COURS COMPLET ET DÉTAILLÉ DE MATHS MP & MPI

Pour avoir des connaissances solides et organiser son raisonnement

Julian Palacios

ellipses

Chapitre 1

Structures algébriques usuelles

1.1 Compléments sur les groupes

1.1.1 Intersection de sous-groupes

Proposition.
On se donne $(G, \times)$ un groupe. On se donne $(H_i, \times)_{i\in I}$ une famille de sous-groupes de G. On pose $H = \underset{i\in I}{\cap} H_i$, alors $(H, \times)$ est un sous-groupe de $(G, \times)$.

Démonstration. Déjà, pour tout $i \in I$, on a $e \in H_i$, donc $e \in H$. En particulier H est non vide. Ensuite, soient x et y deux éléments de H. Pour tout $i \in I, (H_i, \times)$ est un sous-groupe de G, donc $xy^{-1} \in H_i$. Ainsi $xy^{-1} \in H$. ■

Exemple. $(2\mathbb{Z}, +) \cap (3\mathbb{Z}, +) = (6\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$.

1.1.2 Sous-groupe engendré par une partie

Définition d'un sous-groupe engendré par une partie.

On se donne $(G, \times)$ un groupe. On se donne $A \subset G$ une partie de G. On pose

$$\langle A\rangle = \bigcap_{\substack{H \text{ sous-groupe de } G \\ \text{tel que } A\subset H}} H.$$

$\langle A\rangle$ est l'intersection de tous les sous-groupes de G contenant A. D'après la proposition précédente, $(\langle A\rangle, \times)$ est un sous-groupe de $(G, \times)$. On l'appelle le sous-groupe engendré par A. On peut aussi le noter $\mathrm{gr}(A)$.

1.1.3 Partie génératrice d'un groupe

Définition d'une partie génératrice d'un groupe.

On dit qu'une partie S d'un groupe $(G, \times)$ est une partie génératrice si

$$\langle S \rangle = G.$$

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

Théorème.
Tout sous-groupe additif de $(\mathbb{Z}, +)$ est de la forme $(n\mathbb{Z}, +)$, avec $n \in \mathbb{N}$.

Démonstration. Soit $(G, +)$ un sous-groupe de $(\mathbb{Z}, +)$. Si $G = \{0\}$, alors $n = 0$ convient. Supposons maintenant que $G \neq \{0\}$. Soit $g \in G$, $g \neq 0$,

- si $g > 0$, alors $g \in G \cap \mathbb{N}^*$,
- si $g < 0$, alors $-g \in G \cap \mathbb{N}^*$,

dans tous les cas on a $G \cap \mathbb{N}^* \neq \emptyset$. L'ensemble $G \cap \mathbb{N}^*$ admet un plus petit élément. On le note n. Montrons que $G = n\mathbb{Z}$. On procède par double inclusion. Soit $x \in n\mathbb{Z}$, il existe $q \in \mathbb{Z}$ tel que $x = nq$. Comme $n \in G$ et que $(G, +)$ est un sous-groupe de $(\mathbb{Z}, +)$, on en déduit que $nq \in G$. On a montré l'inclusion $n\mathbb{Z} \subset G$.
Soit $g \in G$. On effectue la division euclidienne de g par n,

$$\exists q \in \mathbb{Z}, \quad \exists r \in \mathbb{Z}, \quad 0 \leqslant r < n, \quad \text{tels que} \quad g = nq + r.$$

On a $n \in G$ donc $nq \in G$, ainsi $r = g - nq \in G$. Or $0 \leqslant r < n$, si $r \neq 0$, cela contredit le fait que $n = \min(G \cap \mathbb{N}^*)$. Donc $r = 0$. On obtient alors que $g = nq$, et on a montré que $G \subset n\mathbb{Z}$. Finalement on a $G = n\mathbb{Z}$. ■

1.1.5 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

A. **Une relation d'équivalence sur $\mathbb{Z}$**
On définit sur $\mathbb{Z}$ la relation d'équivalence suivante :

$$\forall (a, b) \in \mathbb{Z}^2, \quad a \sim b \quad \Leftrightarrow \quad a \equiv b[n].$$

Cette relation est bien

- Réflexive :

$$\begin{aligned} & a - a = 0 \\ \text{donc} \quad & n | (a - a) \\ \text{ainsi} \quad & a \equiv a[n] \\ & a \sim a. \end{aligned}$$

