Jean-Marie Monier | Guillaume Haberer

MATHS

MP/MP*-MPI/MPI*

MÉTHODES & EXERCICES

j'intègre

6e édition

DUNOD

Couverture : création Hokus Pokus, adaptation Studio Dunod

Retrouvez nos ouvrages pour les prépas scientifiques ici

http://dunod.link/prepassc

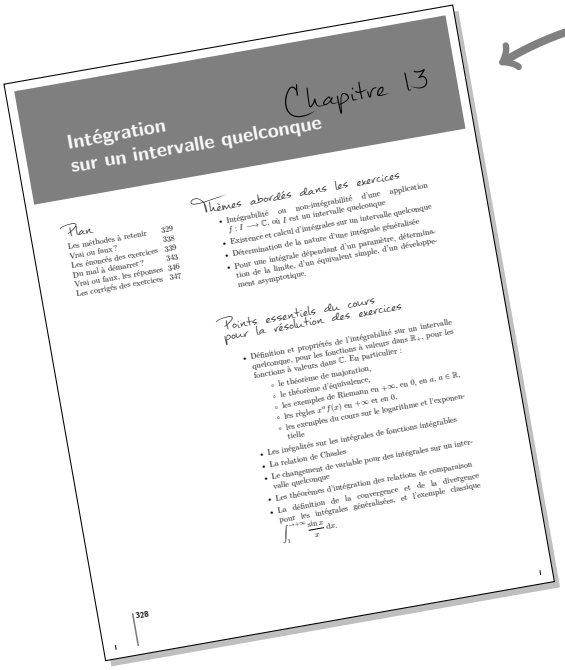
11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-088249-6

Table des matières

Compléments en ligne

Des compléments en ligne, disponibles sur la page de présentation de l'ouvrage du site de Dunod (`https://dunod.com/EAN/9782100879540`), vous donnent accès à des exercices de colles entièrement corrigés.

Pour bien utiliser cet ouvrage


Chapitre 13

Intégration sur un intervalle quelconque

Plan

Thèmes abordés dans les exercices

- Intégrabilité ou non-intégrabilité d'une application $f : I \longrightarrow \mathbb{C}$, où I est un intervalle quelconque
- Existence et calcul d'intégrales sur un intervalle quelconque
- Détermination de la nature d'une intégrale généralisée
- Pour une intégrale dépendant d'un paramètre, détermination de la limite, d'un équivalent simple, d'un développement asymptotique.

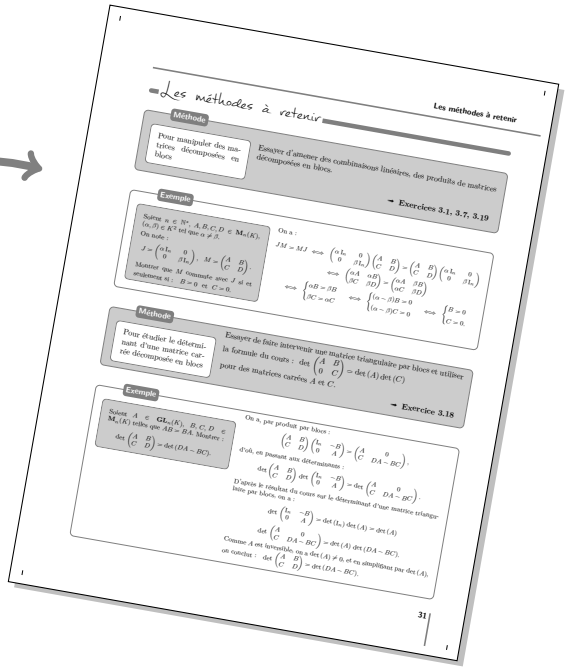
Points essentiels du cours pour la résolution des exercices

- Définition et propriétés de l'intégrabilité sur un intervalle quelconque, pour les fonctions à valeurs dans $\mathbb{R}_+$, pour les fonctions à valeurs dans $\mathbb{C}$. En particulier :
  - le théorème de majoration,
  - le théorème d'équivalence,
  - les exemples de Riemann en $+\infty$, en 0, en a, $a \in \mathbb{R}$,
  - les règles $x^\alpha f(x)$ en $+\infty$ et en 0,
  - les exemples du cours sur le logarithme et l'exponentielle
- Les inégalités sur les intégrales de fonctions intégrables
- La relation de Chasles
- Le changement de variable pour des intégrales sur un intervalle quelconque
- Les théorèmes d'intégration des relations de comparaison
- La définition de la convergence et de la divergence pour les intégrales généralisées, et l'exemple classique $\int_1^{+\infty} \frac{\sin t}{t}\,\mathrm{d}t$.

328

La page d'entrée de chapitre

Elle propose un plan du chapitre, les thèmes abordés dans les exercices, ainsi qu'un rappel des points essentiels du cours pour la résolution des exercices.


Les méthodes à retenir

Les méthodes à retenir

Méthode

Pour manipuler des matrices décomposées en blocs

Essayer d'amener des combinaisons linéaires, des produits de matrices décomposées en blocs.

Exercices 3.1, 3.7, 3.19

Exemple

Soient $n \in \mathbb{N}^*$, $A, B, C, D \in \mathbf{M}_n(K)$, $(\alpha, \beta) \in K^2$ tel que $\alpha \neq \beta$. On note :

$$J = \begin{pmatrix} \alpha I_n & 0 \\ 0 & \beta I_n \end{pmatrix}, \quad M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Montrer que M commute avec J si et seulement si : $B = 0$ et $C = 0$.

On a :

$$JM = MJ \iff \begin{pmatrix} \alpha I_n & 0 \\ 0 & \beta I_n \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} \alpha I_n & 0 \\ 0 & \beta I_n \end{pmatrix}$$

$$\iff \begin{pmatrix} \alpha A & \alpha B \\ \alpha C & \beta D \end{pmatrix} = \begin{pmatrix} \alpha A & \beta B \\ \alpha C & \beta D \end{pmatrix}$$

$$\iff \begin{cases} \alpha B = \beta B \\ \beta C = \alpha C \end{cases} \iff \begin{cases} (\alpha - \beta)B = 0 \\ (\alpha - \beta)C = 0 \end{cases} \iff \begin{cases} B = 0 \\ C = 0. \end{cases}$$

Méthode

Pour étudier le déterminant d'une matrice carrée décomposée en blocs

Essayer de faire intervenir une matrice triangulaire par blocs et utiliser la formule du cours : $\det \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \det(A)\det(C)$ pour des matrices carrées A et C.

Exercice 3.18

Exemple

Soient $A \in \mathbf{GL}_n(K)$, $B, C, D \in \mathbf{M}_n(K)$ telles que $AD = DA$. Montrer : $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(DA - BC)$.

On a, par produit par blocs :

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I_n & -B \\ 0 & A \end{pmatrix} = \begin{pmatrix} A & 0 \\ C & DA - BC \end{pmatrix},$$

d'où, en passant aux déterminants :

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} \det \begin{pmatrix} I_n & -B \\ 0 & A \end{pmatrix} = \det \begin{pmatrix} A & 0 \\ C & DA - BC \end{pmatrix}.$$

D'après le résultat du cours sur le déterminant d'une matrice triangulaire par blocs, on a :

$$\det \begin{pmatrix} I_n & -B \\ 0 & A \end{pmatrix} = \det(I_n)\det(A) = \det(A)$$

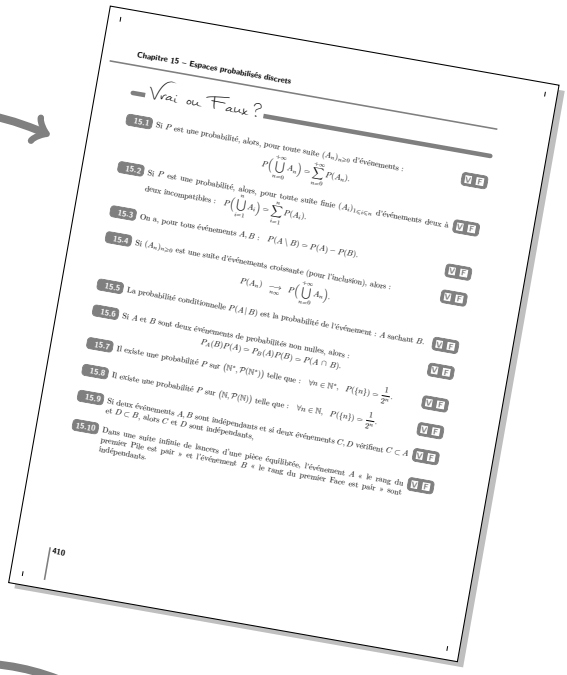
$$\det \begin{pmatrix} A & 0 \\ C & DA - BC \end{pmatrix} = \det(A)\det(DA - BC).$$

Comme A est inversible, on a $\det(A) \neq 0$, et en simplifiant par $\det(A)$, on conclut : $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(DA - BC)$.

31

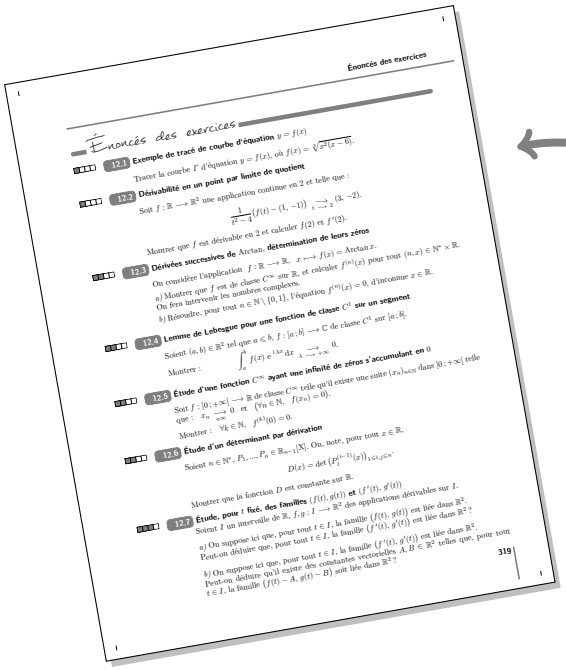
Les méthodes à retenir

Cette rubrique constitue une synthèse des principales méthodes à connaître, détaillées étape par étape, et indique les exercices auxquels elles se rapportent.
Chaque méthode est illustrée par un ou deux exemples qui la suivent.



