j'intègre

MÉTHODES ET EXERCICES

MP | MP*

Jean-Marie **Monier**
Guillaume **Haberer**
Cécile **Lardon**

Mathématiques
méthodes et exercices

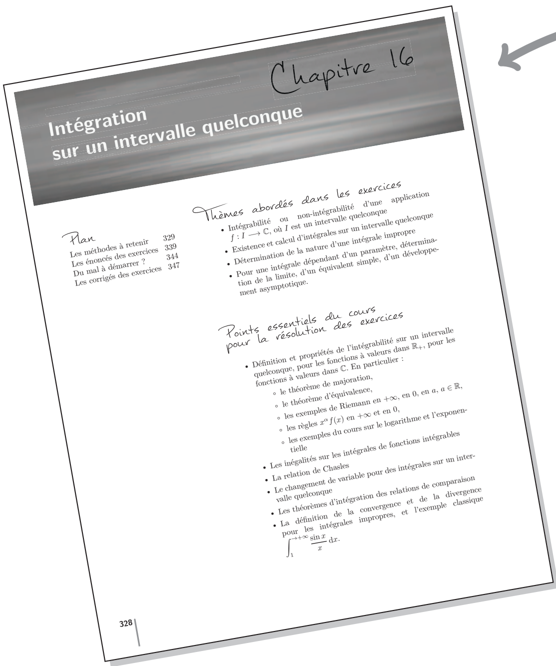
DUNOD

Conception et création de couverture : Atelier 3+

5 rue Laromiguière, 75005 Paris
www.dunod.com

ISBN 978-2-10-071368-4

Pour bien utiliser cet ouvrage



Chapitre 16

Intégration sur un intervalle quelconque

Plan

Les méthodes à retenir 329
Les énoncés des exercices 339
Du mal à démarrer ? 344
Les corrigés des exercices 347

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 impropre
- Pour une intégrale dépendant d'un paramètre, détermination de la limite, d'un équivalent simple, d'un développement asymptotique.

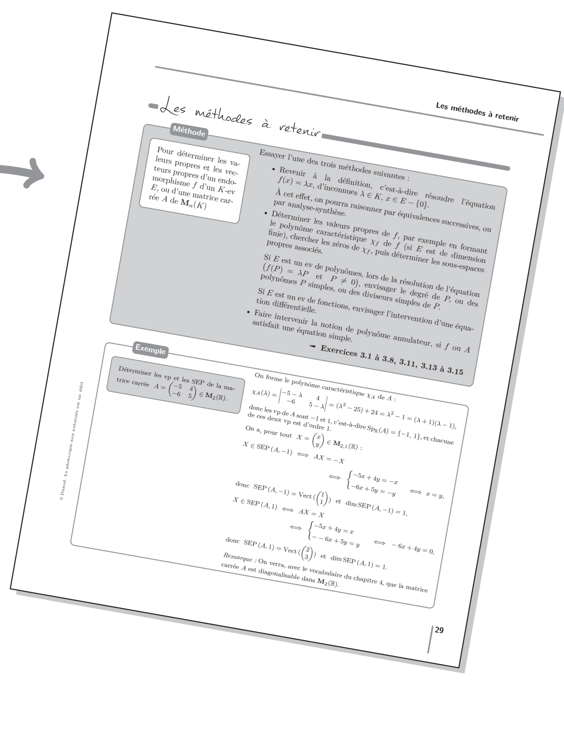
Points essentiels du cours pour la résolution des exercices

- 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 impropres, et l'exemple classique $\int_1^{+\infty} \frac{\sin x}{x}\,dx$.

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 déterminer les valeurs propres et les vecteurs propres d'un endomorphisme f d'un K-ev E, ou d'une matrice carrée A de $\mathbf{M}_n(K)$

Essayer l'une des trois méthodes suivantes :

- Revenir à la définition, c'est-à-dire résoudre l'équation $f(x) = \lambda x$, d'inconnues $\lambda \in K$, $x \in E - \{0\}$. À cet effet, on pourra raisonner par équivalences successives, ou par analyse-synthèse.
- Déterminer les valeurs propres de f, par exemple en formant le polynôme caractéristique χ_f de f (si E est de dimension finie), chercher les zéros de χ_f, puis déterminer les sous-espaces propres associés.

Si E est un ev de polynômes, lors de la résolution de l'équation $(f(P) = \lambda P$ et $P \neq 0)$, envisager le degré de P, ou des polynômes P simples, ou des diviseurs simples de P.

Si E est un ev de fonctions, envisager l'intervention d'une équation différentielle.

- Faire intervenir la notion de polynôme annulateur, si f ou A satisfait une équation simple.

➥ Exercices 3.1 à 3.8, 3.11, 3.13 à 3.15

Exemple

Déterminer les vp et les SEP de la matrice carrée $A = \begin{pmatrix} -5 & 4 \\ -6 & 5 \end{pmatrix} \in \mathbf{M}_2(\mathbb{R})$.

On forme le polynôme caractéristique χ_A de A :

$\chi_A(\lambda) = \begin{vmatrix} -5-\lambda & 4 \\ -6 & 5-\lambda \end{vmatrix} = (\lambda^2 - 25) + 24 = \lambda^2 - 1 = (\lambda+1)(\lambda-1)$,

donc les vp de A sont -1 et 1, c'est-à-dire $\mathrm{Sp}_{\mathbb{R}}(A) = \{-1, 1\}$, et chacune de ces deux vp est d'ordre 1.

On a, pour tout $X = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{M}_{2,1}(\mathbb{R})$:

$X \in \mathrm{SEP}(A, -1) \iff AX = -X \iff \begin{cases} -5x + 4y = -x \\ -6x + 5y = -y \end{cases} \iff x = y$,

donc $\mathrm{SEP}(A, -1) = \mathrm{Vect}\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right)$ et $\dim \mathrm{SEP}(A, -1) = 1$,

$X \in \mathrm{SEP}(A, 1) \iff AX = X \iff \begin{cases} -5x + 4y = x \\ -6x + 5y = y \end{cases} \iff -6x + 4y = 0$,

donc $\mathrm{SEP}(A, 1) = \mathrm{Vect}\left(\begin{pmatrix} 2 \\ 3 \end{pmatrix}\right)$ et $\dim \mathrm{SEP}(A, 1) = 1$.

Remarque : On verra, avec le vocabulaire du chapitre 4, que la matrice carrée A est diagonalisable dans $\mathbf{M}_2(\mathbb{R})$.

© Dunod. La photocopie non autorisée est un délit.