- Symétrique :

$$\begin{aligned} a \sim b &\Leftrightarrow a \equiv b[n] \\ &\Leftrightarrow n|(a-b) \\ &\Leftrightarrow \exists k \in \mathbb{Z}, \quad a-b = kn \\ &\Leftrightarrow \exists k \in \mathbb{Z}, \quad b-a = (-k)n \\ &\Leftrightarrow n|b-a \\ &\Leftrightarrow b \equiv a[n] \\ &\Leftrightarrow b \sim a. \end{aligned}$$

- Transitive :

$$\begin{gathered} a \sim b \quad \text{et} \quad b \sim c \\ a \equiv b[n] \quad \text{et} \quad b \equiv c[n] \\ \exists k \in \mathbb{Z}, \quad a-b = kn \quad \text{et} \quad \exists \ell \in \mathbb{Z}, \quad b-c = \ell n \\ a-c = a-b+b-c = kn+\ell n = (k+\ell)n \\ a \equiv c[n] \\ a \sim c. \end{gathered}$$

B. **L'ensemble $\mathbb{Z}/n\mathbb{Z}$.**
Les classes d'équivalence
Proposition.
Pour $n \in \mathbb{N}^*$ fixé, les classes d'équivalence sont : $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Démonstration. Montrons déjà qu'elles sont toutes distinctes. Soient $i, j \in [\![0\,, n-1]\!]$, supposons que $\overline{i} = \overline{j}$. On a

$$\begin{aligned} 0 \leqslant & i \leqslant n-1 \\ 0 \leqslant & j \leqslant n-1 \\ 1-n \leqslant & -j \leqslant 0 \\ 1-n \leqslant & i-j \leqslant n-1. \end{aligned}$$

Or $\overline{i} = \overline{j}$, donc il existe $k \in \mathbb{Z}$ tel que $i-j = kn$. La seule possibilité est que $k = 0$. Donc $i = j$. On a montré que si $i, j \in [\![0, n-1]\!]$ vérifient $\overline{i} = \overline{j}$, alors $i = j$, ou encore, la contraposée

$$\forall i, j \in [\![0, n-1]\!], \quad i \neq j \;\Rightarrow\; \overline{i} \neq \overline{j}.$$

Les classes d'équivalence sont toutes distinctes. Montrons maintenant qu'il n'y en a pas d'autre. Soit $a \in \mathbb{Z}$. On effectue la division euclidienne de a par n, cela donne

$$\exists q \in \mathbb{Z}, \quad \exists r \in \mathbb{N}, \quad 0 \leqslant r \leqslant n-1, \quad \text{tels que} \quad a = nq + r.$$

Donc $\overline{a} = \overline{r}$. On a montré que tout élément de $\mathbb{Z}$ possède une classe d'équivalence dans $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. ■

Définition de $\mathbb{Z}/n\mathbb{Z}$.

On pose $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. En particulier $\text{Card}(\mathbb{Z}/n\mathbb{Z}) = n$.

C. **Structure de groupe additif sur $\mathbb{Z}/n\mathbb{Z}$**

Définition de l'addition sur $\mathbb{Z}/n\mathbb{Z}$.

On pose pour tout $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$, $\quad \overline{a} + \overline{b} = \overline{a+b}$.

Proposition.
Montrons que cette définition est licite, c'est-à-dire indépendante des représentants de a et b.

Démonstration. Soit $a_1 \in \mathbb{Z}$ tel que $\overline{a} = \overline{a_1}$ et soit $b_1 \in \mathbb{Z}$ tel que $\overline{b} = \overline{b_1}$. Alors il existe $k \in \mathbb{Z}$ tel que $a - a_1 = kn$ et il existe $\ell \in \mathbb{Z}$ tel que $b - b_1 = \ell n$. Ainsi $(a+b) - (a_1 + b_1) = (k+\ell)n$, donc $\overline{a+b} = \overline{a_1 + b_1}$. L'addition est bien définie. ■

Proposition.
$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

Démonstration. L'ensemble est non vide, car $\overline{0} \in \mathbb{Z}/n\mathbb{Z}$. Montrons la commutativité en utilisant la commutativité dans $\mathbb{Z}$

$$\forall a, b \in \mathbb{Z}, \quad \overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}.$$

Montrons que l'élément neutre est $\overline{0}$

$$\forall a \in \mathbb{Z}, \quad \overline{a} + \overline{0} = \overline{a+0} = \overline{a}.$$