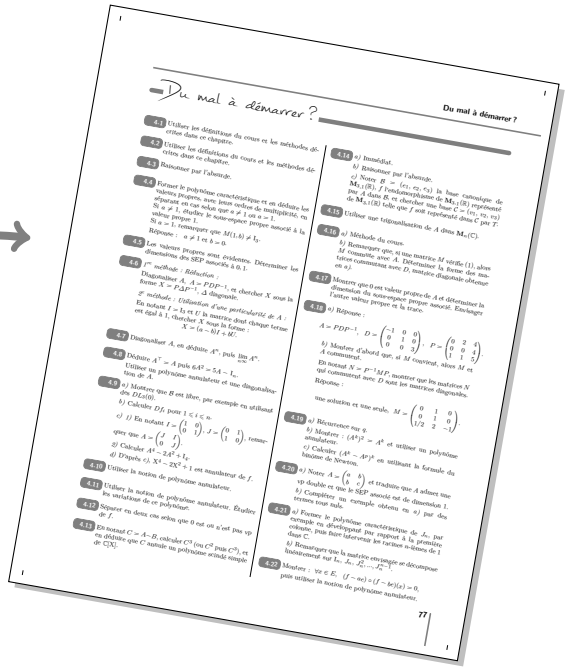
Vrai ou Faux ?

Dix questions pour vérifier la bonne compréhension du cours.



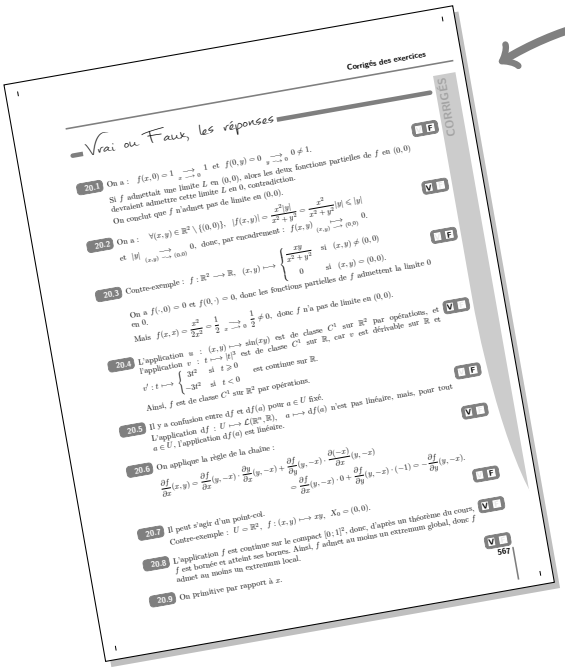
Énoncés des exercices

De nombreux exercices de difficulté croissante sont proposés pour s'entraîner. La difficulté de chaque exercice est indiquée sur une échelle de 1 à 4.



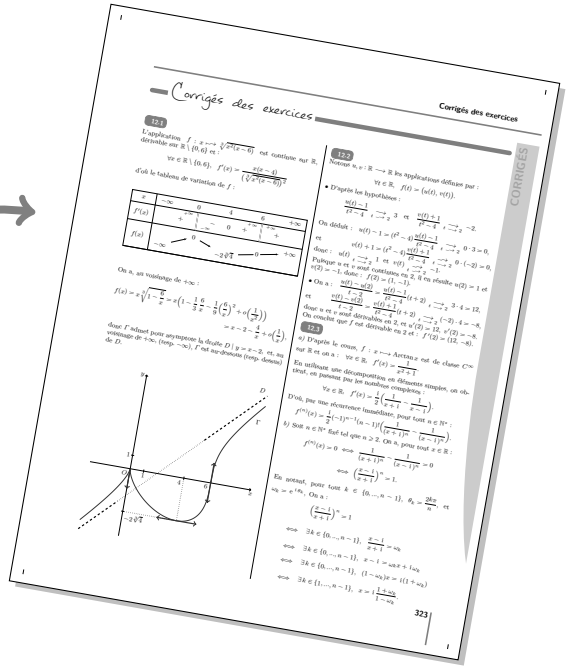
Du mal à démarrer ?

Des conseils méthodologiques sont proposés pour bien aborder la résolution des exercices.



Vrai ou Faux, les réponses

Chaque affirmation vraie est justifiée par une référence au cours ou une courte démonstration, et chaque affirmation fausse est réfutée par la production d'un contre-exemple explicite.



Corrigés des exercices

Tous les exercices sont corrigés de façon détaillée.

Remerciements

Nous tenons ici à exprimer notre gratitude aux nombreux collègues et amis qui ont accepté de réviser des parties du manuscrit :

Marc Albrecht, Bruno Arsac, Jean-Philippe Berne, Gérard Bourgin, Jean-Paul Christin, Sophie Cohéléach, Carine Courant, Sylvain Delpech, Hermin Durand, Viviane Gaggioli, Marguerite Gauthier, Cyril Haberer, Cécile Lardon, Hadrien Larôme, Paul Pichaureau, Nathalie Planche, Philippe Saadé, Marie-Dominique Siéfert, Marie-Pascale Thon, Audrey Verdier, Skander Zannad.

Groupes

Chapitre 1

Plan

Thèmes abordés dans les exercices

- Établir une structure de groupe, de sous-groupe
- Calculs dans un groupe
- Manipulation des morphismes de groupes, endomorphismes d'un groupe, isomorphismes de groupes, automorphismes d'un groupe
- Intervention de la finitude dans les groupes.

Points essentiels du cours pour la résolution des exercices

- Définition et propriétés de la structure de groupe, de sous-groupe, de sous-groupe engendré par une partie
- Produit d'un nombre fini de groupes
- Sous-groupes de $(\mathbb{Z}, +)$
- Définition et propriétés des morphismes de groupes, endomorphismes d'un groupe, isomorphismes de groupes, automorphismes d'un groupe
- Noyau, image d'un morphisme de groupes
- Définition d'un groupe monogène, d'un groupe cyclique, groupes $\mathbb{Z}/n\mathbb{Z}$, classification des groupes monogènes
- Éléments d'ordre fini dans un groupe, ordre d'un tel élément.

Les méthodes à retenir

Méthode

Pour montrer qu'un ensemble G muni d'une loi interne $\cdot$ est un groupe

Essayer de :

- revenir à la définition de la notion de groupe
- montrer que G est un sous-groupe d'un groupe connu.

Exemple

Soient X un ensemble non vide, G l'ensemble des bijections de X dans X. Montrer que G est un groupe pour la loi de composition $\circ$.

Nous allons montrer que G est un groupe pour la loi $\circ$ en revenant à la définition d'un groupe.

- On a $G \neq \varnothing$, car $\mathrm{Id}_X \in G$.
- Soient $f, g \in G$. Puisque f et g sont bijectives de X dans X, d'après le cours, par composition, $g \circ f$ est bijective de X dans X, donc $g \circ f \in G$.
- La loi $\circ$ est associative, en particulier dans G.
- Soit $f \in G$. Puisque f est bijective de X dans X, d'après le cours, f^{-1} existe et est bijective de X dans X, donc $f^{-1} \in G$.

Ainsi, tout élément de G admet un symétrique pour la loi $\circ$ dans G.

On conclut : G est un groupe pour la loi $\circ$.

Exemple

Soit $n \in \mathbb{N}^*$.
On note G l'ensemble des matrices de $\mathbf{M}_n(\mathbb{R})$ triangulaires supérieures et à termes diagonaux tous > 0.
Montrer que G est un groupe pour la multiplication.

Nous allons montrer que G est un groupe pour la multiplication en montrant que G est un sous-groupe du groupe $\mathbf{GL}_n(\mathbb{R})$.

- On a $G \neq \varnothing$, car $\mathrm{I}_n \in G$.
- Pour toute $A \in G$, A est triangulaire supérieure à termes diagonaux tous non nuls, donc, d'après le cours, A est inversible.

Ainsi : $G \subset \mathbf{GL}_n(\mathbb{R})$.

- Soient $A, B \in G$. Puisque A et B sont triangulaires supérieures, d'après le cours leur matrice produit AB est triangulaire supérieure et les termes diagonaux de AB sont les produits des termes diagonaux de A par ceux de B (à la même place), donc sont tous > 0, d'où $AB \in G$.
- Soit $A \in G$. Puisque A est triangulaire supérieure à termes diagonaux tous non nuls, d'après le cours A^{-1} est aussi triangulaire supérieure et les termes diagonaux de A^{-1} sont les inverses de ceux de A (à la même place), donc sont tous > 0, d'où $A^{-1} \in G$.

Ceci montre que G est un sous-groupe du groupe $\mathbf{GL}_n(\mathbb{R})$, et on conclut que G est un groupe pour la multiplication.

Méthode

Pour montrer qu'une partie H d'un groupe G est un sous-groupe de G

Essayer de :

- revenir à la définition de sous-groupe
- montrer que H est le sous-groupe engendré par une certaine partie de G, ou montrer que H est une intersection de sous-groupes de G

- montrer que H est l'image directe ou l'image réciproque d'un sous-groupe d'un groupe par un morphisme de groupes.

➟ **Exercices 1.3, 1.4, 1.6, 1.13**

Exemple

Soit G un groupe noté multiplicativement.
On définit le centre $\mathrm{C}(G)$ du groupe G par :

$$\mathrm{C}(G) = \big\{x \in G\,;\ \forall a \in G,\ \ ax = xa\big\}.$$

Montrer que $\mathrm{C}(G)$ est un sous-groupe de G.

Nous allons montrer que $\mathrm{C}(G)$ est un sous-groupe de G en revenant à la définition d'un sous-groupe.