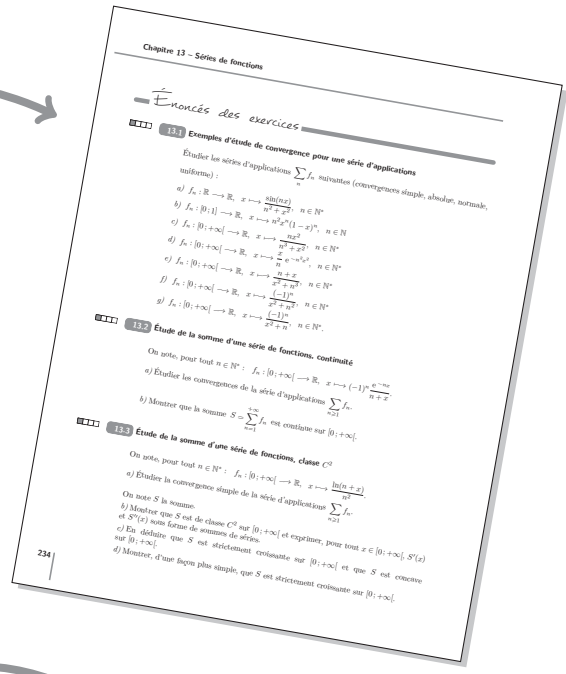
29

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.

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.


Chapitre 13 – Séries de fonctions

Énoncés des exercices

13.1 Exemples d'étude de convergence pour une série d'applications

Étudier les séries d'applications $\sum_n f_n$ suivantes (convergences simple, absolue, normale, uniforme) :

a) $f_n : \mathbb{R} \longrightarrow \mathbb{R},\ x \longmapsto \frac{\sin(nx)}{n^2+x^2},\ n \in \mathbb{N}^*$

b) $f_n : [0;1] \longrightarrow \mathbb{R},\ x \longmapsto n^2x^n(1-x)^n,\ n \in \mathbb{N}$

c) $f_n : [0;+\infty[\longrightarrow \mathbb{R},\ x \longmapsto \frac{nx^2}{n^3+x^3},\ n \in \mathbb{N}^*$

d) $f_n : [0;+\infty[\longrightarrow \mathbb{R},\ x \longmapsto \frac{x}{n}\,e^{-n^2x^2},\ n \in \mathbb{N}^*$

e) $f_n : [0;+\infty[\longrightarrow \mathbb{R},\ x \longmapsto \frac{n+x}{x^2+n^3},\ n \in \mathbb{N}^*$

f) $f_n : [0;+\infty[\longrightarrow \mathbb{R},\ x \longmapsto \frac{(-1)^n}{x^2+n^2},\ n \in \mathbb{N}^*$

g) $f_n : [0;+\infty[\longrightarrow \mathbb{R},\ x \longmapsto \frac{(-1)^n}{x^2+n},\ n \in \mathbb{N}^*$.

13.2 Étude de la somme d'une série de fonctions, continuité

On note, pour tout $n \in \mathbb{N}^*$: $f_n : [0;+\infty[\longrightarrow \mathbb{R},\ x \longmapsto (-1)^n \frac{e^{-nx}}{n+x}$.

a) Étudier les convergences de la série d'applications $\sum_{n\geqslant 1} f_n$.

b) Montrer que la somme $S = \sum_{n=1}^{+\infty} f_n$ est continue sur $[0;+\infty[$.

13.3 Étude de la somme d'une série de fonctions, classe C^2

On note, pour tout $n \in \mathbb{N}^*$: $f_n : [0;+\infty[\longrightarrow \mathbb{R},\ x \longmapsto \frac{\ln(n+x)}{n^2}$.

a) Étudier la convergence simple de la série d'applications $\sum_{n\geqslant 1} f_n$.

On note S la somme.

b) Montrer que S est de classe C^2 sur $[0;+\infty[$ et exprimer, pour tout $x \in [0;+\infty[$, $S'(x)$ et $S''(x)$ sous forme de sommes de séries.

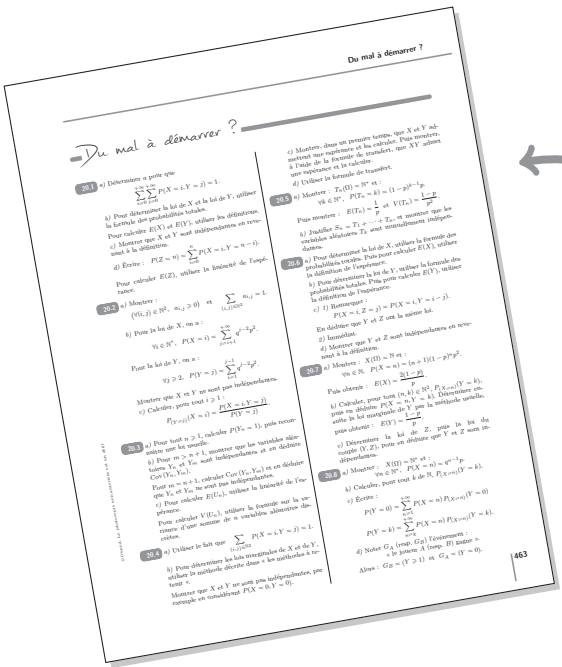
c) En déduire que S est strictement croissante sur $[0;+\infty[$ et que S est concave sur $[0;+\infty[$.

d) Montrer, d'une façon plus simple, que S est strictement croissante sur $[0;+\infty[$.

234

Du mal à démarrer ?

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


Du mal à démarrer ?

20.1 a) Déterminer a priori cette somme :

$$\sum_{i=0}^{+\infty}\sum_{j=0}^{+\infty} P(X=i,Y=j) = 1.$$

b) Pour déterminer la loi de X et la loi de Y, utiliser la formule des probabilités totales.

Pour calculer $E(X)$ et $E(Y)$, utiliser les définitions.

c) Montrer que X et Y sont indépendantes en revenant à la définition.

d) Écrire : $P(Z=n) = \sum_{i=0}^{n} P(X=i, Y=n-i)$.

Pour calculer $E(Z)$, utiliser la linéarité de l'espérance.

20.2 a) Montrer :

$$\forall (i,j) \in \mathbb{N}^2,\ a_{i,j} \geqslant 0 \quad \text{et} \quad \sum_{(i,j)\in\mathbb{N}^2} a_{i,j} = 1.$$

b) Poser la loi de X, on a :

$$\forall i \in \mathbb{N}^*,\ P(X=i) = \sum_{j=i+1}^{+\infty} q^{j-2}p^2.$$

Pour la loi de Y, on a :

$$\forall j \geqslant 2,\ P(Y=j) = \sum_{i=1}^{j-1} q^{j-2}p^2.$$

Montrer que X et Y ne sont pas indépendantes.

c) Calculer, pour tout $i \geqslant 1$:

$$P_{(Y=j)}(X=i) = \frac{P(X=i,Y=j)}{P(Y=j)}.$$

20.3 a) Pour tout $n \geqslant 1$, calculer $P(Y_n=1)$, puis reconnaître une loi usuelle.

b) Pour $m \geqslant n+1$, montrer que les variables aléatoires Y_n et Y_m sont indépendantes et en déduire $\mathrm{Cov}(Y_n, Y_m)$.

