Mathématiques
MP/MP*

PRÉPAS SCIENCES

collection dirigée par Bertrand Hauchecorne

Mathématiques MP/MP*

3e édition actualisée

ouvrage coordonné par

Ivan GOZARD

Professeur au lycée Carnot (Dijon)

Michel GOUMI

Professeur au lycée E. Perrier (Tulle)

Bertrand HAUCHECORNE

Professeur au lycée Pothier (Orléans)

Olivier LEUCK

Professeur au lycée R. Follereau (Belfort)

ellipses

COLLECTION
PRÉPAS SCIENCES

Retrouvez tous les titres de la collection et des extraits sur www.editions-ellipses.fr

Les macros de cet ouvrage ont été réalisées par Nicolas Nguyen.

ISBN 9782340-019256

32, rue Bargue 75740 Paris cedex 15

www.editions-ellipses.fr

Avant-propos

Réussir en classes préparatoires nécessite d'assimiler rapidement un grand nombre de connaissances, mais surtout de savoir les utiliser, à bon escient, et les rendre opérationnelles au moment opportun. Bien sûr, l'apprentissage du cours de votre professeur jour après jour est indispensable. Cependant, on constate que pour beaucoup, c'est loin d'être suffisant. Combien d'entre vous ont bien appris leur cours et pourtant se trouvent démunis lors d'un DS, et plus grave, le jour du concours.

Cette collection a été conçue pour répondre à cette difficulté. Suivant scrupuleusement le programme, chaque ouvrage est scindé en chapitres, dont chacun correspond, en gros, à une semaine de cours. Leur structure est identique pour chaque niveau, en mathématiques comme en physique ou chimie.

Le résumé de cours est là pour vous remettre en mémoire tous les résultats à connaître. Sa relecture est indispensable avant un DS, le passage d'une colle relative au thème traité et lors des révisions précédant les concours. Ils sont énoncés sans démonstration.

La partie « méthodes » vous initie aux techniques utiles pour résoudre les exercices classiques. Complément indispensable du cours, elle l'éclaire et l'illustre.

La partie « vrai/faux » vous permet de tester votre recul par rapport au programme et de remédier à quelques mauvais réflexes. Son corrigé est l'occasion de mettre en garde contre des **erreurs classiques**.

Les exercices sont incontournables pour assimiler le programme et pour répondre aux exigences du concours. Des **indications**, que les meilleurs pourront ignorer, permettront de répondre aux besoins de chacun, selon son niveau. Les **corrigés** sont rédigés avec soin et de manière exhaustive.

Ainsi l'ouvrage de maths comme ceux de physique et de chimie vous accompagneront tout au long de l'année et vous guideront dans votre cheminement vers **la réussite aux concours**.

Bertrand Hauchecorne

Sommaire

Chapitre 1
Groupes

Le professeur de mathématiques de Niels **Abel** détecte ses aptitudes exceptionnelles et récolte des fonds pour permettre à son élève de suivre des cours à l'université d'Oslo. Le jeune prodige obtient alors une bourse d'études qu'il utilise pour rencontrer les plus grands mathématiciens de l'époque en Allemagne et en France. Atteint de tuberculose, il rentre en Norvège sans le sou. C'est au surlendemain de sa mort, à 27 ans, qu'arrive la lettre annonçant sa nomination à l'université de Berlin. Abel démontre que l'équation du cinquième degré ne peut se résoudre par radicaux, c'est-à-dire qu'il n'existe pas de formule, comme pour le degré 2, donnant les solutions à l'aide des coefficients. Ce résultat sera affiné par Évariste **Galois**. Il introduit une classe importante de fonctions appelées intégrales elliptiques. C'est en son honneur que les groupes commutatifs sont aussi appelés abéliens.

Niels Abel
1802-1829

■■ Objectifs

■ Les incontournables

▷ Connaître les propriétés des groupes

▷ Savoir prouver qu'une partie d'un groupe en est un sous-groupe

▷ Savoir calculer modulo un entier fixé

▷ Savoir reconnaître et classifier les groupes monogènes

▷ Savoir déterminer l'ordre d'un élément d'un groupe.

■ Et plus si affinités...

▷ S'intéresser aux groupes classiques

▷ Utiliser des notions de théorie des groupes pour prouver des résultats en algèbre, en géométrie, etc.

■■ Résumé de cours

■ Structure de groupe

Définition : *Un **groupe** est un ensemble G muni d'une loi de composition interne notée $*$ vérifiant les propriétés suivantes :*

– La loi $*$ est associative, c'est-à-dire que : pour tous $a, b, c \in G$, on a : $a * (b * c) = (a * b) * c$.

– Elle est munie d'un élément neutre $e \in G$, c'est-à-dire qu'il existe un élément e qui vérifie : $a * e = e * a$ pour tout $a \in G$.