- D'abord, il est clair que $\mathrm{C}(G)$ est inclus dans G.
- On a : $\forall a \in G,\ \ ae = a = ea$, donc : $e \in \mathrm{C}(G)$.
- Soient $x, y \in \mathrm{C}(G)$. On a :

$$\forall a \in G,\ \ a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a,$$

donc : $xy \in \mathrm{C}(G)$.

- Soit $x \in \mathrm{C}(G)$. On a, pour tout $a \in G$:

$$ax^{-1} = (x^{-1}x)(ax^{-1}) = x^{-1}(xa)x^{-1} = x^{-1}(ax)x^{-1} = x^{-1}a,$$

donc : $x^{-1} \in \mathrm{C}(G)$.

Ou encore :

$$ax = xa \implies x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} \implies x^{-1}a = ax^{-1}.$$

On conclut : $\mathrm{C}(G)$ est un sous-groupe de G.

Exemple

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

$$\mathbf{SL}_n(\mathbb{C}) = \big\{M \in \mathbf{M}_n(\mathbb{C})\,;\ \det(M) = 1\big\}.$$

Montrer que $\mathbf{SL}_n(\mathbb{C})$ est un sous-groupe de $\mathbf{GL}_n(\mathbb{C})$ pour la multiplication.

Nous allons montrer que $\mathbf{SL}_n(\mathbb{C})$ est un sous-groupe de $\mathbf{GL}_n(\mathbb{C})$ en faisant apparaître $\mathbf{SL}_n(\mathbb{C})$ comme image réciproque d'un sous-groupe par un morphisme de groupes.

Considérons l'application $f : \mathbf{GL}_n(\mathbb{C}) \longrightarrow \mathbb{C}^*,\ \ M \longmapsto \det(M)$,

qui est correctement définie car : $\forall M \in \mathbf{GL}_n(\mathbb{C}),\ \ \det(M) \in \mathbb{C}^*$.

D'après le cours, $\mathbf{GL}_n(\mathbb{C})$ est un groupe pour la multiplication (des matrices) et $\mathbb{C}^*$ est un groupe pour la multiplication (des nombres complexes).

L'application f est un morphisme de groupes car, pour tout couple $(M, N) \in \big(\mathbf{GL}_n(\mathbb{C})\big)^2$:

$$f(MN) = \det(MN) = \det(M)\det(N) = f(M)f(N).$$

Par définition de $\mathbf{SL}_n(\mathbb{C})$, on a : $\mathbf{SL}_n(\mathbb{C}) = f^{-1}(\{1\})$.

Il est clair que $\{1\}$ est un sous-groupe de $\mathbb{C}^*$.

Ainsi, $\mathbf{SL}_n(\mathbb{C})$ est l'image réciproque d'un sous-groupe par un morphisme de groupes.

D'après le cours, on conclut que $\mathbf{SL}_n(\mathbb{C})$ est un sous-groupe de $\mathbf{GL}_n(\mathbb{C})$.

Méthode

Pour effectuer des calculs dans un groupe

Utiliser la définition de la notion de groupe : associativité, existence du neutre, existence des symétriques.

➟ **Exercices 1.1, 1.2, 1.5**

Exemple

Soient $(G,\cdot)$ un groupe, $a,b \in G$ tels que :
$$ba = ab^{-1}.$$
Montrer : $b^2a = ab^{-2}$.

Plusieurs calculs sont possibles, par exemple les deux suivants.

- Calculons b^2a en faisant intervenir b^{-1} :
$$b^2a = b(ba) = b(ab^{-1}) = (ba)b^{-1} = (ab^{-1})b^{-1} = ab^{-2}.$$
- Puisque $ba = ab^{-1}$, on a, en composant à droite par b, $bab = a$, puis, en composant à gauche et à droite par b, $b^2ab^2 = bab$ et donc $b^2ab^2 = a$, puis enfin, $b^2a = ab^{-2}$.

Méthode

Pour montrer qu'une application :
$$f : G \longrightarrow G'$$
est un morphisme de groupes

Après avoir vérifié que G et G' sont bien des groupes et que f est correctement définie, revenir à la définition, c'est-à-dire montrer :
$$\forall (x,y) \in G^2, \quad f(xy) = f(x)f(y).$$

➟ **Exercices 1.10, 1.13**

Exemple

Soit $(G,\cdot)$ un groupe commutatif.
Montrer que l'application
$$f : G \longrightarrow G, \quad x \longmapsto x^2$$
est un morphisme de groupes.

On a, pour tout $(x,y) \in G^2$:
$$f(xy) = (xy)^2 = (xy)(xy) = x(yx)y$$
$$= x(xy)y = (xx)(yy) = x^2y^2 = f(x)f(y),$$
donc f est un morphisme de groupes.

Bien remarquer que l'on a utilisé la commutativité de la loi, en remplaçant yx par xy.

Méthode

Pour montrer que deux groupes ne sont pas isomorphes

Raisonner par l'absurde : supposer qu'il existe un isomorphisme de l'un dans l'autre, et amener une contradiction.

Exemple

Montrer que les groupes additifs $\mathbb{Q}$ et $\mathbb{Z}$ ne sont pas isomorphes.

Raisonnons par l'absurde : supposons qu'il existe un isomorphisme de groupes f de $(\mathbb{Q},+)$ sur $(\mathbb{Z},+)$.

Nous allons utiliser le fait que l'équation $x + x = 1$ admet une solution dans $\mathbb{Q}$ mais n'admet pas de solution dans $\mathbb{Z}$.

Notons $a = f^{-1}(1)$.

On a $\dfrac{a}{2} \in \mathbb{Q}$ et : $2f\left(\dfrac{a}{2}\right) = f\left(\dfrac{a}{2}\right) + f\left(\dfrac{a}{2}\right) = f\left(\dfrac{a}{2} + \dfrac{a}{2}\right) = f(a) = 1,$

donc $\dfrac{1}{2} = f\left(\dfrac{a}{2}\right) \in \mathbb{Z}$, contradiction.

Vrai ou Faux ?

1.1 On note, pour tout $(a,b) \in \mathbb{R}^* \times \mathbb{R}$: $f_{a,b} : \mathbb{R} \longrightarrow \mathbb{R}, \quad x \longmapsto ax+b$.
L'ensemble $G = \{f_{a,b} \ (a,b) \in \mathbb{R}^* \times \mathbb{R}\}$ est un groupe pour la loi $\circ$. V F

1.2 $(2\mathbb{Z}) \times (3\mathbb{Z})$ est un sous-groupe de $\mathbb{Z} \times \mathbb{Z}$ pour l'addition. V F

1.3 La réunion de deux sous-groupes H, K d'un groupe G est toujours un sous-groupe de G. V F

1.4 L'intersection de deux sous-groupes H, K d'un groupe G est toujours un sous-groupe de G. V F

1.5 Pour $n \in \mathbb{N}^*$ fixé, l'ensemble G des matrices de $\mathbf{M}_n(\mathbb{C})$ triangulaires supérieures et à termes diagonaux tous non nuls est un sous-groupe de $\mathbf{GL}_n(\mathbb{C})$. V F

1.6 Si deux éléments a, b d'un groupe $(G, \cdot)$ vérifient $ab = ba$, alors $a^2b^{-1} = b^{-1}a^2$. V F

1.7 On a, pour tous groupes $(G, \cdot)$, $(G', \cdot)$, tout morphisme de groupes $f : G \longrightarrow G'$, et tout $x \in G$: $f(x^{-1}) = \big(f(x)\big)^{-1}$. V F

1.8 L'application $f : (\mathbb{Z}/3\mathbb{Z}, +) \longrightarrow (\mathbb{Z}/4\mathbb{Z}, +), \ \widehat{x} \longrightarrow \widetilde{x}$ est un morphisme de groupes. V F

1.9 Dans tout groupe fini $(G, \cdot)$, si deux éléments x, y de G commutent et sont d'ordres finis, alors xy est d'ordre fini. V F

1.10 Les groupes multiplicatifs $\mathbb{Q}^*$ et $\mathbb{R}^*$ sont isomorphes. V F

Énoncés des exercices

1.1 Calculs dans un groupe

Soient $(G,\cdot)$ un groupe, e son neutre, $a,b\in G$ tels que : $ab=ba^2$ et $ba=ab^2$.
Montrer : $a=b=e$.

1.2 Calculs de puissances dans un groupe

Soient $(G,\cdot)$ un groupe, $a,b\in G$.
On note $c=aba^{-1}b^{-1}$, appelé *commutateur* de a et b.
Montrer : $\forall n\in\mathbb{N},\ \ ab^na^{-1}b^{-n}=(cb)^nb^{-n}$.

1.3 Exemple de sous-groupes d'un groupe-produit

Soient G,G' deux groupes, H (resp. H') un sous-groupe de G (resp. G').
Montrer que $H\times H'$ est un sous-groupe de $G\times G'$.

1.4 Centralisateur d'une partie dans un groupe

Soit $(G,\cdot)$ un groupe, de neutre noté e.
Pour toute partie A de G, on appelle *centralisateur de A dans G* la partie, notée $\mathrm{C}(A)$ de G définie par : $\mathrm{C}(A)=\big\{x\in G\,;\ \forall a\in A,\ \ ax=xa\big\}$.

a) Vérifier que, pour toute partie A de G, $\mathrm{C}(A)$ est un sous-groupe de G.

b) Montrer, pour toutes parties A,B de G :

1) $A\subset B\implies \mathrm{C}(A)\supset\mathrm{C}(B)$
2) $A\subset\mathrm{C}\big(\mathrm{C}(A)\big)$
3) $\mathrm{C}(A)=\mathrm{C}(<A>)$
4) $\mathrm{C}\big(\mathrm{C}\big(\mathrm{C}(A)\big)\big)=\mathrm{C}(A)$.

1.5 Exemple de groupe à 4 éléments

Soient $(G,\cdot)$ un groupe, e son neutre, $x,y\in G$ tels que :
$$x^2=e,\ \ y^2=e,\ \ xy=yx,\ \ x\neq e,\ \ y\neq e,\ \ x\neq y,\ \ xy\neq e.$$

a) Déterminer le cardinal du sous-groupe H engendré par $\{x,\,y\}$.

b) À quel groupe usuel H est-il isomorphe ?

