

Jean Franchini
Jean-Claude Jacquens

MATHS

Cours

Exercices et travaux dirigés corrigés

MP-MP*

MPI-MPI*

NOUVEAUX
PROGRAMMES

ellipses

1. Algèbre générale

I. Groupes et sous-groupes

1. Groupes

Nous rappelons dans ce tout premier paragraphe, des résultats vus en MPSI.

1.1. Définition

Un ensemble $G \neq \emptyset$ muni d'une loi de composition interne \star est un groupe si cette loi est associative, s'il existe un élément neutre et si tout élément de G a un symétrique pour la loi \star dans G . Si de plus \star est commutative, le groupe est dit commutatif ou abélien.

1.2. Exemples

$(\mathbb{K}, +)$ est un groupe abélien si $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou \mathbb{C} .

(\mathbb{K}^*, \times) est un groupe abélien si $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_+, \mathbb{R}_+, \mathbb{U}, \mathbb{U}_n$.

$(\mathfrak{S}(E), \circ)$ est le groupe des permutations (bijections) de l'ensemble E .

(\mathfrak{S}_n, \circ) : groupe des permutations de $\llbracket 1, n \rrbracket$ est le groupe symétrique d'ordre n .

1.3. Propriétés

- Dans un groupe, l'élément neutre est unique.
- Dans un groupe, le symétrique de tout élément est unique.
- Si a, b sont deux éléments d'un groupe (G, \cdot) , alors $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

2. Produit de groupes

2.1. Théorème et définition

Si G_1 et G_2 sont deux groupes, alors $G_1 \times G_2$ est muni d'une loi de composition interne notée :

$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$ en notation additive,

$(x_1, x_2) \times (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2)$ en notation multiplicative.

Muni de cette loi $G_1 \times G_2$ a une structure de groupe.

2.2. Exemples

Si $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ alors, pour $n \geq 2$, $(\mathbb{K}^n, +)$ est un groupe abélien.

3. Sous-groupes

3.1. Définition

Une partie non vide H de G est un sous-groupe de (G, \star) si elle est stable par \star et si, munie de la loi induite, elle a une structure de groupe.

3.2. Caractérisations

Soit (G, \star) un groupe. H est un sous-groupe de (G, \star) si l'une des assertions équivalentes suivantes est vraie.

(i) $(H \subset G), (H \neq \emptyset)$ et $(\forall(x, y) \in H^2, x \star y' \in H)$ où y' est le symétrique de y dans G .

(ii) $(H \subset G), (H \neq \emptyset), (\forall(x, y) \in H^2, x \star y \in H)$ et $y' \in H$ où y' est le symétrique de y dans G .

3.3. Exemples

- $\{-1, 1\}$ est un sous-groupe de (\mathbb{R}^*, \times) .
- $\mathbb{Z}[i] = \{z \in \mathbb{C} \mid \exists(a, b) \in \mathbb{Z}^2, z = a + ib\}$ est un sous-groupe de $(\mathbb{C}, +)$.
- $\mathbb{K}^{(I)} = \{x = (x_i) \in \mathbb{K}^I \mid x_i = 0 \text{ sauf sur une partie finie de } I\}$ est un sous-groupe additif de \mathbb{K}^I .
- Si G est un groupe additif (*resp.* multiplicatif), le sous-groupe $\text{gr}(a)$ défini par : $\text{gr}(a) = \{ka \mid k \in \mathbb{Z}\}$ (*resp.* $\{a^k \mid k \in \mathbb{Z}\}$) est le sous-groupe de G engendré par l'élément a de G .

3.4. Intersection

Soit (G, \cdot) un groupe. Si $(G_i)_{i \in I}$ est une famille de sous-groupes de (G, \cdot) , alors leur intersection est un sous-groupe de G .

