PRÉPAS SCIENTIFIQUES

MP/MP*
MPI/MPI*

CONFORME AU NOUVEAU PROGRAMME

Charles Cochet • Xavier Oudot

Maths

TOUT-EN-UN

COURS • MÉTHODES • ENTRAÎNEMENTS ET SUJETS • CORRIGÉS

Tout le cours avec :
- Les objectifs-clés du programme
- Les notions à maîtriser
- Les démonstrations incontournables

Entraînement complet avec :
- Des vrai/faux
- Des exercices d'application
- Des exercices d'approfondissement
- Des sujets de concours

Des fiches de révisions avec :
- La synthèse des notions
- Les méthodes pas à pas

Tous les corrigés détaillés

OFFERT EN LIGNE

- + de 160 **flashcards** interactives
- 16 **synthèses** à télécharger
- Tous les **scripts Python** interactifs

Vuibert

PRÉPAS SCIENTIFIQUES
MP/MP*
MPI/MPI*

CONFORME AU NOUVEAU PROGRAMME

Maths

TOUT-EN-UN

COURS • MÉTHODES • ENTRAÎNEMENTS ET SUJETS • CORRIGÉS

Charles Cochet est professeur
en classe préparatoire scientifique MP
au lycée Fénelon Sainte-Marie à Paris.

Xavier Oudot est professeur de chaire supérieure en retraite,
ancien professeur en classe préparatoire scientifique MP
au lycée Fénelon Sainte-Marie à Paris.

Vuibert

Retrouvez notre collection complète ici :

MODE D'EMPLOI

Cet ouvrage a été conçu comme un **outil de révisions** pratique et agréable pour l'élève. Des rubriques, agrémentées de **pictogrammes**, permettent une lecture non linéaire et des **points de repères** visuels.

Les théorèmes à retenir

Un zoom sur les propositions
Essentielles pour la bonne compréhension du cours.

Conseils méthodologiques
Pour acquérir les bons réflexes et éviter les pièges.

Attention !
Pour mettre en avant les points de vigilance.

D'autres rubriques, **Définition**, **Démonstration**, **Remarque**, **Exemple**, **etc.** viennent enrichir les cours et permettent une meilleure appropriation des contenus.

ISBN : 978-2-311-21289-1

La loi du 11 mars 1957 n'autorisant aux termes des alinéas 2 et 3 de l'article 41, d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite » (alinéa 1er de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du Code pénal. Le « photocopillage », c'est l'usage abusif et collectif de la photocopie sans autorisation des auteurs et des éditeurs. Largement répandu dans les établissements d'enseignement, le « photocopillage » menace l'avenir du livre, car il met en danger son équilibre économique. Il prive les auteurs d'une juste rémunération. En dehors de l'usage privé du copiste, toute reproduction totale ou partielle de cet ouvrage est interdite. Des photocopies payantes peuvent être réalisées avec l'accord de l'éditeur. S'adresser au Centre français d'exploitation du droit de copie : 20, rue des Grands-Augustins, F-75006 Paris. Tél. : 01 44 07 47 70.

DANGER LE PHOTOCOPILLAGE TUE LE LIVRE

© Vuibert – juillet 2022 – 5, allée de la 2e D.B., 75015 Paris – Site Internet : http://www.vuibert.fr

SOMMAIRE

Ressources numériques

Pour accéder aux ressources numériques en ligne, retrouvez nos codes à flasher tout au long du livre :

- **Flashcards d'auto-évaluation interactives**
- **Scripts Python**
- **Synthèses à télécharger**

Chapitre 1. Compléments sur les groupes **7**

Cours, p. 8

1 ► Sous-groupe engendré par une partie, p. 8 — **2** ► Groupe monogène, p. 10 — **3** ► Groupes $\mathbb{Z}/n\mathbb{Z}$, p. 11 — **4** ► Groupe cyclique, p. 12 — **5** ► Ordre d'un élément d'un groupe, p. 13 — **6** ► Produit de deux groupes, p. 16

Fiche de synthèse, p. 17

Méthode pas à pas, p. 18

Exercices, p. 19

Corrigés, p. 24

Chapitre 2. Compléments sur les anneaux **35**

Cours, p. 36

1 ► Idéaux d'un anneau commutatif, p. 36 — **2** ► L'anneau $\mathbb{Z}$, p. 39 — **3** ► Anneaux $\mathbb{Z}/n\mathbb{Z}$, p. 40 — **4** ► Anneaux $\mathbb{K}[X]$, p. 46 — **5** ► Algèbres, p. 50