1.6 Caractérisation des sous-groupes parmi les parties finies d'un groupe

Soient G un groupe, e son neutre, A une partie finie de G. Montrer que A est un sous-groupe de G si et seulement si : $e\in A$ et $\big(\forall(x,y)\in A^2,\ \ xy\in A\big)$.

1.7 Somme des caractères d'un groupe fini commutatif

Soient $(G,\cdot)$ un groupe fini commutatif, $\varphi:(G,\cdot)\longrightarrow(\mathbb{C}^*,\cdot)$ un morphisme de groupes autre que l'application constante égale à 1. Montrer : $\displaystyle\sum_{g\in G}\varphi(g)=0$.

1.8 Images directes et images réciproques de sous-groupes d'un groupe par un morphisme de groupes

Soient G, G' deux groupes commutatifs, $f : G \longrightarrow G'$ un morphisme de groupes.

a) Montrer, pour tout sous-groupe H de G : $f^{-1}\big(f(H)\big) = H + \mathrm{Ker}\,(f)$.

b) Montrer, pour tout sous-groupe H' de G' : $f\big(f^{-1}(H')\big) = H' \cap \mathrm{Im}\,(f)$.

1.9 Commutation dans un groupe

Soient G un groupe, $n \in \mathbb{N} \setminus \{0, 1\}$.

On suppose que l'application $f : G \longrightarrow G, \quad x \longmapsto x^n$ est un morphisme surjectif de groupes.

Démontrer : $\forall (x, y) \in G^2, \quad x^{n-1}y = yx^{n-1}$.

1.10 Morphismes de groupes de $\mathcal{S}_n$ dans $\mathbb{Z}/N\mathbb{Z}$

Soient $n \in \mathbb{N} \setminus \{0, 1\}$, $N \in \mathbb{N}$ impair.

Montrer que le seul morphisme de groupes de $\mathcal{S}_n$ dans $\mathbb{Z}/N\mathbb{Z}$ est l'application nulle.

1.11 Élévation au carré dans un groupe fini d'ordre impair

Soit $(G, \cdot)$ un groupe fini d'ordre impair noté $n = 2p + 1$.

Montrer que l'application $f : G \longrightarrow G, \quad x \longmapsto x^2$ est bijective et expliciter f^{-1}.

1.12 Sous-groupes d'un groupe infini

Montrer que tout groupe infini admet une infinité de sous-groupes.

1.13 Ensemble des éléments d'ordre impair d'un groupe abélien

Soient $(G, +)$ un groupe abélien, 0 son neutre.

On note A l'ensemble des éléments de G d'ordre fini impair.

a) Montrer que A est un sous-groupe de G.

b) Montrer que l'application $f : x \longmapsto 2x$ est un morphisme injectif du groupe A dans lui-même.

Du mal à démarrer ?

1.1 Calculer ab^2a de deux façons, et déduire $ab^2 = e$.

1.2 Récurrence sur n.

1.3 Revenir à la définition d'un sous-groupe d'un groupe.

1.4 *a)* Revenir à la définition de sous-groupe.

b) 1) Utiliser la définition.

2) Évident.

3) $\star$ $\mathrm{C}(< A >) \subset \mathrm{C}(A)$ par *1)*.

$\star$ Soit $x \in \mathrm{C}(A)$. Montrer $A \subset \mathrm{C}(\{x\})$,

puis $< A > \subset \mathrm{C}(\{x\})$, $x \in \mathrm{C}(< A >)$.

4) Appliquer *1)* et *2)* diversement.

1.5 *a)* Calculer les produits de e, x, y, xy entre eux.

b) Penser à un groupe d'isométries du plan euclidien.

1.6 Pour $x \in A$, considérer l'application

$$f : A \longrightarrow A, \quad y \longmapsto xy.$$

1.7 Remarquer que, puisque G est un groupe, pour tout $g_0 \in G$ fixé, l'application $G \longrightarrow G$, $\quad g \longmapsto g_0 g$ est une permutation de G, ce qui permet de réindexer la sommation.

1.8 Utiliser les définitions : morphisme de groupes, noyau, image.

Se rappeler les définitions d'image directe et d'image réciproque d'une partie par une application :

$$\forall y \in G', \quad y \in f(H) \iff \big(\exists\, x \in H, \quad y = f(x)\big),$$

$$\forall x \in G, \quad x \in f^{-1}(H') \iff f(x) \in H'.$$

1.9 Soit $(x, y) \in G^2$.

Utiliser $z \in G$ tel que $y = z^n$ et calculer $zx(x^{n-1}y)x$.

1.10 Soit $f : \mathcal{S}_n \longrightarrow \mathbb{Z}/N\mathbb{Z}$ un morphisme de groupes. Calculer $f(\tau_{ij})$ où τ_{ij} est la transposition qui échange i et j.

1.11 Montrer que f est injective en utilisant le résultat du cours : pour tout $x \in G$, $\quad x^n = e$, où e est le neutre de G et n l'ordre de G.

1.12 Soit G un groupe n'admettant qu'un nombre fini de sous-groupes.

Montrer qu'il existe une partie finie F de G telle que :

$$G = \bigcup_{x \in F} < x > .$$

D'autre part, montrer que, pour tout $x \in G$, $< x >$ est fini.

Conclure.

1.13 *a)* Revenir à la définition d'un sous-groupe et utiliser les propriétés de l'ordre d'un élément du groupe.

b) Revenir à la définition d'un morphisme de groupes et utiliser les propriétés de l'ordre d'un élément du groupe.

Vrai ou Faux, les réponses

1.1 La loi $\circ$ est interne dans G, car, pour tous (a,b), $(c,d) \in \mathbb{R}^* \times \mathbb{R}$, on a $ac \neq 0$ et : **V** F

$$\forall x \in \mathbb{R},\ \ (f_{a,b} \circ f_{c,d})(x) = a(cx+d)+b = acx + (ad+b) = f_{ac,ad+b}(x).$$

La loi $\circ$ est associative (cours), l'application $f_{1,0}$ est l'identité, neutre pour $\circ$, et, pour tout $(a,b) \in \mathbb{R}^* \times \mathbb{R}$:

$$\forall (x,y) \in \mathbb{R}^2,\ \ y = f_{a,b}(x) \iff y = ax+b \iff x = \frac{1}{a}y - \frac{b}{a} \iff x = f_{\frac{1}{a},-\frac{b}{a}}(x),$$

donc $f_{a,b}$ admet un inverse pour $\circ$ dans G, qui est $f_{\frac{1}{a},-\frac{b}{a}}$.

1.2 On a $(2\mathbb{Z} \times 3\mathbb{Z}) \subset \mathbb{Z} \times \mathbb{Z}$, $(0,0) \in (2\mathbb{Z}) \times (3\mathbb{Z})$ et, pour tous $X = (2a,\, 3b)$, $Y = (2c,\, 3d)$ de $(2\mathbb{Z}) \times (3\mathbb{Z})$, où $a,b,c,d \in \mathbb{Z}$: **V** F

$$X - Y = (2a-2c,\, 3b-3d) = \big(2(a-c),\, 3(b-d)\big) \in (2\mathbb{Z}) \times (3\mathbb{Z}).$$

1.3 Contre-exemple : $G = \mathbb{Z}$ est un groupe pour $+$, $H = 2\mathbb{Z}$ et $K = 3\mathbb{Z}$ sont des sous-groupes de G, mais $L = H \cup K$ n'est pas un sous-groupe de $\mathbb{Z}$ car $2 \in L,\ 3 \in L,\ 2+3 = 5 \notin L$. V **F**

1.4 C'est un résultat du cours. **V** F

1.5 D'après les propriétés des matrices triangulaires supérieures, $G \subset \mathbf{GL}_n(\mathbb{C})$, $\mathrm{I}_n \in \mathbf{GL}_n(\mathbb{C})$, le produit de deux éléments de G est dans G, l'inverse d'un élément de G est dans G. **V** F

1.6 On a : $ba^2 = (ba)a = (ab)a = a(ba) = a(ab) = a^2b$, puis, en multipliant chaque membre de cette égalité par b^{-1} à gauche et à droite : $a^2b^{-1} = b^{-1}a^2$. **V** F

Plus généralement, si deux éléments a, b d'un groupe commutent, alors toute puissance (d'exposant dans $\mathbb{Z}$) de a commute avec toute puissance (d'exposant dans $\mathbb{Z}$) de b.

1.7 Puisque f est un morphisme de groupes, on a, en notant e (resp. e') le neutre de G (resp. G') : $f(e) = f(ee) = f(e)f(e)$, donc $f(e) = e'$, **V** F
puis, pour tout $x \in G$, $e' = f(e) = f(xx^{-1}) = f(x)f(x^{-1})$
et, par un raisonnement analogue, $e' = f(x^{-1})f(x)$, donc $f(x^{-1}) = \big(f(x)\big)^{-1}$.

1.8 L'application f n'est pas correctement définie car, par exemple, $\widehat{0} = \widehat{3}$ dans $\mathbb{Z}/3\mathbb{Z}$, mais $\widetilde{0} \neq \widetilde{3}$ dans $\mathbb{Z}/4\mathbb{Z}$. V **F**

1.9 Il existe $a, b \in \mathbb{N}^*$ tels que $x^a = e$ et $y^b = e$, où e est le neutre de G, et on a alors, puisque x et y commutent : $(xy)^{ab} = x^{ab}y^{ab} = (x^a)^b(y^b)^a = e^b\,\mathrm{e}^{\,a} = e$, donc xy est d'ordre fini. **V** F

On peut aussi utiliser le ppcm de a et b, au lieu du produit de a et b.