Démonstration

Notons F l'intersection des $G_i, i \in I$ et e l'élément neutre de G . Comme $e \in G_i$, pour tout $i \in I$, on a $e \in F$. Si $(x, y) \in F^2$, alors $(x, y) \in G_i^2$ pour tout $i \in I$. Comme les G_i sont des sous-groupes de G , pour tout $i \in I, xy^{-1} \in G_i$. Donc $xy^{-1} \in F$. Il s'ensuit que F est un sous-groupe de G . \square

Remarque

La réunion de sous-groupes n'est en général pas un sous-groupe. En effet, \mathbb{R}^2 muni de la loi $+$ définie par $(x, y) + (x', y') = (x + x', y + y')$ est un groupe, d'après 2.2. On montre aisément que $G_1 = \mathbb{R} \times \{0\}$ et $G_2 = \{0\} \times \mathbb{R}$ sont des sous-groupes de $(\mathbb{R}^2, +)$, mais que $G_1 \cup G_2$ n'est pas un sous-groupe de $(\mathbb{R}^2, +)$; en effet, $(1, 1) = (1, 0) + (0, 1) \notin G_1 \cup G_2$ alors que $(1, 0) \in G_1 \subset G_1 \cup G_2$ et que $(0, 1) \in G_2 \subset G_1 \cup G_2$.

Mais, si $\forall(i, j) \in I^2, \exists k \in I, G_i \cup G_j \subset G_k$, on vérifie aisément que la réunion des G_i est un sous-groupe de G .

En particulier si $I = \mathbb{N}$ et si la suite $(G_n)_{n \geq 0}$ est croissante (pour l'inclusion), la réunion des G_n est un sous-groupe de G .

4. Génération

4.1. Définition

Soit (G, \cdot) un groupe et A une partie de G . L'intersection des sous-groupes de (G, \cdot) contenant A est le plus petit sous-groupe de G contenant A . On l'appelle le **sous-groupe de (G, \cdot) engendré par A** , on le note $\text{gr}(A)$. On dit aussi que A est une **partie génératrice** de $\text{gr}(A)$.

Comme intersection de sous-groupes, $\text{gr}(A)$ est un sous-groupe de (G, \cdot) .

4.2. Théorème

Soient (G, \cdot) un groupe d'élément neutre e et A une partie de G .
 Si $A = \emptyset$, alors $\text{gr}(A) = \{e\}$, sinon, $\text{gr}(A)$ est l'ensemble des produits $a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$ où n varie dans \mathbb{N}^* et pour $1 \leq i \leq n$, les a_i sont dans A et les ε_i dans $\{-1, 1\}$.

Démonstration

Si A est non vide, il suffit de montrer que l'ensemble H des produits $a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$ où n varie dans \mathbb{N}^* et pour $1 \leq i \leq n$, les a_i sont dans A et les ε_i dans \mathbb{Z} , est un sous-groupe de G contenant A .

Si $a \in A$, alors $a = a^1 \in H$. Donc H est non vide et contient A .

Si x et y sont éléments de H , il existe deux entiers naturels p et q tels que $x = a_1^{\alpha_1} \dots a_p^{\alpha_p}$, $y = b_1^{\beta_1} \dots b_q^{\beta_q}$ où $(a_i, b_i) \in A^2$ et $(\alpha_i, \beta_i) \in \mathbb{Z}^2$.

Donc $y^{-1} = b_q^{-\beta_q} \dots b_1^{-\beta_1} \in H$ et $x \cdot y^{-1} \in H$. \square

4.3. Exemples

- $\{1\}$ est une partie génératrice du groupe $(\mathbb{Z}, +)$.
- $\mathbb{R} \cup \{i\}$ est une partie génératrice du groupe $(\mathbb{C}, +)$.
- Si E est un plan vectoriel euclidien, $(\mathcal{O}(E), \circ)$ est engendré par l'ensemble des réflexions de E .
- Si $\tau_{i,j}$ est la transposition de $\llbracket 1, n \rrbracket$ qui échange i et j , les parties A , B et C suivantes sont des parties génératrices du groupe symétrique (\mathfrak{S}_n, \circ) .

$$A = \{\tau_{i,j} \mid (i, j) \in \llbracket 1, n \rrbracket^2\}; \quad B = \{\tau_{i,i+1} \mid i \in \llbracket 1, n \rrbracket\};$$

$$C = \{\tau_{1,2}, r\} \text{ où } r \text{ est la permutation circulaire notée } \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}.$$

$\mathfrak{S}_n = \text{gr}(A)$ est un théorème vu en MPSI.