Pour $m = n+1$, calculer $\mathrm{Cov}(Y_n, Y_m)$ et en déduire que Y_n et Y_m ne sont pas indépendantes.

c) Pour calculer $E(U_n)$, utiliser la linéarité de l'espérance.

Puis calculer $V(U_n)$, utiliser la formule sur la variance d'une somme de n variables aléatoires deux à deux.

20.4 a) Utiliser le fait que $\sum_{(i,j)\in\mathbb{N}^2} P(X=i,Y=j) = 1$.

b) Poser déterminer les lois marginales de X et de Y, utiliser la méthode décrite dans « les méthodes à retenir ».

Montrer que X et Y ne sont pas indépendantes, par exemple en remarquant $P(X=0,Y=0)$.

c) Montrer, dans un premier temps, que X et Y admettent une espérance et les calculer. Puis montrer, à l'aide de la formule de transfert, que XY admet une espérance et la calculer.

d) Utiliser la formule de transfert.

20.5 a) Montrer : $T_1(\Omega) = \mathbb{N}^*$ et :

$$\forall k \in \mathbb{N}^*,\ P(T_1=k) = (1-p)^{k-1}p.$$

Puis montrer : $E(T_1) = \frac{1}{p}$ et $V(T_1) = \frac{1-p}{p^2}$.

b) Justifier $S_n = T_1 + \cdots + T_n$ et montrer que les variables aléatoires T_k sont mutuellement indépendantes.

20.6 a) Pour déterminer la loi de X, utiliser la formule des probabilités totales. Puis pour calculer $E(X)$, utiliser la définition de l'espérance.

b) Poser déterminer la loi de Y, utiliser la formule des probabilités totales. Puis pour calculer $E(Y)$, utiliser la définition de l'espérance.

c) 1) Remarquer :

$$P(X=i, Z=j) = P(X=i, Y=i-j).$$

En déduire que Y et Z ont la même loi.

2) Immédiat.

d) Montrer que Y et Z sont indépendantes en revenant à la définition.

20.7 a) Montrer : $X(\Omega) = \mathbb{N}$ et :

$$\forall n \in \mathbb{N},\ P(X=n) = (n+1)(1-p)^n p^2.$$

Puis obtenir : $E(X) = \frac{2(1-p)}{p}$.

b) Calculer, pour tout $(n,k) \in \mathbb{N}^2$, $P_{(X=n)}(Y=k)$, puis en déduire $P(X=n, Y=k)$. Déterminer ensuite la loi marginale de Y par la méthode usuelle, puis obtenir : $E(Y) = \frac{1-p}{p}$.

c) Déterminer la loi de Z, puis la loi du couple (X,Z), puis en déduire que Y et Z sont indépendantes.

20.8 a) Montrer : $X(\Omega) = \mathbb{N}^*$ et :

$$\forall n \in \mathbb{N}^*,\ P(X=n) = q^{n-1}p.$$

b) Calculer, pour tout k de $\mathbb{N}$, $P_{(X=n)}(Y=k)$.

c) Écrire :

$$P(Y=0) = \sum_{n=1}^{+\infty} P(X=n)\,P_{(X=n)}(Y=0)$$

$$P(Y=k) = \sum_{n=k}^{+\infty} P(X=n)\,P_{(X=n)}(Y=k).$$

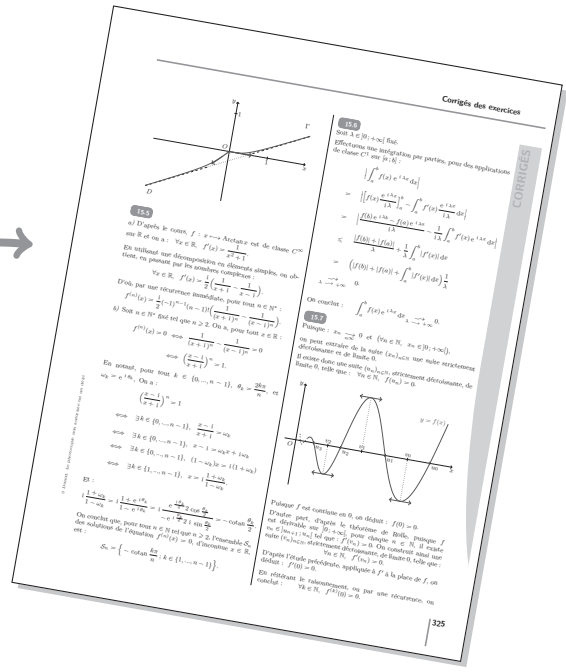
d) Noter G_A (resp. G_B) l'événement : « le jeteur A (resp. B) gagne ».

Alors : $G_B = (Y \geqslant 1)$ et $G_A = (Y=0)$.

463

Corrigés des exercices

Tous les exercices sont corrigés de façon détaillée.


Corrigés des exercices

CORRIGÉS

15.5

15.6

15.7

325

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, Cyril Haberer, Sylvain Delpech, Hermin Durand, Viviane Gaggioli, Marguerite Gauthier, Hadrien Larôme, Paul Pichaureau, Nathalie Planche, Philippe Saadé, Marie-Dominique Siéfert, Marie-Pascale Thon, Audrey Verdier, Skander Zannad.

Chapitre 1

Groupes

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**

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, e son neutre, $a,\, b \in G$ tels que : $ab = b^2a$.

Montrer : $a^3b = b^8a^3$.

Calculons a^3b en faisant passer les b vers la gauche de l'écriture, par étapes successives :

$$\begin{aligned} a^3b &= a^2(ab) = a^2(b^2a) = a(ab)ba = a(b^2a)ba = ab^2(ab)a \\ &= ab^2(b^2a)a = (ab)b^3a^2 = (b^2a)(b^3a^2) = b^2(ab)b^2a^2 = b^2(b^2a)b^2a^2 \\ &= b^4(ab)ba^2 = b^4(b^2a)ba^2 = b^6(ab)a^2 = b^6(b^2a)a^2 = b^8a^3. \end{aligned}$$

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 $(x,y) \in G^2$:

$$\begin{aligned} f(xy) = (xy)^2 &= (xy)(xy) = x(yx)y \\ &= x(xy)y = (xx)(yy) = x^2y^2 = f(x)f(y), \end{aligned}$$

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 : $2f\Big(\dfrac{a}{2}\Big) = f\Big(\dfrac{a}{2}\Big) + f\Big(\dfrac{a}{2}\Big) = f\Big(\dfrac{a}{2} + \dfrac{a}{2}\Big) = f(a) = 1,$

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

Énoncés des exercices

1.1 Calculs dans un groupe

Soient G un groupe, e son neutre, $a, b \in G$ tels que : $a^3 b = ba^3$ et $a^5 = e$.
Montrer : $ab = ba$.