1.10 S'il existait un isomorphisme de groupes f de $\mathbb{Q}^*$ dans $\mathbb{R}^*$, alors f serait une bijection, contradiction avec $\mathbb{Q}^*$ dénombrable et $\mathbb{R}^*$ non dénombrable. V **F**

Corrigés des exercices

1.1

Calculons ab^2a de deux façons :

$ab^2a = (ab)(ba) = (ba^2)(ab^2)$, $ab^2a = (ab^2)a = (ba)a = ba^2$,

donc $(ba^2)(ab^2) = (ba^2)$, puis comme G est un groupe, on peut simplifier par ba^2 à gauche, d'où $ab^2 = e$.
On a donc $ba = ab^2 = e$, puis : $ab = ba^2 = (ba)a = ea = a$, d'où, en simplifiant par a à gauche dans le groupe G, $b = e$, et enfin $e = ba = ea = a$.

1.2

Notons e le neutre de G et effectuons une récurrence sur n.

Pour $n = 0$, on a d'une part $ab^na^{-1}b^{-n} = aea^{-1}e = e$ et d'autre part $(cb)^nb^{-n} = ee = e$, donc la formule est vraie pour $n = 0$.

Supposons la formule vraie pour un $n \in \mathbb{N}$ fixé, c'est-à-dire $ab^na^{-1}b^{-n} = (cb)^nb^{-n}$, ce qui revient à $ab^na^{-1} = (cb)^n$.
On a alors :

$$\begin{aligned} ab^{n+1}a^{-1}b^{-(n+1)} &= (ab^n)(ba^{-1}b^{-1}b^{-n}) \\ &= (ab^na^{-1})(aba^{-1}b^{-1})b^{-n} \\ &\underset{HR_n}{=} (cb)^ncb^{-n} = (cb)^n(cb)b^{-n-1} \\ &= (cb)^{n+1}b^{-(n+1)}, \end{aligned}$$

donc la formule est vraie pour $n + 1$.
On conclut, par récurrence sur n, à la formule voulue, pour tout $n \in \mathbb{N}$.

1.3

Rappelons que, d'après le cours, $G \times G'$ est un groupe, la loi étant définie par :

$$\forall (h,\, h'),\ (k,\, k') \in G \times G',\quad (h,\, h')(k,\, k') = (hk,\, h'k').$$

Notons e (resp. e') le neutre de G (resp. G').

- On a, pour tous $(h,\, h')$, $(k,\, k') \in H \times H'$:
$$(h,\, h')(k,\, k') = (hk,\, h'k') \in H \times H'.$$
- Puisque $e \in H$ et $e' \in H'$, on a : $(e, e') \in H \times H'$.
- On a, pour tout $(h,\, h') \in H \times H'$:
$$(h,\, h')^{-1} = (h^{-1},\, h'^{-1}) \in h \times H'.$$

On conclut que $H \times H'$ est un sous-groupe de $G \times G'$.

1.4

a) Soit A une partie de G.

- On a $e \in \mathrm{C}(A)$, puisque : $\forall a \in A,\quad ae = ea$.
- On a, pour tous $x, y \in \mathrm{C}(A)$:

$\forall a \in A,\quad (xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$,
et donc : $xy \in \mathrm{C}(A)$.

Soit $x \in \mathrm{C}(A)$. On a : $\forall a \in A,\quad ax = xa$,
d'où, en composant par x^{-1} à gauche et à droite :

$$\forall a \in A,\quad x^{-1}a = ax^{-1},$$

et donc : $x^{-1} \in \mathrm{C}(A)$.

Ainsi, $\mathrm{C}(A)$ est un sous-groupe de G.

b) 1) Supposons $A \subset B$, et soit $x \in \mathrm{C}(B)$.

On a : $\forall b \in B,\quad bx = xb$,
donc, a fortiori : $\forall a \in A,\quad ax = xa$,
c'est-à-dire : $x \in \mathrm{C}(A)$.

Ceci montre : $\mathrm{C}(B) \subset \mathrm{C}(A)$.

2) Soit $a \in A$. On a, par définition de $\mathrm{C}(A)$:

$$\forall x \in \mathrm{C}(A),\quad ax = xa,$$

donc, par définition de $\mathrm{C}\big(\mathrm{C}(A)\big)$: $\quad a \in \mathrm{C}\big(\mathrm{C}(A)\big)$.

Ceci montre : $A \subset \mathrm{C}\big(\mathrm{C}(A)\big)$.

3) • On a $A \subset < A >$,
donc, d'après *b) 1)* : $\mathrm{C}(A) \supset \mathrm{C}\big(< A > \big)$.

• Soit $x \in \mathrm{C}(A)$.
Puisque : $\forall a \in A,\quad ax = xa$, on a : $A \subset \mathrm{C}(\{x\})$.

Comme $\mathrm{C}(\{x\})$ est un sous-groupe de G, il en résulte :

$$< A > \subset \mathrm{C}(\{x\}),$$

c'est-à-dire : $\forall \alpha \in < A >,\quad \alpha x = x\alpha$,

et donc : $\quad x \in \mathrm{C}\big(< A > \big)$.

Ainsi : $\quad \mathrm{C}(A) = \mathrm{C}\big(< A > \big)$.

4) D'après *2)* appliqué à $\mathrm{C}(A)$ à la place de A, on a :

$$\mathrm{C}(A) \subset \mathrm{C}\Big(\mathrm{C}\big(\mathrm{C}(A)\big)\Big).$$

D'après *2)*, on a : $\quad A \subset \mathrm{C}\big(\mathrm{C}(A)\big)$,

puis, d'après α) : $\quad \mathrm{C}(A) \supset \mathrm{C}\Big(\mathrm{C}\big(\mathrm{C}(A)\big)\Big)$.

On conclut : $\quad \mathrm{C}(A) = \mathrm{C}\Big(\mathrm{C}\big(\mathrm{C}(A)\big)\Big)$.

1.5

a) • Il est clair que H contient e, x, y, xy et que ces quatre éléments sont deux à deux distincts.

• Notons $L = \{e, x, y, xy\}$ et calculons les composés des éléments de L entre eux deux à deux.

Par exemple : $(xy)(xy) = x(yx)y = x(xy)y = x^2y^2 = ee = e$.

	e	x	y	xy
e	e	x	y	xy
x	x	e	xy	y
y	y	xy	e	x
xy	xy	y	x	e

On remarque :

⋆ le neutre e est dans L

⋆ le produit de deux éléments de L est dans L

⋆ l'inverse d'un élément de L est dans L.

Ainsi, L est un sous-groupe de G.

Comme $\{x, y\} \subset L$, on a donc, d'après le cours : $H \subset L$.

Finalement : $H = \{e, x, y, xy\}$ et on conclut :

$$\mathrm{Card}\,(H) = 4.$$

b) Le groupe H est isomorphe, par exemple, au groupe des isométries vectorielles du plan euclidien rapporté à un repère orthonormé, formé par l'identité, les deux réflexions par rapport aux deux axes de coordonnées, et la symétrie centrale par rapport à l'origine.

1.6

1) Si A est un sous-groupe de G, alors, d'après le cours :

$$e \in A \ \text{ et } \ \big(\forall x, y \in A, \ \ xy \in A\big).$$

2) Réciproquement, supposons :

$$e \in A \ \text{ et } \ \big(\forall x, y \in A, \ \ xy \in A\big).$$

Soit $x \in A$ fixé. Considérons l'application

$$f : A \longrightarrow A, \ \ y \longmapsto xy,$$

qui est correctement définie d'après l'hypothèse.

On a, pour tout $(y_1, y_2) \in A^2$:

$$f(y_1) = f(y_2) \iff xy_1 = xy_2 \iff y_1 = y_2,$$

car, G étant un groupe, x admet un inverse.

Ceci montre que f est injective.

Puisque $f : A \longrightarrow A$ est injective et que A est finie, on déduit que f est bijective.

Comme $e \in A$ et que f est surjective, il existe $x' \in A$ tel que $f(x') = e$, c'est-à-dire : $xx' = e$, et on a donc : $x^{-1} = x' \in A$.

Finalement :

$$e \in A, \ \ \big(\forall x, y \in A, \ \ xy \in A\big), \ \ \big(\forall x \in A, \ \ x^{-1} \in A.\big)$$

On conclut que A est un sous-groupe de G.

1.7

Comme $\varphi \neq 1$, il existe $g_0 \in G$ tel que $\varphi(g_0) \neq 1$. Puisque G est un groupe, l'application $G \longrightarrow G, \ g \longmapsto g_0 g$ est une permutation de G, d'où :

$$\sum_{g \in G} \varphi(g) = \sum_{g \in G} \varphi(g_0 g) = \sum_{g \in G} \varphi(g_0)\varphi(g) = \varphi(g_0) \sum_{g \in G} \varphi(g).$$

On déduit : $\big(\underbrace{1 - \varphi(g_0)}_{\neq 0}\big) \displaystyle\sum_{g \in G} \varphi(g) = 0,$

et on conclut : $\displaystyle\sum_{g \in G} \varphi(g) = 0.$

1.8

a) 1) Soit $x \in f^{-1}\big(f(H)\big)$. Alors, $f(x) \in f(H)$, donc il existe $h \in H$ tel que : $f(x) = f(h)$.
D'où : $f(x - h) = f(x) - f(h) = 0$,

donc : $x - h \in \mathrm{Ker}\,(f)$.

Ainsi : $x = h + (x - h), \ \ h \in H, \ \ x - h \in \mathrm{Ker}\,(f)$.

Ceci montre : $f^{-1}\big(f(H)\big) \subset H + \mathrm{Ker}\,(f)$.

2) Réciproquement, soit $x \in H + \mathrm{Ker}\,(f)$.
Il existe $h \in H$, $u \in \mathrm{Ker}\,(f)$ tels que : $x = h + u$.
On a : $f(x) = f(h + u) = f(h) + f(u) = f(h) \in f(H)$,

donc : $x \in f^{-1}\big(f(H)\big)$.

Ceci montre : $H + \mathrm{Ker}\,(f) \subset f^{-1}\big(f(H)\big)$.