$\mathfrak{S}_n = \text{gr}(C)$ peut se déduire de $\mathfrak{S}_n = \text{gr}(B)$. Il suffit de vérifier que :

$$\tau_{i+1,i+2} = r^i \circ \tau_{1,2} \circ r^{-i}, \text{ car } r^i = \begin{pmatrix} 1 & 2 & \dots & (n-i) & (n-i+1) & \dots & n \\ i+1 & i+2 & \dots & n & 1 & \dots & i \end{pmatrix}.$$

Montrons que $\mathfrak{S}_n = \text{gr}(B)$. Comme $\mathfrak{S}_n = \text{gr}(A)$, il suffit de montrer que si $i < j$, $\tau_{i,j}$ est produit d'éléments de B , puisque $\tau_{k,\ell}^{-1} = \tau_{k,\ell}$.

La permutation $\sigma = \tau_{j-1,j} \circ \tau_{j-2,j} \circ \dots \circ \tau_{i+1,i+2} \circ \tau_{i,i+1}$ est élément de \mathfrak{S}_n . On a $\sigma(i) = j$ mais $\sigma(i+1) = i$, $\sigma(i+2) = i+1, \dots, \sigma(j-1) = j$. On vérifie aisément que $\tau_{i,j} = \tau_{i,i+1} \circ \tau_{i+1,i+2} \circ \dots \circ \tau_{j-2,j-1} \circ \sigma$.

4.4. Définition

Un groupe est dit **monogène** s'il admet une partie génératrice réduite à un élément. Un groupe monogène fini est appelé **groupe cyclique**.

4.5. Définition

Soit (G, \cdot) un groupe d'élément neutre e . On appelle **ordre** d'un élément x de G , s'il existe, le plus petit entier positif non nul n tel que $x^n = e$. Si un tel entier n'existe pas, on dit que l'élément x est d'ordre infini.

4.6. Théorème

Soit (G, \cdot) un groupe et x un élément de G d'ordre n . Alors tout entier naturel k non nul tel que $x^k = e$ est divisible par n .

Démonstration

Si $k \in \mathbb{N}^*$ et $x^k = e$, par division euclidienne par n , on a $k = nq + r$ avec $0 \leq r < n$. Donc $e = x^k = (x^n)^q x^r = x^r$. Comme $r < n$, par définition de n , on a $r = 0$. \square

Exemple

Dans (\mathbb{U}, \cdot) , le groupe multiplicatif des nombres complexes de module 1, les éléments $i, j, -j$ et ij sont d'ordres respectifs : 4, 3, 6 et 12.

4.7. Complément

| Soit \mathcal{R} une relation d'équivalence sur un ensemble non vide E . Si l'on note $cl(x)$ la classe d'équivalence de x ie. $\{x' \in E \mid x' \mathcal{R} x\}$, Les classes d'équivalence forment une partition de E .

Démonstration

- Pour tout $x \in E$, $cl(x) \neq \emptyset$. En effet, $x \in cl(x)$ puisque \mathcal{R} est réflexive.
- Pour tout $(x, y) \in E^2$, $cl(x) \neq cl(y) \Rightarrow cl(x) \cap cl(y) = \emptyset$.

En effet, en raisonnant par contraposition, on a puisque \mathcal{R} est symétrique : $z \in cl(x) \cap cl(y) \Rightarrow [(x \mathcal{R} z) \text{ et } (z \mathcal{R} y)] \Rightarrow x \mathcal{R} y$. D'où $cl(x) = cl(y)$.

- E est réunion des classes d'équivalence. En effet, pour tout x de E , on a : $x \in cl(x) \subset \bigcup_{y \in E} cl(y)$. L'inclusion inverse est évidente puisqu'une réunion de parties de E est incluse dans E . \square

4.8. Théorème de Lagrange

| Si G est fini, le cardinal de tout sous-groupe de (G, \cdot) divise $\text{Card}[G]$.

Démonstration

On montre que si H est un sous-groupe de G , la relation binaire définie par $x \mathcal{R} y \iff xy^{-1} \in H$ est une relation d'équivalence.