Puis montrons l'associativité en utilisant l'associativité dans $\mathbb{Z}$

$$\begin{aligned} \forall a, b, c \in \mathbb{Z}, \quad (\overline{a} + \overline{b}) + \overline{c} &= \overline{a+b} + \overline{c} \\ &= \overline{(a+b)+c} \\ &= \overline{a + (b+c)} \\ &= \overline{a} + \overline{b+c} \\ &= \overline{a} + (\overline{b} + \overline{c}). \end{aligned}$$

Enfin, montrons que tout élément possède un inverse.

$$\forall a \in \mathbb{Z}, \quad \overline{a} + \overline{-a} = \overline{a-a} = \overline{0}.$$

l'inverse de $\overline{a}$ est $\overline{-a}$. ■

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

Théorème.

$$\mathbb{Z}/n\mathbb{Z} = \langle \overline{k} \rangle \quad \Leftrightarrow \quad k \wedge n = 1.$$

Démonstration. Supposons que $\mathbb{Z}/n\mathbb{Z} = \langle \overline{k} \rangle$, alors $\overline{1} \in \langle \overline{k} \rangle$, ainsi

$$\begin{aligned} \exists \ell \in \mathbb{Z}, \quad \overline{1} &= \ell \overline{k} \\ \overline{1} &= \overline{\ell k} \\ \exists a \in \mathbb{Z}, \quad 1 - \ell k &= an \\ an + \ell k &= 1 \\ n \wedge k &= 1. \end{aligned}$$

Inversement, soit $k \in \mathbb{Z}$ tel que $n \wedge k = 1$. On a déjà $\langle \overline{k} \rangle \subset \mathbb{Z}/n\mathbb{Z}$. Ensuite, d'après la relation de Bézout

$$\begin{aligned} \exists (a, b) \in \mathbb{Z}^2, \quad an + bk &= 1 \\ bk &= 1 - an \\ \overline{bk} &= \overline{1}. \end{aligned}$$

Soit $\overline{u} \in \mathbb{Z}/n\mathbb{Z}, \overline{u} = u \times \overline{1} = u \times \overline{bk} = u \times b \times \overline{k}$. Donc $\overline{u} \in \langle \overline{k} \rangle$, on a montré que $\mathbb{Z}/n\mathbb{Z} \subset \langle \overline{k} \rangle$. Par double inclusion on a finalement que $\mathbb{Z}/n\mathbb{Z} = \langle \overline{k} \rangle$. ■

Exercice.
Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation suivante

$$x^2 + x + 3 = 0.$$

Réponse. Attention, on est dans $\mathbb{Z}/5\mathbb{Z}$ et pas dans $\mathbb{R}$, donc se dire qu'il s'agit d'une équation du second degré et que le discriminant est négatif, par conséquent il n'y a pas de solution est fausse.
Dans $\mathbb{Z}/5\mathbb{Z}$ il n'y a que cinq éléments : $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, on les teste un par un et on trouve ainsi les solutions.

- Pour $x = 0$, on a $x^2 + x + 3 = 3 \neq 0[5]$, donc $x = 0$ n'est pas solution.
- Pour $x = 1$, on a $x^2 + x + 3 = 5 = 0[5]$, donc $x = 1$ est une solution.
- Pour $x = 2$, on a $x^2 + x + 3 = 4 + 2 + 3 = 9 = 4 \neq 0[5]$, donc $x = 2$ n'est pas une solution.
- Pour $x = 3$, on a $x^2 + x + 3 = 9 + 3 + 3 = 15 = 0[5]$, donc $x = 3$ est une solution.
- Pour $x = 4$, on a $x^2 + x + 3 = 16 + 4 + 3 = 23 = 3 \neq 0[5]$, donc $x = 4$ n'est pas une solution.

Conclusion, les solutions de cette équation sont $S = \{\overline{1}, \overline{3}\}$.
Une autre méthode sera proposée au 1.4.3.

1.1.7 Groupe monogène, groupe cyclique

Définition d'un groupe monogène.

$(G, \times)$ est un groupe monogène s'il existe $a \in G$ tel que $G = \langle a \rangle$. C'est-à-dire

$$G = \{a^k, k \in \mathbb{Z}\}.$$

Définition d'un groupe cyclique.

$(G, \times)$ est un groupe cyclique s'il est fini et monogène.