On conclut : $f^{-1}\big(f(H)\big) = H + \mathrm{Ker}\,(f)$.

b) 1) Soit $y \in f\big(f^{-1}(H')\big)$.
Il existe $x \in f^{-1}(H')$ tel que $y = f(x)$.
Alors, $f(x) \in H'$, donc $y = f(x) \in H'$.
De plus, par définition de $\mathrm{Im}\,(f)$: $y = f(x) \in \mathrm{Im}\,(f)$.

On déduit : $y \in H' \cap \mathrm{Im}\,(f)$.

Ceci montre : $f\big(f^{-1}(H')\big) \subset H' \cap \mathrm{Im}\,(f)$.

2) Réciproquement, soit $y \in H' \cap \mathrm{Im}\,(f)$.
Alors, $y \in H'$ et il existe $x \in G$ tel que $y = f(x)$.
Comme $f(x) = y \in H'$, on a : $x \in f^{-1}(H')$.
Ainsi : $y = f(x) \in f\big(f^{-1}(H')\big)$.

Ceci montre : $H' \cap \mathrm{Im}\,(f) \subset f\big(f^{-1}(H')\big)$.

On conclut : $f\big(f^{-1}(H')\big) = H' \cap \mathrm{Im}\,(f)$.

1.9

Soit $(x, y) \in G^2$.

Puisque f est surjectif, il existe $z \in G$ tel que : $y = f(z) = z^n$.

On a : $x^n y = x^n z^n = f(x)f(z) = f(xz) = (xz)^n$,

puis :

$$z(x^n y)x = z\big((xz)^n\big)x = (zx)^{n+1}$$
$$= (zx)(zx)^n = zxf(zx) = zxf(z)f(x) = zxz^n x^n.$$

En simplifiant à gauche par zx et à droite par x, on déduit :

$$x^{n-1}y = z^n x^{n-1} = yx^{n-1}.$$

1.10

Soit $f : \mathcal{S}_n \longrightarrow \mathbb{Z}/N\mathbb{Z}$ un morphisme de groupes.

- Soit $(i, j) \in \{1, ..., n\}^2$ tel que $i < j$.

Notons τ_{ij} la transposition qui échange i et j. On a :

$$2f(\tau_{ij}) = f(\tau_{ij}^2) = f(\mathrm{Id}_{\{1,...,n\}}) = 0.$$

Comme N est impair, 2 est premier avec N, donc on peut simplifier par 2 et déduire : $f(\tau_{ij}) = 0$.

Ceci montre que, pour toute transposition τ, on a : $f(\tau) = 0$.

- Soit $\sigma \in \mathcal{S}_n$. D'après le cours, il existe $p \in \mathbb{N}^*$ et des transpositions $\tau_1, ..., \tau_p$ telles que : $\sigma = \tau_1 \circ \cdots \circ \tau_p$.
On a alors, puisque f est un morphisme de groupes :

$$f(\sigma) = f(\tau_1 \circ \cdots \circ \tau_p)$$
$$= f(\tau_1) + \cdots + f(\tau_p) = 0 + \cdots + 0 = 0.$$

On déduit : $f = 0$.

On conclut que le seul morphisme de groupes de $\mathcal{S}_n$ dans $\mathbb{Z}/N\mathbb{Z}$ (pour N impair) est l'application nulle.

1.11

- Montrons que f est injective.

Soit $(x, y) \in G^2$ tel que $f(x) = f(y)$, c'est-à-dire $x^2 = y^2$.
Puisque G est d'ordre fini, noté n, on a, d'après le cours, en notant e le neutre de G : $\ \forall t \in G, \ \ t^n = e$.
Comme $n = 2p + 1$, on a donc : $\ x^{2p+1} = e \ \text{ et } \ y^{2p+1} = e$.
D'où :

$$x = ex = x^{2p+1}x = x^{2p+2} = (x^2)^{p+1}$$
$$= (y^2)^{p+1} = y^{2p+2} = y^{2p+1}y = ey = y.$$

Ceci montre que f est injective.

• On a, pour tout $z \in G$:

$$z = ez = z^{2p+1}z = z^{2p+2} = (z^{p+1})^2 = f(z^{p+1}),$$

donc f est surjective, puis bijective, et l'application réciproque f^{-1} de f est donnée par :

$$\forall z \in G, \quad f(z) = z^{p+1}.$$

1.12

Par contraposition, montrons que, si un groupe n'admet qu'un nombre fini de sous-groupes, alors ce groupe est fini.

Soit G un groupe n'admettant qu'un nombre fini de sous-groupes.

• Il est clair qu'en notant, pour tout $x \in G$, $< x >$ le sous-groupe de G engendré par x, on a : $G = \bigcup_{x \in G} < x >$.

Comme G n'a qu'un nombre fini de sous-groupes, il existe une partie finie F de G telle que : $G = \bigcup_{x \in F} < x >$.

• D'autre part, montrons que, pour tout $x \in G$, $< x >$ est fini. Raisonnons par l'absurde. Supposons qu'il existe $x \in G$ tel que $< x >$ soit infini. D'après le cours, on a alors : $< x > \simeq \mathbb{Z}$. On sait, d'après le cours, que $\mathbb{Z}$ admet une infinité de sous-groupes, les $n\mathbb{Z}$, pour $n \in \mathbb{N}^*$, deux à deux distincts. Par isomorphisme, $< x >$ admet une infinité de sous-groupes, puis G admet une infinité de sous-groupes, contradiction.

Ceci montre que, pour tout $x \in G$, $< x >$ est fini.

• Puisque $G = \bigcup_{x \in F} < x >$, et que F et les $< x >$ sont finis, on conclut que G est fini.

1.13

a) • On a $A \subset G$ et $0 \in A$ puisque 0, le neutre de G, est d'ordre 1, impair.

• Soient $x, y \in A$. Il existe $\alpha, \beta \in \mathbb{N}$, impairs, tels que $\alpha x = 0$ et $\beta y = 0$. On a alors $\alpha\beta(x + y) = \beta(\alpha x) + \alpha(\beta y) = 0$. Il en résulte que l'ordre γ de $x + y$ divise $\alpha\beta$. Comme α et β sont impairs, ce produit $\alpha\beta$ est impair, donc γ est impair, d'où $x + y \in A$.

• Soit $x \in A$. Il existe $\alpha \in \mathbb{N}$ impair tel que $\alpha x = 0$. On a alors $\alpha(-x) = -\alpha x = 0$, donc l'ordre de $-x$ divise α, donc cet ordre est impair, puis $-x \in A$.

On conclut : A est un sous-groupe de G.

b) • D'après *a)*, on a, pour tout $x \in A$, $f(x) = 2x = x + x \in A$, donc l'application f est correctement définie de A dans A.

• On a, pour tout $(x, y) \in A^2$:

$$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y),$$

donc f est un morphisme de groupes de A dans lui-même.

• Soit $x \in \mathrm{Ker}\,(f)$. On a alors $2x = f(x) = 0$, donc l'ordre de x divise 2. Comme x est d'ordre impair, cet ordre est nécessairement égal à 1, d'où $x = 0$.

On conclut : f est un morphisme injectif du groupe G dans lui-même.

Anneaux, arithmétique

Chapitre 2

Plan

Thèmes abordés dans les exercices

- Établir une structure d'anneau, de sous-anneau, d'idéal d'un anneau commutatif
- Calculs dans un anneau, manipulation d'éléments nilpotents, d'éléments idempotents, de diviseurs de 0
- Manipulation de morphismes d'anneaux, endomorphismes d'un anneau, isomorphismes d'anneaux, automorphismes d'un anneau
- Résolution de congruences à une ou plusieurs inconnues, résolution d'équations dans $\mathbb{Z}/n\mathbb{Z}$
- Résolution d'équations sur l'indicateur φ d'Euler
- Intervention de la finitude dans les anneaux.

Points essentiels du cours pour la résolution des exercices

- Définition et propriétés de la structure d'anneau, de sous-anneau, d'idéal d'un anneau commutatif
- Définition et propriétés des morphismes d'anneaux, endomorphismes d'un anneau, isomorphismes d'anneaux, automorphismes d'un anneau
- Anneaux usuels $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $K[\mathrm{X}]$, $\mathbb{R}^E, \mathcal{L}(E)$, $\mathbf{M}_n(K)$
- Dans $\mathbb{Z}$: notion de nombres premiers entre eux, pgcd, ppcm, théorème de Gauss, théorème de Bézout, théorème chinois, décomposition primaire, caractérisation des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, indicateur d'Euler, théorème d'Euler
- Dans $K[\mathrm{X}]$: notion de polynômes premiers entre eux, pgcd, théorème de Gauss, théorème de Bézout, décomposition primaire.

Les méthodes à retenir

Méthode

Pour montrer qu'un ensemble A muni de deux lois $+$ et $\cdot$ est un anneau

Essayer de :

- revenir à la définition d'un anneau
- montrer que A est un sous-anneau d'un anneau connu.

➟ **Exercices 2.2, 2.9**

Exemple

Montrer que l'ensemble A des applications bornées de $\mathbb{R}$ dans $\mathbb{R}$ est un anneau pour les lois usuelles (addition et multiplication).

Nous allons montrer que A est un sous-anneau de l'anneau F de toutes les applications de $\mathbb{R}$ dans $\mathbb{R}$.

- Il est clair que $A \subset F$ et que l'élément neutre de la multiplication dans F, qui est l'application constante 1, est dans A.
- Pour tout $(f, g) \in A^2$, $f - g$ et fg sont bornées puisque la différence et le produit de deux applications bornées sont bornées.

On conclut que A est un sous-anneau de F, donc A est un anneau.

Méthode

Pour utiliser une hypothèse portant sur les éléments d'un anneau

Penser à appliquer cette hypothèse, par exemple, à x, à y, à $x + y$, à $1 + x$, à $1 - x$, ...

➟ **Exercices 2.5, 2.17**

Exemple

Soit A un anneau tel que :
$$\forall a \in A,\ \ a^3 = a^2.$$
Montrer : $\forall a \in A,\ \ a^2 = a.$

Remarquons d'abord que l'on n'a pas le droit de simplifier directement par a.