Pour $x \in G$ la classe de x modulo cette relation d'équivalence est donc :

$\mathcal{O}(x) = \{y \in G \mid y = xz, z \in H\} = xH$. Donc $\text{Card}[\mathcal{O}(x)] = \text{Card}[H]$. Comme les classes d'équivalence forment une partition de G et qu'elles ont toutes même cardinal, on a le résultat. \square

4.9. Corollaire

| Si G est fini de cardinal n , l'ordre de tout élément de G divise n . En particulier, $a^n = e$ quel que soit a élément de G .

Démonstration

Si ω est l'ordre de $a \in G$, alors $a^\omega = e$. Le groupe cyclique $\text{gr}(a)$ étant isomorphe à $\mathbb{Z}/\omega\mathbb{Z}$, son cardinal est ω et ω divise n d'après le corollaire précédent. Donc $n = \omega r$ avec $r \in \mathbb{N}$. D'où $a^n = e$. \square

5. Sous-groupes du groupe $(\mathbb{Z}, +)$

| H est un sous-groupe de $(\mathbb{Z}, +)$ si, et seulement si, il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Démonstration

Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Supposons $H \neq \{0\}$. Alors il existe $x \in H \setminus \{0\}$. Comme H est un sous-groupe de $(\mathbb{Z}, +)$, l'élément $-x$ appartient à H , donc

$|x| \in H \cap \mathbb{Z}_+^* = H'$. D'où H' est une partie non vide de \mathbb{N} . Il existe un unique $n \in \mathbb{N}^*$ tel que $n = \min_{\mathbb{N}}(H')$. Le sous-groupe de H engendré par n i.e. $(n) = n\mathbb{Z}$ est inclus dans H . Inversement, si x est un élément quelconque de H , par division euclidienne, $x = nq + r$ où $(q, r) \in \mathbb{Z}^2$ et $0 \leq r < n$. Comme $nq \in n\mathbb{Z} \subset H$ qui est sous-groupe de $(\mathbb{Z}, +)$, $r = x - nq$ est élément de H . Comme $r < n$, donc $r \notin H'$. D'où $r = 0$ et $x = nq \in n\mathbb{Z}$. L'unicité du plus petit élément strictement positif de H implique l'unicité de $a \in \mathbb{N}^*$ tel que $H = a\mathbb{Z}$ si $H \neq \{0\}$. \square

II. Morphismes de groupes

1. Définition

Si (G, T) et (G', T') sont deux groupes, une application f de G dans G' est un morphisme de groupes si, pour tout $(x, y) \in G^2$, $f(xTy) = f(x)T'f(y)$.

2. Propriétés

On conserve les notations de la définition précédente.

- L'image par f du neutre de (G, T) est le neutre de (G', T') .
- L'image par f du symétrique de $x \in G$ pour la loi T est le symétrique de $f(x) \in G'$ pour la loi T' .
- $f(G)$ est un sous-groupe de (G', T') .
- L'image réciproque de l'élément neutre e' de (G', T') , appelée le **noyau** du morphisme f et notée $\text{Ker}(f)$, est un sous-groupe de (G, T) .
- f est injective si, et seulement si, $\text{Ker}(f)$ est réduit à l'élément neutre de (G, T) .
- Si f est un **isomorphisme** de groupes i.e. si f est un morphisme bijectif de groupes, il en est de même de f^{-1} .

Démonstrations

a) Si e est l'élément neutre dans G et e' l'élément neutre dans G' , pour tout $x \in G$, $xTe = eTx = e \Rightarrow f(x)T'f(e) = f(e)T'f(x) = f(e) \Rightarrow f(e) = e'$.

b) Si $xTx' = x'Tx = e$, alors $f(x)T'f(x') = f(x')T'f(x) = f(e) = e'$. Donc $f(x')$ est le symétrique de $f(x)$ dans le groupe (G', T') .

c) On a déjà $f(e) = e' \in f(G)$. Donc $f(G)$ est non vide. Si a et b sont éléments de $f(G)$, il existe x et y dans G tels que $a = f(x)$ et $b = f(y)$. Si b' est le symétrique de b pour T' , on a vu que $b' = f(y')$ où y' est le symétrique de y dans G pour T .

Donc $aT'b' = f(x)T'f(y') = f(xTy') \in f(G)$ car (G, T) est un groupe.