1.2 Calculs de puissances dans un groupe

Soient G un groupe, $a, b \in G$, $n \in \mathbb{N}^*$ tels que : $b^n a = ab$.

a) Montrer : $\forall k \in \mathbb{N}, \quad b^{kn} a = ab^k$.

b) En déduire : $\forall p \in \mathbb{N}, \quad b^{n^p} a^p = a^p b$.

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

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 :

$$x^2 = e, \quad y^2 = e, \quad xy = yx, \quad x \neq e, \quad y \neq e, \quad x \neq y, \quad xy \neq e.$$

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 $\big(\forall (x, y) \in A^2, \quad xy \in A\big)$.

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, $n \in \mathbb{N} - \{0,1\}$.

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

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

1.11 Condition suffisante pour qu'un groupe fini soit abélien

Soient G un groupe fini, e le neutre de G. On suppose qu'il existe un endomorphisme de groupes $f : G \longrightarrow G$ tel que : $\begin{cases} \forall t \in G, \quad f \circ f(t) = t \\ \forall u \in G, \quad \big(f(u) = u \implies u = e\big). \end{cases}$

a) Montrer : $\forall x \in G, \ \exists\, t \in G, \quad x = t\big(f(t)\big)^{-1}$.

b) En déduire : $\forall x \in G, \quad f(x) = x^{-1}$.

c) Montrer que G est abélien.

1.12 Sous-groupes d'un groupe infini

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

1.13 Morphismes de groupes de $\mathbb{Z}/a\mathbb{Z}$ dans $\mathbb{Z}/b\mathbb{Z}$

On fixe $(a,b) \in (\mathbb{N}^*)^2$.

Déterminer tous les morphismes de groupes de $\big(\mathbb{Z}/a\mathbb{Z},+\big)$ dans $\big(\mathbb{Z}/b\mathbb{Z},+\big)$.

Du mal à démarrer ?

1.1 Calculer, par exemple : $ab = a^5(ab) = \dots$

1.2 *a)* Récurrence sur k.

b) Récurrence sur p, en utilisant le résultat de *a)* pour transformer $b^{n^p}a$ en ab^{n^p}.

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 $G \longrightarrow G$, $g \longmapsto g_0 g$ 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 *a)* Considérer l'application

$$g : G \longrightarrow G, \quad t \longmapsto t\big(f(t)\big)^{-1}.$$

Montrer que g est injective, et en déduire que g est surjective.

b) Soit $x \in G$. Utiliser *a)* et calculer $f(x)$.

c) Utiliser *b)*.

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 Pour $x \in \mathbb{Z}$ (resp. $y \in \mathbb{Z}$), noter $\widehat{x}$ (resp. $\widehat{y}$) la classe de x (resp. y) dans $\mathbb{Z}/a\mathbb{Z}$ (resp. $\mathbb{Z}/b\mathbb{Z}$).

• Soit $f : \mathbb{Z}/a\mathbb{Z} \longrightarrow \mathbb{Z}/b\mathbb{Z}$ un morphisme de groupes.

Montrer : $\forall x \in \mathbb{Z}, \quad f(\widehat{x}) = x f\big(\widehat{1}\big)$

et considérer $\xi \in \{0, ..., b-1\}$ tel que $f\big(\widehat{1}\big) = \widetilde{\xi}$.

Montrer que ξ est multiple de $\dfrac{b}{\delta}$ où on a noté

$$\delta = \mathrm{pgcd}\,(a, b).$$

• Réciproquement, soit ξ un multiple de $\dfrac{b}{\delta}$.

Montrer :

$$\forall x_1, x_2 \in \mathbb{Z}, \quad \big(\widehat{x_1} = \widehat{x_2} \implies \widetilde{\xi x_1} = \widetilde{\xi x_2}\big).$$

Considérer alors $f : \mathbb{Z}/a\mathbb{Z} \longrightarrow \mathbb{Z}/b\mathbb{Z}$, $\widehat{x} \longmapsto \widetilde{\xi x}$

et montrer que f est un morphisme de groupes.

Corrigés des exercices

1.1

On a :

$$ab = a^5(ab) = a^6b = a^3(a^3b) = a^3(ba^3)$$
$$= (a^3b)a^3 = (ba^3)a^3 = ba^6 = (ba)a^5 = ba.$$

1.2

a) Récurrence sur k.

- La propriété est évidente pour $k = 0$.
- Supposons, pour $k \in \mathbb{N}$ fixé : $b^{kn}a = ab^k$. Alors :

$$b^{(k+1)n}a = b^{kn}(b^n a) = b^{kn}(ab)$$
$$= (b^{kn}a)b = (ab^k)b = ab^{k+1},$$

donc la propriété est vraie pour $k+1$.

On conclut, par récurrence sur k : $\forall k \in \mathbb{N}, \quad b^{kn}a = ab^k$.

b) Récurrence sur p.

- La propriété est évidente pour $p = 0$.
- Supposons, pour $p \in \mathbb{N}$ fixé : $b^{n^p}a^p = a^pb$. Alors :

$$b^{n^{p+1}}a^{p+1} = (b^{n^p n}a)a^p \underset{a)}{=} (ab^{n^p})a^p$$
$$= a(b^{n^p}a^p) = a(a^pb) = a^{p+1}b,$$

donc la propriété est vraie pour $p+1$.

On conclut, par récurrence sur p : $\forall p \in \mathbb{N}, \quad b^{n^p}a = a^pb$.

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 : $\quad H = \{e, x, y, xy\}$ 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 : $\big(\underbrace{1 - \varphi(g_0)}_{\neq 0}\big) \sum_{g \in G} \varphi(g) = 0,$

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 : $x - h \in \operatorname{Ker}(f)$.

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

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

2) Réciproquement, soit $x \in H + \operatorname{Ker}(f)$.

Il existe $h \in H$, $u \in \operatorname{Ker}(f)$ 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 : $H + \operatorname{Ker}(f) \subset f^{-1}\big(f(H)\big)$.

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

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 $\operatorname{Im}(f)$: $y = f(x) \in \operatorname{Im}(f)$.

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

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

2) Réciproquement, soit $y \in H' \cap \operatorname{Im}(f)$.

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 : $H' \cap \operatorname{Im}(f) \subset f\big(f^{-1}(H')\big)$.

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

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 :

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

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

a) Considérons l'application $g : G \longrightarrow G, \ \ t \longmapsto t\big(f(t)\big)^{-1}$.