1.1.8 Le groupe des racines n-ièmes de l'unité

Proposition.
Le groupe des racines n-ièmes de l'unité est un groupe cyclique. $\mathbb{U}_n = \langle e^{\frac{2i\pi}{n}} \rangle$.

1.1.9 Groupe monogène infini

Proposition.
Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.

Démonstration. Soit $(G, \times)$, un groupe monogène infini. Soit a un générateur de G. Ainsi $G = \langle a \rangle$. On considère l'application

$$\begin{aligned} \varphi : \mathbb{Z} &\to G \\ n &\mapsto a^n. \end{aligned}$$

Montrons que φ est un isomorphisme du groupe $(\mathbb{Z}, +)$ vers le groupe $(G, \times)$. On commence par montrer que φ est un morphisme, en effet, on a

$$\varphi(n + m) = a^{n+m} = a^n \times a^m = \varphi(n) \times \varphi(m).$$

Comme $G = \langle a \rangle$, on sait que $\mathrm{Im}(\varphi) = G$, c'est-à-dire que φ est surjective. Enfin, on recherche le noyau de φ. Supposons par l'absurde que $\ker(\varphi) \neq \{0\}$. Alors il existe $n \neq 0$ tel que $a^n = e$. Si $n < 0$, on peut écrire $e^{-1} = (a^n)^{-1}$ ou encore $e = a^{-n}$. Que n soit positif ou négatif, il existe $m \in \mathbb{N}^*$ tel que $a^m = e$, dans ce cas montrons que $G = \{e, a, a^2, \ldots, a^{m-1}\}$. On procède par double inclusion. On pose $H = \{e, a, a^2, \ldots, a^{m-1}\}$. Déjà $H \subset G$. Inversement, soit $x \in G$. Comme $G = \langle a \rangle$, il existe $k \in \mathbb{Z}$ tel que $x = a^k$. On effectue la division euclidienne de k par m

$$\exists q \in \mathbb{Z}, \quad \exists r \in \mathbb{N}, \quad 0 \leqslant r \leqslant m - 1, \quad \text{tels que} \quad k = qm + r.$$

Alors $x = a^k = (a^m)^q a^r = a^r \in H$. Ainsi $G = H$. Or H est de cardinal fini et G est infini, c'est impossible. Par conséquent $\ker(\varphi) = \{0\}$. On peut conclure que l'application φ est injective et surjective, c'est un isomorphisme. G est isomorphe à $\mathbb{Z}$. ■

1.1.10 Groupe monogène fini

Proposition.
Tout groupe monogène fini de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Ce résultat justifie qu'un groupe monogène fini soit également appelé un groupe cyclique.

Démonstration. Comme G est un groupe monogène, il existe $a \in G$ tel que $G = \langle a \rangle$. Supposons par l'absurde que pour tout $m \in \mathbb{N}^*$ on ait $a^m \neq e$, on va démontrer qu'alors pour tout $k, \ell \in \mathbb{N}^*$, avec $k \neq \ell$ on aurait $a^k \neq a^\ell$. Supposons qu'il existe k et $\ell \in \mathbb{N}^*$ tels que $k > \ell$ et $a^k = a^\ell$ alors $a^{k-\ell} = e$, ce qui est en contradiction avec l'affirmation que pour tout $m \in \mathbb{N}^*$ on ait $a^m \neq e$. Ainsi G admettrait une infinité d'éléments. Ce qui contredit le fait que G soit fini. En résumé, si G est monogène et fini il existe $k \in \mathbb{N}^*$ tel que $a^k = e$. Soit m le plus petit entier strictement positif tel que $a^m = e$. Montrons que $m = n$. On pose $H = \{e, a, a^2, \ldots, a^{m-1}\}$. On commence par montrer que tous les éléments de H sont distincts. Supposons qu'il existe k et $\ell \in [\![0, m-1]\!]$ tel que $k > \ell$ et $a^k = a^\ell$, alors $a^{k-\ell} = e$. Or $0 < k - \ell < m$, ce qui est en contradiction avec la définition de m. Donc tous les éléments de H sont distincts et il contient m éléments. Montrons maintenant que $H = G$. On procède par double inclusion. Déjà $H \subset G$. Inversement, soit $x \in G$, comme $G = \langle a \rangle$, il existe $k \in \mathbb{Z}$ tel que $x = a^k$. On effectue la division euclidienne de k par m,

$$\exists q \in \mathbb{Z}, \quad \exists r \in \mathbb{N}, \quad 0 \leqslant r < m \quad \text{tels que} \quad k = mq + r.$$