Donc $f(G)$ est un sous-groupe de (G', T') .

d) $\text{Ker}(f) = f^{-1}(\{e'\}) = \{x \in G \mid f(x) = e'\}$ contient e , d'après a), donc $\text{Ker}(f)$ est non vide. Si $(x, y) \in (\text{Ker}(f))^2$ $f(xTy) = f(x)T'f(y) = e'T'e' = e'$.

Si y' est le symétrique de y dans G pour T , alors $f(y')$ est le symétrique de $f(y)$ dans G' pour T' . Donc $f(y) = e' \Rightarrow f(y') = e'$ i.e. $y' \in \text{Ker}(f)$.

Donc $\text{Ker}(f)$ est un sous-groupe de (G, \cdot) .

e) Si f est injective, $x \in \text{Ker}(f) \iff f(x) = e' \iff f(x) = f(e) \Rightarrow x = e$.

Donc, si f est injective, son noyau est réduit à $\{e\}$.

Réciproquement si $\text{Ker}(f) = \{e\}$, pour tout $x, y \in G$, $f(x) = f(y)$ implique $f(x)T'f(y') = e'$ d'après b), si y' est le symétrique de y dans G pour T . Comme

f est un morphisme, $f(xTy') = e'$ i.e. $xTy' \in \text{Ker}(f)$. Comme $\text{Ker}(f) = \{e\}$, il s'ensuit que $xTy' = e$ ce qui équivaut à $x = y$. Donc f est injective.

f) Il suffit de prouver que f^{-1} est un morphisme de groupes.

Soit $(x', y') \in G'^2$, il existe un unique couple $(x, y) \in G^2$ tel que :

$x' = f(x)$ et $y' = f(y)$ puisque f est bijective.

$f^{-1}(x')Tf^{-1}(y') = xTy = f^{-1}(f(xTy)) = f^{-1}(f(x)T'f(y))$ car f est un morphisme. Donc $f^{-1}(x')Tf^{-1}(y') = f^{-1}(x'T'y')$. \square

3. Exemples

- \ln est un isomorphisme du groupe (\mathbb{R}_+^*, \times) sur le groupe $(\mathbb{R}, +)$.
- \det est un morphisme du groupe $(\text{GL}_n(\mathbb{C}), \times)$ dans le groupe (\mathbb{C}^*, \cdot) .
- L'application $\varepsilon : \mathfrak{S}_n \rightarrow \{-1, 1\}, \sigma \mapsto \varepsilon(\sigma)$, la signature de la permutation σ , est un morphisme de groupes.

III. Groupes monogènes et cycliques

1. Congruence modulo n

1.1. Théorème et définition

Pour $n \in \mathbb{N}$ donné, la relation \mathcal{R} définie sur \mathbb{Z} par $x\mathcal{R}y$ si, et seulement si, $x - y \in n\mathbb{Z}$, est une relation d'équivalence appelée relation de congruence modulo n . On note $x\mathcal{R}y : x \equiv y \pmod{n}$.

La classe d'équivalence de x modulo n est $\bar{x} = \{y \in \mathbb{Z} \mid x \equiv y \pmod{n}\}$.

$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble quotient \mathbb{Z}/\mathcal{R} .

Démonstration

\mathcal{R} est réflexive car $0 \in n\mathbb{Z}$ puisque $(n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$) (1)

\mathcal{R} est symétrique car si $z \in n\mathbb{Z}$, alors $-z \in n\mathbb{Z}$ d'après (1).

\mathcal{R} est transitive d'après (1), car $(x - z) = (x - y) + (y - z)$.

Donc \mathcal{R} est une relation d'équivalence sur \mathbb{Z} . \square

1.2. Proposition

(x, y) appartenant à \mathbb{Z}^2 et n étant un entier naturel non nul, $x \equiv y \pmod{n}$ si, et seulement si, x et y ont même reste dans la division euclidienne par n .

Démonstration

Si $x = nq + r$ et $y = nq' + r$ avec $(q, q', r) \in \mathbb{Z}^3$, alors $x - y = n(q - q') \in n\mathbb{Z}$.

Réciproquement, si $x \equiv y \pmod{n}$, il existe $k \in \mathbb{Z}$ tel que $x - y = nk$.