- Montrons que g est injective.

Soit $(t, u) \in G^2$ tel que $g(t) = g(u)$. On, a alors :

$$t\big(f(t)\big)^{-1} = u\big(f(u)\big)^{-1},$$

d'où, en composant à gauche par u^{-1} et à droite par $f(t)$:

$$u^{-1}t = \big(f(u)\big)^{-1}f(t) = f(u^{-1}t),$$

puisque f est un endomorphisme du groupe G.

D'après l'hypothèse, il s'ensuit : $u^{-1}t = e, \ u = t$.

Ceci établit que g est injective.

- Puisque $g : G \longrightarrow G$ est injective et que G est fini, g est surjective.

On conclut : $\forall x \in G,\ \exists\, t \in G,\quad x = t\big(f(t)\big)^{-1}$.

b) Soit $x \in G$.

D'après *a)*, il existe $t \in G$ tel que $x = t\big(f(t)\big)^{-1}$.

On a :

$$f(x) = f\big(t\big(f(t)\big)^{-1}\big) = f(t)f\big(\big(f(t)\big)^{-1}\big)$$
$$= f(t)t^{-1} = \big(t\big(f(t)\big)^{-1}\big)^{-1} = x^{-1}.$$

c) Soit $(x, y) \in G^2$. On a, en utilisant le résultat de *b)* appliqué à xy, à x, à y :

$$xy = \big((xy)^{-1}\big)^{-1} = \big(f(xy)\big)^{-1} = \big(f(x)f(y)\big)^{-1}$$
$$= \big(f(y)\big)^{-1}\big(f(x)\big)^{-1} = (y^{-1})^{-1}(x^{-1})^{-1} = yx.$$

On conclut : G est abélien.

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

Pour $x \in \mathbb{Z}$, notons $\widehat{x}$ la classe de x dans $\mathbb{Z}/a\mathbb{Z}$ et pour $y \in \mathbb{Z}$, notons $\widetilde{y}$ la classe de y dans $\mathbb{Z}/b\mathbb{Z}$

- Soit $f : \mathbb{Z}/a\mathbb{Z} \longrightarrow \mathbb{Z}/b\mathbb{Z}$ un morphisme de groupes.

Puisque $\mathbb{Z}/a\mathbb{Z}$ est monogène, engendré par $\widehat{1}$, f est entièrement déterminé par la donnée de $f(\widehat{1})$, et on a alors :

$$\forall x \in \mathbb{Z},\quad f(\widehat{x}) = x\, f(\widehat{1}).$$

Il existe $\xi \in \{0, ..., n-1\}$ tel que $f(\widehat{1}) = \widetilde{\xi}$.

On a : $\widetilde{a\xi} = a\,\widetilde{\xi} = a\, f(\widehat{1}) = f(a\,\widehat{1}) = f(\widehat{a}) = f(\widehat{0}) = \widetilde{0}$,

d'où : $b \mid a\xi$.

Notons $\delta = a \wedge b$.

Il existe alors $(a',\, b') \in \mathbb{N}^{*\,2}$ tel que :

$$a = \delta a',\quad b = \delta b',\quad a' \wedge b' = 1.$$

On a : $b \mid a\xi \iff \delta b' \mid \delta a'\xi \iff b' \mid a'\xi \iff b' \mid \xi$,

en utilisant le théorème de Gauss.

Ainsi, si $f : \mathbb{Z}/a\mathbb{Z} \longrightarrow \mathbb{Z}/b\mathbb{Z}$ est un morphisme de groupes, alors $f(\widehat{1}) = \widetilde{\xi}$, où ξ est un multiple de $\dfrac{b}{\delta}$.

- Réciproquement, soit ξ un multiple de $\dfrac{b}{\delta}$.

Soient $x, x' \in \mathbb{Z}$ tels que $\widehat{x} = \widehat{x'}$.
On a alors : $a \mid x - x'$, donc $\xi\delta a' = \xi a \mid (\xi x - \xi x')$.

Comme $b \mid \xi\delta$, on déduit $b \mid (\xi x - \xi x')$, c'est-à-dire $\widetilde{\xi x} = \widetilde{\xi x'}$.

On peut donc définir une application $f : \mathbb{Z}/a\mathbb{Z} \longrightarrow \mathbb{Z}/b\mathbb{Z}$ par :

$$\forall x \in \mathbb{Z},\quad f(\widehat{x}) = \widetilde{\xi x}.$$

L'application f ainsi définie est un morphisme de groupes, car, pour tout $(x, y) \in \mathbb{Z}^2$:

$$f(\widehat{x} + \widehat{y}) = f(\widehat{x + y}) = \xi\widetilde{(x + y)}$$
$$= \xi\widetilde{x + \xi y} = \widetilde{\xi x} + \widetilde{\xi y} = f(\widehat{x}) + f(\widehat{y}).$$

Finalement, les morphismes de groupes de $\mathbb{Z}/a\mathbb{Z}$ dans $\mathbb{Z}/b\mathbb{Z}$ sont les applications $\mathbb{Z}/a\mathbb{Z} \longrightarrow \mathbb{Z}/b\mathbb{Z},\ \ \widehat{x} \longmapsto \widetilde{\xi x}$,
où $\xi \in \{0, ..., b-1\}$ est un multiple de $\dfrac{b}{a \wedge b}$.

Il est clair que les morphismes ainsi obtenus sont deux à deux distincts et qu'il y en a $a \wedge b$.

Par exemple, les morphismes de $\mathbb{Z}/12\,\mathbb{Z}$ dans $\mathbb{Z}/18\,\mathbb{Z}$ sont les six applications $f_\xi : \widehat{x} \longrightarrow \widetilde{\xi x}$, où $\xi = 0,\ 3,\ 6,\ 9,\ 12,\ 15$.

Chapitre 2

Anneaux, arithmétique

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 :
$$\forall a \in A, \quad a^3 = a^2.$$
Montrer : $\forall a \in A, \quad a^2 = a$.

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'es-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 :
$$\forall (x, y) \in B^2, \quad x + y \in B, \ -x \in B, \ xy \in B.$$

➟ **Exercices 2.1, 2.2, 2.12, 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, 2.13**

Exemple

On note $A = C([0\,;1], \mathbb{R})$ et :
$$I = \big\{ f \in A \,;\, f(1) = 0 \big\}.$$
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.

