si $A\mid BC$ et $A\wedge B=1$, alors $A\mid C$.

3 – Décomposition en facteurs irréductibles dans $\mathbb{K}[X]$

Définition 19.55

Un polynôme $P\in\mathbb{K}[X]$ est irréductible si :

$$P=QR\text{ avec }Q,R\in\mathbb{K}[X]\implies Q\text{ ou }R\text{ constant}$$

Tout polynôme de degré 1 est nécessairement irréductible.

Proposition 19.56

Tout polynôme $P \in \mathbb{K}[X]$ admet une unique décomposition comme produit d'un scalaire par un produit de facteurs unitaires irréductibles (à permutation des facteurs près).

Le fait que tout polynôme soit scindé sur $\mathbb{C}$ garantit que les seuls irréductibles de $\mathbb{C}[X]$ sont de degré 1.

Théorème 19.57 : Théorème de d'Alembert-Gauss

Un polynôme complexe non constant admet au moins une racine dans $\mathbb{C}$.

Tout polynôme $P \in \mathbb{C}[X]$ de degré $n \geqslant 1$ admet donc exactement n racines dans $\mathbb{C}$ (comptées avec leur ordre de multiplicité) et peut s'écrire sous la forme :

$$P = \lambda \prod_{i=1}^{n} (X - \alpha_i) \quad (\alpha_i \in \mathbb{C})$$

Soient $P \in \mathbb{R}[X]$ et $\alpha \in \mathbb{C}$. Si α est racine de P, il en va de même pour $\overline{\alpha}$. On peut dès lors factoriser P par :

$$(X-\alpha)(X-\overline{\alpha}) = X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2 \in \mathbb{R}[X]$$

Tout polynôme de $\mathbb{R}[X]$ se factorise sous forme d'un produit de polynômes de degré 1 et de polynômes de degré 2 à discriminant négatif.

Théorème 19.58 : Polynômes irréductibles

- Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
- Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et de degré 2 à discriminant négatif.

En pratique, on commencera par décomposer un polynôme dans $\mathbb{C}[X]$ pour faire apparaître les facteurs réels en regroupant les racines conjuguées et ainsi obtenir sa décomposition dans $\mathbb{R}[X]$.

III | Structure d'algèbre

Définition 19.59 : Algèbre

Une algèbre sur un corps $\mathbb{K}$, ou $\mathbb{K}$-algèbre, est un ensemble $\mathscr{A}$ munis de trois lois $+$, $\times$ et $\cdot$ tels que :

(i) $(\mathscr{A}, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel ;

(ii) $(\mathscr{A}, +, \times)$ est un anneau ;

(iii) les lois $\times$ et $\cdot$ sont compatibles :

$$\forall a, b \in \mathbb{K}, \quad \forall x, y \in \mathscr{A}, \quad (a \cdot x) \times (b \cdot y) = ab \cdot (x \times y)$$

Exemples

Parmi les exemples les plus classiques, on peut citer :

$$(\mathbb{K}[X], +, \times, \cdot), \quad (\mathscr{M}_n(\mathbb{K}), +, \times, \cdot), \quad (\mathscr{L}(E), +, \circ, \cdot) \quad \text{et} \quad (\mathscr{F}(I, \mathbb{K}), +, \times, \cdot)$$

Une sous-algèbre de $\mathscr{A}$ est une partie $\mathscr{B}$ de $\mathscr{A}$ telle que $\mathscr{B}$ est à la fois un sous-anneau de $\mathscr{A}$ et un sous-espace vectoriel de $\mathscr{A}$. On peut par exemple citer l'ensemble des fonctions de classe $\mathscr{C}^\infty$ définies sur un intervalle et à valeurs dans $\mathbb{K}$ ou bien les matrices carrées d'ordre n triangulaires supérieures.

Définition 19.60 : Morphisme d'algèbres

Soient $\mathscr{A}$ et $\mathscr{B}$ deux $\mathbb{K}$-algèbres. On appelle morphisme de $\mathscr{A}$ dans $\mathscr{B}$ toute application $\phi : \mathscr{A} \to \mathscr{B}$ telle que ϕ est un morphisme d'anneaux et ϕ un morphisme d'espaces vectoriels.

Exemple

Pour $a \in \mathbb{K}$, l'application $P \mapsto P(a)$ est un morphisme entre les $\mathbb{K}$-algèbres $(\mathbb{K}[X], +, \times, \cdot)$ et $(\mathbb{K}, +, \times, \cdot)$.