Si r est le reste de la division euclidienne de y par n , alors $y = np + r$ où $0 \leq r < n$, donc $x = n(p + k) + r$. De l'unicité du couple quotient-reste dans la division euclidienne, on déduit que r est le reste de la division euclidienne de x par n . \square

1.3. Conséquence

$$\text{Si } n \geq 2, \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

En effet, les seuls restes possibles sont $0, 1, \dots, (n-1)$. Donc, si $x = nq + r$, alors $x \equiv r \pmod{n}$ i.e. $\bar{x} = \bar{r}$.

1.4. Compatibilité

Soit $n \in \mathbb{N}^*$. Si $x \equiv x' \pmod{n}$ et $y \equiv y' \pmod{n}$, alors :
 $x + y \equiv x' + y' \pmod{n}$ et $xy \equiv x'y' \pmod{n}$.

Démonstration

L'hypothèse s'écrit $(x - x' \in n\mathbb{Z}$ et $y - y' \in n\mathbb{Z})$ ou $(x = x' + nk$ et $y = y' + nk')$ avec $(k, k') \in \mathbb{Z}^2$. Donc :

$(x + y) - (x' + y') = (x - x') + (y - y') \in n\mathbb{Z}$ car $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.
 D'autre part $xy - x'y' = n(nkk' + ky' + k'x) \in n\mathbb{Z}$. \square

1.5. Conséquence

$$x \equiv y \pmod{n} \Rightarrow \forall p \in \mathbb{N}, x^p \equiv y^p \pmod{n}.$$

Exercice

Déterminer, pour $n \in \mathbb{N}$, les restes R_n de la division euclidienne de 3^n par 5.

Solution

$$3 \equiv 3 \pmod{5} \Rightarrow 3^2 \equiv 4 \pmod{5} \Rightarrow 3^3 \equiv 2 \pmod{5} \Rightarrow 3^4 \equiv 1 \pmod{5}.$$

$\forall n \in \mathbb{N}, \exists!(q, r) \in \mathbb{N}^2, n = 4q + r, 0 \leq r < 4$.

Comme $3^n = (3^4)^q 3^r$, on a : $3^n \equiv 3^r \pmod{5}$. D'où la conclusion.

Si $n \equiv 0 \pmod{4}$, alors $R_n = 1$. Si $n \equiv 1 \pmod{4}$, alors $R_n = 3$.

Si $n \equiv 2 \pmod{4}$, alors $R_n = 4$. Si $n \equiv 3 \pmod{4}$, alors $R_n = 2$.

2. Morphisme canonique

2.1. Définition

Soit $n \in \mathbb{N}$. L'application $\pi_n : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, x \mapsto \bar{x}$ est surjective. On l'appelle la surjection canonique de \mathbb{Z} sur $\mathbb{Z}/n\mathbb{Z}$.

2.2. Théorème et définition

On définit une loi de composition interne notée $+$ sur $\mathbb{Z}/n\mathbb{Z}$ en posant :

$$\bar{x} + \bar{y} = \overline{x + y}.$$

$\mathbb{Z}/n\mathbb{Z}$ est alors muni d'une structure de groupe abélien et π_n est un morphisme de groupes additifs.

Démonstration

On déduit de C.1.4. que si $\bar{x} = \bar{x}'$ et $\bar{y} = \bar{y}'$, alors $\overline{x + y} = \overline{x' + y'}$. Donc on a bien défini une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$. On a : $\pi_n(x + y) = \pi_n(x) + \pi_n(y)$.

Comme π_n est surjective et $(\mathbb{Z}, +)$ un groupe abélien, $\mathbb{Z}/n\mathbb{Z}$ est alors muni d'une structure de groupe abélien. \square

3. Groupes cycliques

3.1. Théorème

Soit G un groupe et $a \in G$. Le morphisme $k \mapsto ka$ (ou $k \mapsto a^k$) du groupe $(\mathbb{Z}, +)$ dans G a pour image le groupe monogène $gr(a)$ et pour noyau $n\mathbb{Z}$.

Si $n = 0$, $gr(a)$ est isomorphe à $(\mathbb{Z}, +)$.