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 $(s, y) \in \left(\mathbb{Z}/7\mathbb{Z}\right)^2$:

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

Comme $2 \wedge 7 = 1$, $\widehat{2}$ est inversible dans $\mathbb{Z}/7\mathbb{Z}$.
De plus, comme $2 \cdot 4 = 8 \equiv 1 \ [7]$, on a : $\widehat{2} \cdot \widehat{4} = \widehat{1}$.
Ainsi, dans la première équation de (S) :

$$\widehat{2}x + \widehat{3}y = \widehat{1} \iff \widehat{4}(\widehat{2}x + \widehat{3}y) = \widehat{4} \cdot \widehat{1}$$
$$\iff x + \widehat{12}y = \widehat{4} \iff x = \widehat{4} - \widehat{12}y = \widehat{4} + \widehat{2}y.$$

Puis, en reportant dans la deuxième équation de (S) :

$$\widehat{3}x + \widehat{5}y = \widehat{2} \iff \widehat{3}(\widehat{4} + \widehat{2}y) + \widehat{5}y = \widehat{2}$$
$$\iff \widehat{11}y = -\widehat{10} \iff \widehat{4}y = \widehat{4}.$$

Comme $\widehat{4}$ est inversible dans $\mathbb{Z}/7\mathbb{Z}$, on a : $\widehat{4}y = \widehat{4} \iff \widehat{y} = \widehat{1}$.
Enfin : $x = \widehat{4} + \widehat{2}y = \widehat{4} + \widehat{2}\,\widehat{1} = \widehat{6} = -\widehat{1}$.
On conclut : $\mathcal{S} = \{(-\widehat{1}, \widehat{1})\}$.

On peut d'ailleurs contrôler que ce couple est bien une solution du système proposé.

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 $(-x)^4 = x^4$:

$$\widehat{0}^4 = \widehat{0}, \quad \widehat{1}^4 = \widehat{1}, \quad \widehat{2}^4 = \widehat{16} = -\widehat{2},$$
$$\widehat{3}^4 = \widehat{9}^2 = \widehat{0}^2 = \widehat{0}, \quad \widehat{4}^4 = \widehat{16}^2 = (-\widehat{2})^2 = \widehat{4}.$$

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

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 : $\forall i \in \{3,...,N\},\ \ p_i - 1 < p_i$,
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 :

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

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

Énoncés des exercices

2.1 Centre d'un anneau

Soit A un anneau.
Montrer que le *centre* Z de A, défini par : $Z = \{x \in A\,;\, \forall a \in A,\ \ ax = xa\}$, 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 $(x, y) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^2$:

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

2.5 Caractérisation des anneaux n'ayant que 0 comme élément nilpotent

Soient A un anneau, N l'ensemble des éléments nilpotents de A, c'est-à-dire :

$$N = \{x \in A\,;\, \exists\, n \in \mathbb{N}^*,\ \ x^n = 0\}.$$

Montrer que les deux propriétés suivantes sont équivalentes :

(i) $N = \{0\}$ (ii) $\forall x \in A,\ \ \left(x^2 = 0 \implies x = 0\right)$.

2.6 Produits de diviseurs de 0

Soit A un anneau commutatif.

On note $D = \{x \in A - \{0\} \,;\, \exists\, y \in A - \{0\},\ xy = 0\}$ 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 Correspondance entre idéaux par un morphisme d'anneaux surjectif

Soient A, A' deux anneaux commutatifs, $f : A \longrightarrow A'$ un morphisme d'anneaux surjectif. Montrer que l'application $\widetilde{f} : I \longmapsto f(I)$ (où $f(I)$ est l'image directe de I par f) est une bijection de l'ensemble $\mathcal{I}$ des idéaux de A contenant $\mathrm{Ker}\,(f)$ sur l'ensemble $\mathcal{I}'$ des idéaux de A'.

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 $\mathbb{Z}/13\,\mathbb{Z}$

Résoudre l'équation (1) d'inconnue $x \in \mathbb{Z}/13\mathbb{Z}$: $x^8 + 2x^6 + 3x^4 + 2x^2 + 1 = 0$.

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 : $a \mid 3(a-3)^{\varphi(a)-1} + 1$.

2.12 Sous-anneaux d'un anneau-produit

a) Montrer que, si A' (resp. B') est un sous-anneau d'un anneau A (resp. B), alors $A' \times B'$ est un sous-anneau de l'anneau-produit $A \times B$.

b) Montrer que les sous-anneaux de $\mathbb{Z}^2$ sont les $A_n = \{(x, y) \in \mathbb{Z}^2 \,;\, x \equiv y \ [n]\}$, pour $n \in \mathbb{N}$.

2.13 Idéaux d'un anneau-produit

Soient A, A' deux anneaux commutatifs. Trouver tous les idéaux de l'anneau-produit $A \times A'$ en fonction des idéaux de A et des idéaux de A'.

2.14 Anneaux $\mathbb{Z}^n$, $n \in \mathbb{N}^*$

Montrer que les anneaux $\mathbb{Z}^n$, $n \in \mathbb{N}^*$ sont deux à deux non isomorphes.

2.15 Exemple de divisibilité

CNS sur $(a, b) \in \mathbb{N}^2$ pour que : $\forall n \in \mathbb{N},\ \ 5 \mid 2^{an+b} + 3^n$.

2.16 Calcul de $\varphi(ab)$, où φ est l'indicateur d'Euler

a) Montrer : $\forall (a, b) \in (\mathbb{N}^*)^2,\ \ \varphi(ab)\varphi(a \wedge b) = (a \wedge b)\varphi(a)\varphi(b)$.

b) En déduire :

1) $\forall (a, b) \in (\mathbb{N}^*)^2,\ \ a \wedge b = 1 \implies \varphi(ab) = \varphi(a)\varphi(b)$

2) $\forall (a, b) \in (\mathbb{N}^*)^2,\ \ a \mid b \implies \varphi(ab) = a\varphi(b)$

3) $\forall (a, b) \in (\mathbb{N}^*)^2,\ \ \varphi(ab) = (a \wedge b)\varphi(a \vee b)$.

2.17 Centre d'un anneau régulier

Un anneau A est dit *régulier* si et seulement si : $\forall x \in A,\ \exists\, y \in A,\ \ xyx = x$.

On appelle *centre* d'un anneau A l'ensemble : $Z = \{x \in A \,;\, \forall a \in A,\ \ ax = xa\}$.

Démontrer que le centre d'un anneau régulier est un anneau régulier.

2.18 Anneaux intègres n'ayant qu'un nombre fini d'idéaux

Soit A un anneau (commutatif) intègre tel que $A \neq \{0\}$. On suppose que A n'a qu'un nombre fini d'idéaux. Démontrer que A est un corps.

Du mal à démarrer ?

2.1 Se rappeler la définition d'un sous-anneau. On dit qu'une partie B de A est un sous-anneau de A si et seulement si : $1_A \in B$ et

$$\forall (x,y) \in B^2,\ \big(x+y \in B,\ -x \in B,\ xy \in B\big).$$

2.2 *a)* Immédiat.

b) Utiliser la définition de : sous-anneau.