Alors $x = a^k = a^{qm+r} = (a^m)^q a^r = e^q a^r = a^r \in H$. On peut conclure que $G = H$. Comme G est de cardinal n, on en déduit que $m = n$ et que $G = \{e, a, \ldots, a^{n-1}\}$. Il reste à montrer que $(G, \times)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. On considère l'application

$$\begin{aligned} \varphi : \mathbb{Z}/n\mathbb{Z} &\to G \\ \bar{k} &\mapsto a^k. \end{aligned}$$

On commence par montrer que φ est bien définie. Si $\bar{k} = \bar{\ell}$, alors il existe $t \in \mathbb{Z}$ tel que $k = \ell + tn$. Alors $a^k = a^{\ell+tn} = a^\ell a^{tn} = a^\ell (a^n)^t = a^\ell e^t = a^\ell$. On a bien $\varphi(\bar{k}) = \varphi(\bar{\ell})$. Montrons que φ est un morphisme de groupes.

$$\varphi(\bar{k} + \bar{\ell}) = \varphi\left(\overline{k + \ell}\right) = a^{k+\ell} = a^k a^\ell = \varphi(\bar{k})\varphi(\bar{\ell}).$$

Montrons que l'application φ est surjective : soit $x \in G$. Il existe $k \in [\![0, n-1]\!]$ tel que $x = a^k$, donc $x = \varphi(\bar{k})$. Montrons que φ est injective. Soit $k \in [\![0, n-1]\!]$ tel que $\varphi(\bar{k}) = e$. On a $a^k = e$. Par définition de n (le plus petit entier m strictement positif pour lequel $a^m = e$), on en déduit que $k = 0$, donc $\bar{k} = \bar{0}$. Conclusion φ est un isomorphisme. Par conséquent

$$(\mathbb{Z}/n\mathbb{Z}, +) \simeq (G, \times).$$

■

1.1.11 Ordre d'un élément d'un groupe

Définition de l'ordre d'un élément d'un groupe.

On se donne $(G, \times)$ un groupe. On note e son élément neutre. On se donne $x \in G$.

- On dit que x est d'ordre infini si pour tout $n \in \mathbb{N}^*, x^n \neq e$.
- On dit que x est d'ordre fini s'il existe $n \in \mathbb{N}^*$ tel que $x^n = e$, dans ce cas on définit l'ordre de x par

$$\text{ordre de } x = \min\{n \in \mathbb{N}^*, \quad x^n = e\}.$$

Proposition.

$$\text{ordre de } x = \text{Card}(\langle x \rangle).$$

Démonstration. On note n l'ordre de x. Comme on l'a vu $\langle x \rangle = \{e, x, \ldots, x^{n-1}\}$. Donc l'ordre de x est égal au cardinal du groupe engendré par x. ■

1.1.12 Élément d'ordre fini

Proposition.
On se donne $(G, \times)$ un groupe. Si x est un élément d'ordre fini d et si e désigne le neutre de G, alors

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

Démonstration. Supposons que $x^n = e$. On effectue la division euclidienne de n par d,

$$\exists q \in \mathbb{Z}, \quad \exists r \in \mathbb{N}, \quad 0 \leqslant r < d \quad n = qd + r.$$

Alors $x^n = x^{qd+r} = (x^d)^q x^r = e^q x^r = x^r$, ainsi $x^r = e$, donc $r = 0$, soit $d|n$.
Supposons maintenant que $d|n$, alors il existe $q \in \mathbb{Z}$ tel que $n = qd$, on a alors $x^n = x^{qd} = (x^d)^q = e^q = e$. ■

1.1.13 Groupe fini

Exemples.

- Le groupe $(\mathbb{Z}/4\mathbb{Z}, +)$ est un groupe fini commutatif.
- On note $(S_3, \circ)$ le groupe des permutations de l'ensemble $\{1, 2, 3\}$. Alors $(S_3, \circ)$ est un groupe fini non commutatif. Il est constitué des éléments suivants : $\{id, (12), (13), (23), (123), (132)\}$, il a donc $6 = 3!$ éléments et il n'est pas commutatif car $(12)(13) = (132)$ et $(13)(12) = (123)$ sont différents.

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