Si $n \neq 0$, $gr(a)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ donc cyclique.

Démonstration

(Dans le cas où la loi sur G est multiplicative). Donc $\text{gr}(a) = \{a^k \mid k \in \mathbb{Z}\}$.

L'application $\varphi : \mathbb{Z} \rightarrow \text{gr}(a), k \mapsto a^k$ est un morphisme surjectif de groupes. $\text{Ker}(\varphi)$ étant un sous-groupe de $(\mathbb{Z}, +)$, il existe un unique $n \in \mathbb{N}$ tel que $\text{Ker}(\varphi) = n\mathbb{Z}$.

- Si $n = 0$, φ est injective, donc bijective et réalise un isomorphisme de $(\mathbb{Z}, +)$ sur $(\text{gr}(a), \cdot)$.

- Si $n > 0$, soit π_n la surjection canonique de \mathbb{Z} sur $\mathbb{Z}/n\mathbb{Z}$, montrons qu'il existe une unique $\bar{\varphi} : \mathbb{Z}/n\mathbb{Z} \rightarrow \text{gr}(a)$ telle que $\varphi = \bar{\varphi} \circ \pi_n$ et que $\bar{\varphi}$ est un isomorphisme de groupes.

Si $\bar{\varphi}$ existe, alors pour tout $k \in \mathbb{Z}, \varphi(k) = (\bar{\varphi} \circ \pi)(k) = \bar{\varphi}(\bar{k})$. Elle est donc unique.

De plus, elle est surjective puisque φ l'est. D'autre part, on a :

$$a^k = a^{k'} \iff a^{k-k'} = e \iff k - k' \in \text{Ker}(\varphi) = n\mathbb{Z} \iff \bar{k} = \bar{k}'. \quad (\star)$$

Donc, on définit bien une application $\bar{\varphi}$ de $\mathbb{Z}/n\mathbb{Z}$ dans $\text{gr}(a)$ en posant $\bar{\varphi}(\bar{k}) = a^k$.

De plus, elle est injective d'après (\star) . Elle est un isomorphisme de groupes car

$$\bar{\varphi}(\bar{k} + \bar{k}') = \varphi(k + k') = \varphi(k) \varphi(k') = a^k a^{k'} = \bar{\varphi}(\bar{k}) \bar{\varphi}(\bar{k}'). \quad \square$$

3.2. Théorème

Soit $n \in \mathbb{N}, n \geq 2$. Un élément \bar{x} est générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si, et seulement si, x et n sont premiers entre eux.

Démonstration

\bar{x} est générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si, et seulement si, il existe $y \in \mathbb{Z}$ tel que $\bar{1} = y\bar{x}$ i.e. (il existe $(y, z) \in \mathbb{Z}^2$ tel que $1 = xy + nz$), ce qui, d'après le théorème de Bézout, équivaut à $(x$ et n sont premiers entre eux). \square

3.3. Exemple

Soit $n \in \mathbb{N}^*$. L'ensemble $\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\} = \{\omega^k \mid 0 \leq k \leq n-1\}$ où $\omega = \exp\left(\frac{2i\pi}{n}\right)$ est un sous-groupe cyclique de (\mathbb{C}^*, \cdot) isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. Ses générateurs sont les $\alpha_k = \exp\left(\frac{2ik\pi}{n}\right)$ où k et n sont premiers entre eux.

IV. Anneaux

1. Définitions

1. Définition

$(A, +, \star)$ est un anneau si $(A, +)$ est un groupe abélien, la loi \star est associative et distributive par rapport à la loi $+$ et si A admet un élément neutre 1_A pour la loi \star .
Si la loi \star est commutative, l'anneau est dit commutatif.

Exemples

Si \mathbb{K} est l'un des ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, les ensembles $\mathbb{K}, \mathbb{K}[X], \mathcal{F}(A, \mathbb{K}), \mathbb{K}^{\mathbb{N}}$ sont munis d'une structure d'anneau commutatif et $\mathfrak{M}_n(\mathbb{K})$ d'une structure d'anneau non commutatif.

Si $(E, +, \cdot)$ est un \mathbb{K} espace vectoriel, $(\mathcal{L}(E), +, \circ)$ est un anneau.