Raisonner par l'absurde, en utilisant la fonction constante 1 et une fonction continue non de classe C^1.

c) Utiliser la définition de : idéal.

Remarquer : $1 \notin I$.

d) Remarquer : $1 \notin E$.

Analogue à *b) 2)*.

2.3 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.

a) Par (1) : $x = 1+2a$, puis, par (2) : $a = -1+3b$, etc

b) Par (1) : $x = 1+6a$, puis, par (2), une contradiction.

c) Par (1) : $x = 7+18a$, puis, par (2) : $a = -2+5b$, et le report dans (3) donne une équation satisfaite pour tout $b \in \mathbb{Z}$.

2.4 *a)* Essayer, à partir d'une des deux équations, d'exprimer une inconnue en fonction de l'autre, puis reporter dans l'autre équation. Se rappeler qu'un élément $\widehat{x}$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si $x \wedge n = 1$.

b) Même méthode que pour *a)*.

c) Dans cet exemple, comme aucun coefficient de x ou y n'est premier avec 60, essayer d'éliminer x ou y par combinaison d'équations.

2.5 Un sens est évident.

Pour l'autre sens, si $a^n = 0$ et $a^{n-1} \neq 0$, considérer $x = a^{n-1}$.

2.6 *a)* Si $ab \in D$ il existe $c \in A - \{0\}$ tel que $(ab)c = 0$, et séparer en cas : $bc \neq 0$, $bc = 0$.

b) Si $a \in D$, il existe $c \in A - \{0\}$ tel que $ac = 0$ et séparer en cas : $ab \neq 0$, $ab = 0$.

2.7 *a)* Immédiat.

b) Montrer que A^* (resp. B^*) est un groupe pour la loi $\cdot$, en revenant aux définitions et montrer que f^* est un morphisme de groupes.

2.8 *1)* Montrer que, pour tout idéal I de A (contenant $\mathrm{Ker}\,(f)$), $f(I)$ est un idéal de A', en revenant aux définitions et en utilisant la surjectivité de f.

2) Montrer que, si I et J sont deux idéaux de A contenant $\mathrm{Ker}\,(f)$, et tels que $f(I) = f(J)$, alors $I \subset J$, puis $I = J$.

3) Montrer que, pour tout idéal I' de A', $f^{-1}(I')$ est un idéal de A, et montrer que $f\big(f^{-1}(I')\big) = I'$, en utilisant la surjectivité de f.

2.9 *a)* Évident.

b) 1) Raisonner par l'absurde et, si $u = (u_n)_{n\in\mathbb{N}}$ engendre I, montrer que les u_n sont tous non nuls et envisager $w = \big(\sqrt{|u_n|}\big)_{n\in\mathbb{N}}$.

2) Construire $u = (u_n)_{n\in\mathbb{N}}$, $v = (v_n)_{n\in\mathbb{N}} \in A$ telles que : $uv = 0$, $u \notin I$, $v \notin I$, en séparant les rôles de n pair, n impair.

3) Considérer, par exemple, l'ensemble J des suites mixées d'une suite de termes d'indices pairs tendant vers 0 et d'une suite de termes d'indices impairs bornée.

c) Immédiat. On obtient : $\sqrt{I} = I$.

2.10 Remarquer qu'il s'agit du carré de $x^4 + x^2 + 1$.

Procéder par examen de tous les cas :
$x = 0,\ \pm 1,\ \pm 2 \ldots$

2.11 Montrer : $(a-3) \wedge a = 1$ et utiliser le théorème d'Euler.

2.12 *a)* Revenir à la définition de : sous-anneau.

b) Montrer que, pour tout $n \in \mathbb{N}$, A_n est un sous-anneau de $\mathbb{Z}^2$.

Soit C un sous-anneau de $\mathbb{Z}^2$. Considérer

$$E = \big\{|x-y|\,;\,(x,y) \in C,\ x \neq y\big\}$$

et, si $E \neq \varnothing$, considérer le plus petit élément n de E. Montrer alors $C = A_n$, en utilisant une division euclidienne.

2.13 *1)* Montrer que, si I (resp. I') est un idéal de A (resp. A'), alors $I \times I'$ est un idéal de $A \times A'$.

2) Réciproquement, soit J un idéal de $A \times A'$. Considérer les deux projections I, I' de J :

$$I = \big\{x \in A\,;\,\exists\, x' \in A',\ \ (x,x') \in J\big\},$$

$$I' = \big\{x' \in A'\,;\,\exists\, x \in A,\ \ (x,x') \in J\big\}.$$

Montrer que I (resp. I') est un idéal de A (resp. A') et que $J = I \times I'$.

2.14 Soit $(m,n) \in (\mathbb{N}^*)^2$. Supposer qu'il existe un isomorphisme d'anneaux $f : \mathbb{Z}^m \longrightarrow \mathbb{Z}^n$. Alors, les solutions d'une équation dans $\mathbb{Z}^m$ doivent correspondre aux solutions de la même équation dans $\mathbb{Z}^n$. Envisager, par exemple, les idempotents, c'est-à-dire les solutions de l'équation $x^2 = x$.

2.15 En notant, pour tout $n \in \mathbb{N}$, $u_n = 2^{an+b} + 3^n$, montrer que $(u_n)_{n\in\mathbb{N}}$ est une suite récurrente linéaire du second ordre, à coefficients constants et entiers. En déduire :

$$\big(\forall n \in \mathbb{N},\ \ 5 \mid u_n\big) \iff \big(5 \mid u_0 \ \text{ et } \ 5 \mid u_1\big).$$

Étudier ensuite les congruences, modulo 5, des puissances de 2.

2.16 *a)* Utiliser la formule donnant l'indicateur d'Euler d'un entier à l'aide de la décomposition primaire de cet entier.

b) 1) Appliquer le résultat de *a)*.

2) Appliquer le résultat de *a)*.

3) Appliquer le résultat de *b) 2)* à $(a \wedge b,\ a \vee b)$.

2.17 Montrer d'abord que Z est un anneau, cf. exercice 2.1.

Soit $x \in Z$. Il existe $y \in A$ tel que : $x = xyx$. Noter $z = yxy$. Montrer : $x = xzx$, $xy \in Z$, $z \in Z$.

2.18 Il existe $a \in A - \{0\}$.
Considérer, pour $n \in \mathbb{N}^*$:

$$I_n = a^n A = \{a^n x\,;\, x \in A\}.$$

Il existe $p, q \in \mathbb{N}^*$ tels que : $p < q$ et $I_p = I_q$.
Il existe $b \in A$ tel que : $a^p = a^q b$.
Déduire : $a(a^{q-p-1}b) = 1_A$.

Corrigés des exercices

2.1

- On a : $Z \subset A$ et $1 \in Z$.
- On a, pour tout $(x, y) \in Z^2$:

$$\forall a \in A, \quad a(x+y) = ax + ay = xa + ya = (x+y)a,$$

donc : $x + y \in Z$.