– Tout élément $x \in G$ possède un symétrique, c'est-à-dire qu'il existe $x' \in G$ tel que :

$$x * x' = x' * x = e.$$

Théorème 1.1.— Groupe produit —. Étant donnés deux groupes $(G_1, *)$ et (G_2, Δ), on définit sur le produit cartésien $G = G_1 \times G_2$ l'opération : $(x_1, x_2)\Upsilon(y_1, y_2) = (x_1 * y_1, x_2 \Delta y_2)$.
L'opération Υ définit sur G une structure de groupe.
Par récurrence, on définit, plus généralement, le groupe produit d'une famille finie de groupes.

Définition : *Une partie H du groupe $(G, *)$ est un **sous-groupe** de G lorsqu'elle vérifie les assertions suivantes :*

i) H n'est pas vide ;

ii) H est stable pour $*$, c'est-à-dire : $\forall (x, y) \in H^2$, $x * y$ appartient à H ;

iii) le symétrique de tout élément de H est un élément de H.

Proposition 1.2.— H est un sous-groupe de G si, et seulement si, H contient l'élément neutre e et pour tout $(a, b) \in H \times H$, $a * b^{-1}$ appartient à H.

Remarque : Si H est un sous-groupe de G, alors la loi induite par $*$ sur H est une loi de composition interne, et H, muni de cette loi, est un groupe.

Lemme 1.3.— Toute intersection de sous-groupes de G est un sous-groupe de G.

Théorème-Définition 1.4.— Soit A une partie du groupe G. L'intersection de tous les sous-groupes de G contenant A est un sous-groupe. C'est le plus petit sous-groupe de G contenant A. Ce groupe s'appelle le ***sous-groupe engendré*** par A.

Définition : *Une partie X du groupe G est une partie génératrice lorsque le sous-groupe engendré par X est égal à G.*

Exemple : Soit E un espace euclidien. L'ensemble des réflexions est une partie génératrice du groupe orthogonal $O(E)$.

Théorème 1.5.— Sous-groupes de $\mathbb{Z}$ —. Les sous-groupes de $(\mathbb{Z}, +)$ sont les ensembles $n\mathbb{Z}$ pour $n \in \mathbb{Z}$.

■ Morphismes de groupes

Définition : *Soit $(G,*)$ et (G',Δ) deux groupes. On appelle* ***morphisme de groupes*** *de $(G,*)$ dans (G',Δ) une application f de G dans G' qui vérifie :*

$$\forall (a,b)\in G^2,\ f(a*b)=f(a)\Delta f(b).$$

Proposition 1.6.— Soit f un morphisme de groupes de $(G,*)$ dans (G',Δ).
a) Si H est un sous-groupe de G, $f(H)$ est un sous-groupe de G'. Si H' est un sous-groupe de G', $f^{-1}(H')=\{x\in G\ /\ f(x)\in H'\}$ est un sous-groupe de G.
b) $f(G)$ est un sous-groupe de G, appelé image de f et noté $\mathrm{Im}\ f$.
$f^{-1}(\{e'\})=\{x\in G\ /\ f(x)=e'\}$ est un sous-groupe de G, appelé ***noyau*** de f et noté $\mathsf{Ker}\, f$.
c) f est surjectif si, et seulement si, $\mathsf{Im}\, f=G'$. f est injectif si, et seulement si, $\mathsf{Ker}\, f=\{e\}$.

Définition : *On appelle* ***isomorphisme de groupes*** *de $(G_1,*_1)$ sur $(G_2,*_2)$ un morphisme de groupes bijectif.*

Proposition 1.7.— Si f est un isomorphisme de groupes de $(G_1,*_1)$ sur $(G_2,*_2)$, sa bijection réciproque f^{-1} est un isomorphisme de groupes de $(G_2,*_2)$ sur $(G_1,*_1)$.

■ Groupe $\mathbb{Z}/n\mathbb{Z}$

Définition : Congruence modulo n **—.** *Fixons un entier $n\in\mathbb{N}$; les entiers $a\in\mathbb{Z}$ et $b\in\mathbb{Z}$ sont dits congrus modulo n lorsque $b-a\in n\mathbb{Z}$. On note alors $a\mathcal{R}_n b$.*

Proposition 1.8.— La relation $\mathcal{R}_n$ de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Notation : *Dans la suite, $\bar{k}$ désigne la classe d'équivalence de $k\in\mathbb{Z}$.*
On a donc : $\bar{0}=n\mathbb{Z}$, $\bar{1}=\{\dots,1-2n,1-n,1,n+1,2n+1\dots\}$, etc.
L'ensemble dont les éléments sont les classes d'équivalence selon $\mathcal{R}_n$ se note $\mathbb{Z}/n\mathbb{Z}$.