Soit $a \in A$.

Appliquons l'hypothèse à $1 - a$: $\ (1-a)^3 = (1-a)^2$,

c'est-à-dire : $\ 1 - 3a + 3a^2 - a^3 = 1 - 2a + a^2$,

et, puisque $a^3 = a^2$, on obtient : $\ a^2 = a$.

Méthode

Pour montrer qu'une partie B d'un anneau A est un sous-anneau de A

Revenir à la définition, c'est-à-dire montrer $1_A \in B$ et :
$$\forall (x, y) \in B^2,\ \ x + y \in B,\ -x \in B,\ xy \in B.$$

➟ **Exercices 2.1, 2.2, 2.8, 2.17**

Exemple

On note $A = \mathbf{M}_2(\mathbb{R})$.

Montrer que l'ensemble B des matrices de A à coefficients dans $\mathbb{Z}$ est un sous-anneau de A.

D'abord, d'après le cours, A est un anneau pour l'addition et la multiplication des matrices.

- On a clairement : $B \subset A$ et $\mathrm{I}_2 \in B$.
- Soient $M, N \in B$.

Puisque M et N sont à coefficients dans $\mathbb{Z}$, par addition, opposition, produit matriciel, les matrices $M+N$, $-M$, MN sont à coefficients dans $\mathbb{Z}$, donc sont dans B.

On conclut : B est un sous-anneau de A.

Méthode

Pour montrer qu'une partie I d'un anneau commutatif A est un idéal de A

Revenir à la définition, c'est-à-dire montrer :

$$0_A \in I, \quad \forall (x,y) \in I^2, \ x - y \in I, \quad \forall a \in A, \ \forall x \in I, \ ax \in I.$$

➟ **Exercices 2.2, 2.8, 2.9, 2.12, 2.13**

Exemple

On note $A = C([0\,;1], \mathbb{R})$ et :
$$I = \{f \in A\,;\, f(1) = 0\}.$$
Montrer que I est un idéal de l'anneau commutatif A.

D'abord, A est bien un anneau commutatif, d'après le cours.

- On a : $I \subset A$ et $0 \in I$.
- On a, pour tout $(f,g) \in I^2$:
$$(f-g)(1) = f(1) - g(1) = 0 - 0 = 0,$$
donc $f - g \in I$.
- On a, pour toute $f \in I$ et toute $h \in A$:
$$(hf)(1) = h(1)f(1) = h(1)0 = 0,$$
donc $hf \in I$.

On conclut, d'après la définition, que I est un idéal de l'anneau commutatif A.

Méthode

Pour montrer que deux anneaux ne sont pas isomorphes

Raisonner par l'absurde : supposer qu'il existe un isomorphisme de l'un dans l'autre, et amener une contradiction.

➟ **Exercice 2.14**

Exemple

Montrer que les anneaux :
$$\mathbb{Z}/4\mathbb{Z} \text{ et } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
ne sont pas isomorphes.

Remarquons d'abord que ces deux anneaux sont finis et ont le même cardinal.

Supposons qu'il existe un isomorphisme d'anneaux f de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Pour amener une contradiction, l'idée est de remarquer que l'équation $x^2 = x$ est satisfaite par tous les éléments de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ mais ne l'est pas par tous les éléments de $\mathbb{Z}/4\mathbb{Z}$.

Notons $\widetilde{a}$ la classe d'un élément a de $\mathbb{Z}$ dans $\mathbb{Z}/4\mathbb{Z}$.
On a clairement : $\forall x \in \mathbb{Z}/2\mathbb{Z},\ \ x^2 = x$,
donc : $\forall (x,y) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \ (x,y)^2 = (x^2, y^2) = (x,y)$.
On a alors, puisque $f(\widetilde{2}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$:

$$f(\widetilde{2}) = \big(f(\widetilde{2})\big)^2 = f(\widetilde{2}^2) = f(\widetilde{4}) = f(\widetilde{0}),$$

d'où, puisque f est injective : $\widetilde{2} = \widetilde{0}$, contradiction.

On conclut que les deux anneaux envisagés ne sont pas isomorphes.

Méthode

Pour obtenir des résultats concernant des anneaux finis

Penser à utiliser des applications du genre, pour $a \in A$ fixé :

$$f : A \longrightarrow A,\ \ x \longmapsto ax,$$

et essayer de montrer que f est injective, pour en déduire, puisque A est supposé fini, que f est surjective.

➟ **Exercice 2.18**

Exemple

Montrer que tout anneau commutatif intègre fini est un corps.

Soit A un anneau commutatif intègre fini. Soit $a \in A \setminus \{0\}$.
L'application $f : A \longrightarrow A,\ \ x \longmapsto ax$ est injective car, pour tout $(x,x') \in A^2$, puisque A est intègre et que $a \neq 0$, on a :

$$f(x) = f(x') \iff ax = ax' \implies x = x'.$$

Ainsi, f est une application injective d'un ensemble fini dans lui-même. D'après le cours, il en résulte que f est surjective.
Il existe donc $b \in A$ tel que $f(b) = 1$, c'est-à-dire $ab = 1$.

Ceci montre que tout élément non nul de A admet un inverse, et on conclut que A est un corps.

Méthode

Pour résoudre un système de congruences simultanées, à une inconnue dans $\mathbb{Z}$

Résoudre la première équation, par exemple, en exprimant x en fonction d'un autre entier, noté a par exemple, puis reporter dans la deuxième équation, et réitérer.

➟ **Exercice 2.3**

Exemple

Résoudre le système d'équations, d'inconnue $x \in \mathbb{Z}$:

$$\begin{cases} x \equiv 2 \ \ [12] \\ x \equiv 10 \ \ [16]. \end{cases}$$

Soit $x \in \mathbb{Z}$. On a : $x \equiv 2\ \ [12] \iff \big(\exists\, a \in \mathbb{Z},\ \ x = 2 + 12a\big)$.
Ensuite :

$$x \equiv 10\ \ [16] \iff 2 + 12a \equiv 10\ \ [16] \iff 12a \equiv 8\ \ [16]$$
$$\iff 3a \equiv 2\ \ [4] \iff -a \equiv 2\ \ [4] \iff a \equiv -2\ \ [4]$$
$$\iff a \equiv 2\ \ [4] \iff \big(\exists\, b \in \mathbb{Z},\ \ a = 2 + 4b\big).$$

On obtient : $x = 2 + 12a = 2 + 12(2 + 4b) = 26 + 48b$.
On conclut : $\mathcal{S} = \big\{26 + 48b\,;\, b \in \mathbb{Z}\big\}$.

Méthode

Pour résoudre un système d'équations dont l'inconnue est :
$(x, y) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^2$

Essayer de :

- exprimer une des deux inconnues en fonction de l'autre à partir d'une des deux équations, puis reporter dans l'autre
- combiner les équations pour éliminer une des deux inconnues.

➟ **Exercice 2.4**

Exemple

Résoudre le système d'équations, d'inconnue $(x, y) \in (\mathbb{Z}/8\mathbb{Z})^2$:

$$\text{(S)} \quad \begin{cases} \widehat{3}x + \widehat{2}y = \widehat{4} \\ \widehat{2}x + \widehat{3}y = -\widehat{3}. \end{cases}$$

Plusieurs calculs sont possibles.

On essaiera, autant que possible, de maintenir des équivalences logiques entre systèmes successifs.
On a, par $L_1 \longleftarrow L_1 - L_2$:

$$\text{(S)} \iff \begin{cases} x - y = \widehat{7} = -\widehat{1} \\ \widehat{2}x + \widehat{3}y = -\widehat{3} \end{cases} \iff \begin{cases} x = y - \widehat{1} \\ \widehat{2}(y - \widehat{1}) + \widehat{3}y = -\widehat{3} \end{cases} \iff \begin{cases} x = y - \widehat{1} \\ \widehat{5}y = -\widehat{1}. \end{cases}$$

Comme $\widehat{5} \cdot (-\widehat{3}) = -\widehat{15} = \widehat{1}$, l'élément $\widehat{5}$ est inversible dans $\mathbb{Z}/8\mathbb{Z}$ et son inverse est $-\widehat{3}$, donc :

$$\text{(S)} \iff \begin{cases} x = y - \widehat{1} \\ y = (-\widehat{3})(-\widehat{1}) = \widehat{3} \end{cases} \iff \begin{cases} x = \widehat{2} \\ y = \widehat{3}. \end{cases}$$

On conclut : $\mathcal{S} = \{(\widehat{2}, \widehat{3})\}$.

On peut contrôler que le couple $(\widehat{2}, \widehat{3})$ vérifie bien le système (S), le calcul peut être fait de tête.

Méthode

Pour résoudre une équation algébrique d'inconnue $x \in \mathbb{Z}/n\mathbb{Z}$

Essayer, si n n'est pas trop grand, tous les $x \in \mathbb{Z}/n\mathbb{Z}$, ou, si possible, seulement tous ceux vérifiant une condition nécessaire.

➟ **Exercice 2.10**

Exemple

Résoudre l'équation $x^4 = \widehat{4}$,
d'inconnue $x \in \mathbb{Z}/9\mathbb{Z}$.

On calcule x^4 pour chaque valeur de x, en remarquant que, pour tout $x \in \mathbb{Z}/9\mathbb{Z}$, on a $(-x)^4 = x^4$:

$\widehat{0}^4 = \widehat{0}$, $\widehat{1}^4 = \widehat{1}$, $\widehat{2}^4 = \widehat{16} = -\widehat{2}$,

$\widehat{3}^4 = \widehat{9}^2 = \widehat{0}^2 = \widehat{0}$, $\widehat{4}^4 = \widehat{16}^2 = (-\widehat{2})^2 = \widehat{4}$.

On conclut : $\mathcal{S} = \{-\widehat{4}, \widehat{4}\}$.

Méthode

Pour manipuler l'indicateur d'Euler φ

Essayer d'utiliser :

- la définition : pour tout $n \in \mathbb{N}^*$, $\varphi(n)$ est le nombre d'entiers compris entre 1 et n et premiers avec n
- la formule $\varphi(n) = n\prod_{i=1}^{N}\left(1-\frac{1}{p_i}\right)$ si n admet la décomposition primaire $n = \prod_{i=1}^{N} p_i^{r_i}$.