- On a, pour tout $x \in Z$:

$$\forall a \in A, \quad a(-x) = -ax = -xa = (-x)a,$$

donc : $-x \in Z$.

- On a, pour tout $(x, y) \in Z^2$:

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

donc : $xy \in Z$.

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

Remarque : Il en résulte que Z (muni des lois induites par celles de A) est lui-même un anneau, avec le même neutre que A pour la multiplication.

2.2

a) D'après le cours, A est un anneau pour les lois usuelles, addition et multiplication.

b) • On a $1 \in B$ et, pour toutes $f, g \in B$:

$$f + g \in B, \quad -f \in B, \quad fg \in B.$$

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

• Si B était un idéal de A, puisque $1 \in B$, on aurait $B = A$, contradiction car, par exemple, l'application $x \longmapsto \left|x - \dfrac{1}{2}\right|$ est élément de A mais non de B.

On conclut : B n'est pas un idéal de A.

c) • On a $0 \in I$ et, pour toutes $f, g \in I$ et $h \in A$:

$$f - g \in I \quad \text{et} \quad hf \in I,$$

car : $\quad (f-g)(0) = f(0) - g(0) = 0$

et : $\quad (hf)(0) = h(0)f(0) = h(0)0 = 0.$

On conclut : I est un idéal de A.

• Comme $1 \notin I$, I n'est pas un sous-anneau de A.

d) • On a $1 \notin E$, car $1 \notin I$ et $E \subset I$, donc E n'est pas un sous-anneau de A.

• Considérons $f, h : [0\,;1] \longrightarrow \mathbb{R}$ définies par :

$$f : x \longmapsto x, \quad h : x \longmapsto \sqrt{1-x}.$$

Il est clair que : $f \in E$ et $h \in A$.

Mais $hf : x \longmapsto x\sqrt{1-x}$ n'est pas dérivable en 1, donc :

$$hf \notin E.$$

On conclut : E n'est pas un idéal de A.

2.3

Notons (S) le système proposé et $\mathcal{S}$ l'ensemble des solutions de (S).

a) • On a : $x \equiv 1 \ [2] \iff \big(\exists\, a \in \mathbb{Z}, \quad x = 1 + 2a\big)$.

• Puis, pour $a \in \mathbb{Z}$:

$$x \equiv 2 \ [3] \iff 1 + 2a \equiv 2 \ [3] \iff 2a \equiv 1 \ [3]$$
$$\iff -2a \equiv -1 \ [3] \iff a \equiv -1 \ [3]$$
$$\iff \big(\exists\, b \in \mathbb{Z}, \quad a = -1 + 3b\big).$$

On obtient : $x = 1 + 2a = 1 + 2(-1 + 3b) = -1 + 6b$.

• Puis, pour $b \in \mathbb{Z}$:

$$x \equiv 3 \ [5] \iff -1 + 6b \equiv 3 \ [5] \iff 6b \equiv 4 \ [5]$$
$$\iff b \equiv -1 \ [5] \iff \big(\exists c \in \mathbb{Z}, \quad b = -1 + 5c\big).$$

Ainsi :

$$(\mathrm{S}) \iff \exists\, c \in \mathbb{Z}, \quad x = -1 + 6(-1 + 5c) = -7 + 30c.$$

On conclut : $\mathcal{S} = \big\{-7 + 30c\,;\, c \in \mathbb{Z}\big\}$.

b) Si x convient, alors, puisque $x \equiv 1 \ [6]$, x est impair, et, puisque $x \equiv 4 \ [10]$, x est pair, contradiction.

On conclut : $\mathcal{S} = \varnothing$.

c) • On a : $x \equiv 7 \ [18] \iff \big(\exists\, a \in \mathbb{Z}, \quad x = 7 + 18a\big)$.

• Puis, pour $a \in \mathbb{Z}$:

$$x \equiv 1 \ [30] \iff 7 + 18a \equiv 1 \ [30] \iff 18a \equiv -6 \ [30]$$
$$\iff 3a \equiv -1 \ [5] \underset{2\wedge 5 = 1}{\iff} 2 \cdot 3a \equiv -2 \ [5]$$
$$\iff a \equiv -2 \ [5] \iff \big(\exists\, b \in \mathbb{Z}, \quad a = -2 + 5b\big).$$

On obtient :

$$x = 7 + 18a = 7 + 18(-2 + 5b) = -29 + 90b.$$

• Puis, pour $b \in \mathbb{Z}$:

$$x \equiv 16 \ [45] \iff -29 + 90b \equiv 16 \ [45]$$
$$\iff 90b \equiv 45 \ [45] \iff 2b \equiv 1 \ [1],$$

vrai pour tout $b \in \mathbb{Z}$.

Ainsi : $(\mathrm{S}) \iff \big(\exists\, b \in \mathbb{Z}, \quad x = -29 + 90b\big)$.

On conclut : $\mathcal{S} = \big\{-29 + 90b\,;\, b \in \mathbb{Z}\big\}$.

2.4

Notons (S) le système proposé et $\mathcal{S}$ l'ensemble des solutions de (S).

a) Puisque $2 \wedge 13 = 1$, $\widehat{2}$ est inversible dans $\mathbb{Z}/13\mathbb{Z}$.

De plus, comme $2 \cdot 7 = 14$, on a : $\widehat{2} \cdot \widehat{7} = \widehat{1}$.

Ainsi, dans la première équation de (S) :

$$\widehat{2}\,x + \widehat{3}\,y = \widehat{4} \iff \widehat{7}\,(\widehat{2}\,x + \widehat{3}\,y) = \widehat{7} \cdot \widehat{4}$$
$$\iff x + \widehat{21}\,y = \widehat{28} \iff x = \widehat{2} + \widehat{5}\,y.$$

Puis, en reportant dans la deuxième équation de (S) :

$$\widehat{3}\,x + \widehat{2}\,y = \widehat{5} \iff \widehat{3}\,(\widehat{2} + \widehat{5}\,y) + \widehat{2}\,y = \widehat{5}$$
$$\iff \widehat{17}\,y = -\widehat{1} \iff \widehat{4}\,y = -\widehat{1}$$
$$\underset{(-3)\wedge 13 = 1}{\iff} -\widehat{3}\,(\widehat{4}\,y) = (-\widehat{3})(-\widehat{1}) \iff y = \widehat{3}.$$

Enfin : $\quad x = \widehat{2} + \widehat{5}\,y = \widehat{2} + \widehat{5} \cdot \widehat{3} = \widehat{17} = \widehat{4}$.

On conclut : $\mathcal{S} = \big\{(\widehat{4}, \widehat{3})\big\}$.