Proposition 1.9.— Pour $n\in\mathbb{N}^*$ fixé, $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini de cardinal n :

$$\boxed{\mathbb{Z}/n\mathbb{Z}=\{\bar{0},\bar{1},\dots,\overline{n-1}\}\ .}$$

Lemme 1.10.— Soit $(a,a',b,b')\in\mathbb{Z}^4$ avec $a\ \mathcal{R}_n\ a'$ et $b\ \mathcal{R}_n\ b'$, alors $a+b\ \mathcal{R}_n\ a'+b'$. On dit que la relation $\mathcal{R}_n$ est *compatible* avec l'addition. On peut donc définir sur $\mathbb{Z}/n\mathbb{Z}$ l'opération :

$$u+v=\overline{a+b},\ \text{où } u=\bar{a} \text{ et } v=\bar{b}\ .$$

L'élément de $\mathbb{Z}/n\mathbb{Z}$ ainsi défini ne dépend pas des représentants choisis.

Théorème 1.11.— Muni de l'addition ainsi définie, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un groupe commutatif. L'application $\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}, z\mapsto\bar{z}$ est un morphisme de groupes surjectif. On l'appelle le morphisme canonique, ou la surjection canonique, de $\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$.

Groupe engendré par un élément

Notation : *En général, la loi du groupe G est noté multiplicativement et sans symbole : $ab = a * b$; l'élément neutre se note e ou 1_G, le symétrique d'un élément x est noté x^{-1}.*

Lemme 1.12.— Soit $(G, .)$ un groupe et $a \in G$. Le sous-groupe engendré par a est :

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

Définition : *Un groupe G est dit* **monogène** *lorsqu'il est engendré par un seul élément. Tout élément qui l'engendre s'appelle un générateur.*

Définition : *Un groupe* **cyclique** *est un groupe monogène fini, c'est-à-dire fini et engendré par un seul élément. Tout élément qui l'engendre s'appelle un générateur.*

Exemple : Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique engendré par $\bar{1}$ car $\bar{k} = k\ 1 = 1 + 1 + \ldots + 1$ (k fois). Plus généralement :

Théorème 1.13.— Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{k}$ avec $k \wedge n = 1$.

Théorème 1.14.— Un groupe monogène infini est isomorphe à $\mathbb{Z}$.
Un groupe cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Corollaire 1.15.— Le groupe $\mathbb{U}_n = \{e^{2ik\pi/n},\ 0 \leqslant k < n\}$ des racines n-ièmes de l'unité est engendré par $e^{2i\pi/n}$ puisque $e^{2ik\pi/n} = (e^{2i\pi/n})^k$. Il est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Ordre d'un élément d'un groupe

Définition : *Soit $(G, .)$ un groupe. On dit que l'élément x de G est* **d'ordre fini** *lorsque le cardinal du sous-groupe de G engendré par x est fini ; celui-ci est alors appelé l'ordre de l'élément x.*

Théorème 1.16.— Si x est d'ordre fini d et si e désigne le neutre de G, alors, pour n dans $\mathbb{Z}$, on a :

$$x^n = e \Longleftrightarrow d | n.$$

Théorème 1.17.— Si G est un groupe fini, alors tout élément de G est d'ordre fini, et son ordre divise Card (G).

Groupe symétrique

Définition : Groupe symétrique —. *Le groupe symétrique $\mathcal{S}_n$ est l'ensemble des bijections de l'ensemble $\{1, 2, \ldots, n\}$ dans lui-même (appelées* **permutations** *de $\{1, \ldots, n\}$), muni de la composition des applications. Le groupe symétrique $\mathcal{S}_n$ possède $n!$ éléments.*

Remarque : $\mathcal{S}_1 = \{\mathrm{id}\}$, aussi, dans la suite de ce paragraphe, on suppose que $n \geqslant 2$.

Proposition 1.18.— L'application $\epsilon : \mathcal{S}_n \to \{-1, 1\}$, $\sigma \mapsto \displaystyle\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}$ est un morphisme de groupes, appelé la ***signature***.
Son noyau $\mathsf{Ker}\,(\epsilon)$ est un sous-groupe de cardinal $n!/2$, on le note $\mathcal{A}_n$ et on l'appelle le *groupe alterné* d'indice n.

Vocabulaire : *Une transposition intervertit deux éléments et laisse fixe tous les autres.*
Plus généralement, on nomme k-cycle, ou cycle de longueur k, une bijection qui opère une permutation circulaire sur k éléments $a_1, a_2, \dots a_k$ et laisse fixe les autres. On le note $(a_1, a_2, \dots a_k)$.
Par exemple une transposition est un 2-cycle.

Proposition 1.19.— Un k-cycle est d'ordre k et a pour signature $(-1)^{k-1}$.

Théorème 1.20.— Les transpositions engendrent $\mathcal{S}_n$.

Remarque : Chaque élément de $\mathcal{S}_n \setminus \{\mathrm{id}\}$ s'écrit, de manière unique à l'ordre près des facteurs, comme composée (on dit « produit ») de cycles disjoints.