➟ **Exercice 2.11**

Exemple

Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$.

Combien y a-t-il d'éléments inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$?

D'après le cours, les éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont les classes modulo n des entiers compris entre 1 et n et premiers avec n, donc il y en a $\varphi(n)$.

Exemple

Résoudre l'équation

$$\varphi(n) = \frac{n}{3},$$

d'inconnue $n \in \mathbb{N}^*$.

1) Soit n convenant. Notons $n = \prod_{i=1}^{N} p_i^{r_i}$ la décomposition primaire de n.

D'après le cours, on a : $\varphi(n) = n\prod_{i=1}^{N}\left(1-\frac{1}{p_i}\right)$.

Puisque $\varphi(n) = \frac{n}{3}$, on déduit $3\prod_{i=1}^{N}(p_i-1) = \prod_{i=1}^{N} p_i$.

On a alors : $3 \,\Big|\, \prod_{i=1}^{N} p_i$.

Quitte à renuméroter les p_i, on peut supposer $p_1 = 3$.

On a alors : $3\cdot 2\cdot\prod_{i=2}^{N}(p_i-1) = 3\prod_{i=2}^{N} p_i$, d'où : $2\prod_{i=2}^{N}(p_i-1) = \prod_{i=2}^{N} p_i$.

Il en résulte : $2 \,\Big|\, \prod_{i=2}^{N} p_i$.

Quitte à renuméroter les p_i, on peut supposer $p_2 = 2$.

On a alors : $\prod_{i=3}^{N}(p_i-1) = \prod_{i=3}^{N} p_i$.

Si $N \geqslant 3$, alors, comme : $\forall i \in \{3,\dots,N\},\ \ p_i - 1 < p_i$,
on déduit une contradiction. Il en résulte $N \leqslant 2$, donc : $n = 3^{r_1}2^{r_2}$.

2) Réciproquement, pour tout $(r_1, r_2) \in (\mathbb{N}^*)^2$, on a :

$$\varphi(3^{r_1}2^{r_2}) = n\Big(1-\frac{1}{3}\Big)\Big(1-\frac{1}{2}\Big) = \frac{n}{3}.$$

On conclut : $\mathcal{S} = \left\{3^a 2^b\,;\,(a,b)\in(\mathbb{N}^*)^2\right\}$.

Vrai ou Faux ?

2.1 L'ensemble $C^\infty(\mathbb{R},\mathbb{R})$ est un anneau pour les lois usuelles, addition et multiplication. V F

2.2 Si un anneau A vérifie : $\forall a \in A,\ \ (a-1)a(a+1)=0$,
alors A admet au plus trois éléments, qui sont -1, 0, 1. V F

2.3 Pour tout $n \in \mathbb{N}^*$, l'ensemble $\mathbf{T}_{n,\mathrm{s}}(\mathbb{R})$ des matrices triangulaires supérieures de $\mathbf{M}_n(\mathbb{R})$ est un sous-anneau de $\mathbf{M}_n(\mathbb{R})$. V F

2.4 Dans l'anneau $A = C([0\,;1],\mathbb{R})$, la partie $I = \{f \in A\,;\, f(0) = f(1)\}$ est un idéal de A. V F

2.5 L'ensemble I des suites réelles convergeant vers 0 est un sous-anneau de l'ensemble A des suites réelles convergentes. V F

2.6 Les anneaux $\mathbb{R}[X]$ et $\mathbb{C}[X]$ sont isomorphes. V F

2.7 La somme de deux idéaux I, J d'un anneau (commutatif) est un idéal de A. V F

2.8 Pour tout $n \in \mathbb{N}^*$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est un nombre premier. V F

2.9 L'indicateur d'Euler φ vérifie la formule : $\forall (a,b) \in (\mathbb{N}^*)^2,\ \ \varphi(ab) = \varphi(a)\varphi(b)$. V F

2.10 Le corps $\mathbb{R}$ n'a que deux sous-corps, et ceux-ci sont $\mathbb{R}$ et $\mathbb{Q}$. V F

Énoncés des exercices

2.1 Centre d'un anneau

Soit A un anneau.
Montrer que le *centre* Z de A, défini par : $Z = \big\{x \in A\,;\, \forall a \in A,\ \ ax = xa\big\}$,
est un sous-anneau de A.

2.2 Sous-anneau, idéal : exemples dans un anneau de fonctions

On note

$$A = C([0\,;1],\mathbb{R}),\ B = C^1([0\,;1],\mathbb{R}),\ I = \{f \in A\,;\, f(0) = 0\},\ E = B \cap I.$$

Vérifier :

a) A est un anneau pour les lois usuelles

b) B est un sous-anneau de A, et B n'est pas un idéal de A

c) I est un idéal de A, et I n'est pas un sous-anneau de A

d) E n'est ni un sous-anneau ni un idéal de A.

2.3 Exemples de systèmes de congruences simultanées, à une inconnue

Résoudre les systèmes d'équations suivants, d'inconnue $x \in \mathbb{Z}$:

$$a)\ \begin{cases} x \equiv 1 \ \ [2] \\ x \equiv 2 \ \ [3] \\ x \equiv 3 \ \ [5] \end{cases} \qquad b)\ \begin{cases} x \equiv 1 \ \ [6] \\ x \equiv 4 \ \ [10] \\ x \equiv 7 \ \ [15] \end{cases} \qquad c)\ \begin{cases} x \equiv 7 \ \ [18] \\ x \equiv 1 \ \ [30] \\ x \equiv 16 \ \ [45]. \end{cases}$$

2.4 Exemples de systèmes d'équations dans $\mathbb{Z}/n\mathbb{Z}$

Résoudre les systèmes d'équations suivants, d'inconnue $(x, y) \in \big(\mathbb{Z}/n\mathbb{Z}\big)^2$:

$$a)\ \begin{cases} \widehat{2}\,x + \widehat{3}\,y = \widehat{4} \\ \widehat{3}\,x + \widehat{2}\,y = \widehat{5} \end{cases} \text{ avec } n = 13 \qquad b)\ \begin{cases} \widehat{4}\,x + \widehat{7}\,y = \widehat{1} \\ \widehat{5}\,x + \widehat{2}\,y = \widehat{2} \end{cases} \text{ avec } n = 18 \qquad c)\ \begin{cases} \widehat{3}\,x + \widehat{10}\,y = \widehat{9} \\ \widehat{15}\,x + \widehat{4}\,y = \widehat{9} \end{cases} \text{ avec } n = 60.$$

2.5 Étude d'inversibilité dans un anneau vérifiant une condition d'intégrité

Soit $(A, +, \times)$ un anneau tel que : $\forall (x, y) \in A^2,\ \ \big(xy = 0 \implies (x = 0 \quad \text{ou} \quad y = 0)\big)$.
Soit $(a, b) \in A^2$ tel que $ab = 1$. Montrer : $ba = 1$.

2.6 Produits de diviseurs de 0

Soit A un anneau commutatif.

On note $D = \{x \in A \setminus \{0\} \,;\, \exists\, y \in A \setminus \{0\},\ xy = 0\}$ l'ensemble des diviseurs de 0 dans A. Montrer, pour tout $(a, b) \in A^2$:

a) $ab \in D \implies (a \in D \text{ ou } b \in D)$

b) $(a \in D \text{ ou } b \in D) \implies ab \in D \cup \{0\}$.

2.7 Morphisme des groupes d'inversibles induit par un morphisme d'anneaux

Soient A, B deux anneaux, A^* (resp. B^*) l'ensemble des éléments inversibles de A (resp. B), $f : A \longrightarrow B$ un morphisme d'anneaux.

a) Montrer : $f(A^*) \subset B^*$.

b) Établir que l'application $f^* : A^* \longrightarrow B^*,\ x \longmapsto f(x)$ est un morphisme de groupes (pour les lois $\cdot$ de A et de B).

2.8 Image réciproque d'un sous-anneau par un morphisme d'anneaux, noyau

Soient A, B des anneaux commutatifs, $f : A \longrightarrow B$ un morphisme d'anneaux, C un sous-anneau de B.

a) Montrer que $f^{-1}(C)$ est un sous-anneau de A.

b) Montrer que le noyau de f, $\mathrm{Ker}\,(f) = f^{-1}(\{0\})$, est un idéal de l'anneau $f^{-1}(C)$.

2.9 Exemple d'idéal d'un anneau de suites

On note A l'ensemble des suites réelles bornées et I l'ensemble des suites réelles convergeant vers 0.

a) Vérifier que A est un anneau pour les lois usuelles et que I est un idéal de A.

b) 1) Est-ce que I est principal, c'est-à-dire est-ce qu'il existe $u \in A$ tel que :

$$I = \{uv \,;\, v \in A\} \ ?$$

2) Est-ce que I est premier, c'est-à-dire est-ce que :

$$\forall (u, v) \in I^2,\ \Big(uv \in I \implies (u \in I \text{ ou } v \in I)\Big) \ ?$$

3) Est-ce que I est maximal, c'est-à-dire est-ce qu'il n'existe pas d'idéal J de A tel que : $I \subsetneqq J \subsetneqq A$?

c) Déterminer le radical $\sqrt{I}$ de I, défini par : $\sqrt{I} = \{u \in A \,;\, \exists\, p \in \mathbb{N}^*,\ u^p \in I\}$.

2.10 Exemples de résolution d'équation algébrique dans $\mathbb{Z}/12\,\mathbb{Z}$

Résoudre l'équation, d'inconnue $x \in \mathbb{Z}/12\mathbb{Z}$: $x^6(x - \widehat{4})^7 = \widehat{1}$.

2.11 Exemple d'utilisation du théorème d'Euler

Soit $a \in \mathbb{N}$, non multiple de 3 et tel que $a \geqslant 4$. Montrer : $a \mid 3(a-3)^{\varphi(a)-1} + 1$.