Fiche de synthèse, p. 53

Méthode pas à pas, p. 55

Exercices, p. 57

Corrigés, p. 65

Chapitre 3. Compléments d'algèbre linéaire **79**

Cours, p. 80

1 ► Somme, somme directe d'une famille finie de sous-espaces vectoriels, p. 80 — **2** ► Calcul matriciel par blocs, p. 84 — **3** ► Stabilité par un endomorphisme, p. 86 — **4** ► Éléments propres d'un endomorphisme ou d'une matrice carrée, p. 88 — **5** ► Éléments propres en dimension finie, p. 90

Fiche de synthèse, p. 96

Méthode pas à pas, p. 98

Exercices, p. 99

Corrigés, p. 104

Chapitre 4. Réduction des endomorphismes et des matrices carrées **111**

Cours, p. 112

1 ► Polynômes d'un endomorphisme, p. 112 — **2** ► Le théorème de Cayley-Hamilton et ses conséquences, p. 117 — **3** ► Décomposition des noyaux, p. 120 — **4** ► Endomorphismes et matrices carrées diagonalisables, p. 122 — **5** ► Endomorphismes et matrices carrées trigonalisables, p. 126 — **6** ► Endomorphismes nilpotents, matrices nilpotentes, p. 130 — **7** ► Trigonalisation à l'aide des sous-espaces caractéristiques, p. 131

Fiche de synthèse, p. 136

Méthode pas à pas, p. 138

Exercices, p. 140

Corrigés, p. 147

Chapitre 5. Endomorphismes d'un espace euclidien **161**

Cours, p. 162

1 ► Adjoint d'un endomorphisme, p. 162 — **2** ► Isométries vectorielles, p. 165 — **3** ► Matrices orthogonales, p. 169 — **4** ► Isométries vectorielles en dimension 2, p. 172 — **5** ► Réduction des isométries, p. 175 — **6** ► Réduction des endomorphismes autoadjoints, p. 179

Fiche de synthèse, p. 182

Méthode pas à pas, p. 185

Exercices, p. 187

Corrigés, p. 195

Chapitre 6. Espaces vectoriels normés **209**

Cours, p. 210

1 ► Normes et distances, p. 210 — **2** ► Premières notions topologiques dans un espace vectoriel normé, p. 215 — **3** ► Équivalence des normes, p. 220 — **4** ► Suites extraites. Valeurs d'adhérence, p. 223

Fiche de synthèse, p. 225

Méthode pas à pas, p. 227

Exercices, p. 229

Corrigés, p. 235

Chapitre 7. Topologie d'un espace vectoriel normé **245**

Cours, p. 246

1 ► Topologie d'un espace normé, p. 246 — **2** ► Étude locale d'une application, p. 256 — **3** ► Applications linéaires continues, p. 264 — **4** ► Compacité, p. 268 — **5** ► Espaces normés de dimension finie, p. 271 — **6** ► Connexité par arcs, p. 274

Fiche de synthèse, p. 279

Méthode pas à pas, p. 281

Exercices, p. 283

Corrigés, p. 291

Chapitre 8. Séries numériques et vectorielles **305**

Cours, p. 306

1 ► Séries d'éléments d'un espace vectoriel normé, p. 306 — **2** ► Convergence absolue, p. 309 — **3** ► Compléments sur les séries numériques, p. 314

Fiche de synthèse, p. 320

Méthode pas à pas, p. 322

Exercices, p. 323

Corrigés, p. 329

Chapitre 9. Suites et séries de fonctions **339**

Cours, p. 340

1 ► Convergence d'une suite de fonctions, p. 340 — **2** ► Intégration et dérivation d'une suite de fonctions, p. 346 — **3** ► Convergence d'une série de fonctions, p. 349 — **4** ► Approximation des fonctions d'une variable réelle, p. 355

Fiche de synthèse, p. 360

Méthode pas à pas, p. 362

Exercices, p. 364

Corrigés, p. 371

Chapitre 10. Séries entières **385**

Cours, p. 386

1 ► Séries entières d'une variable complexe, p. 386 — **2** ► Opérations sur les séries entières, p. 392 — **3** ► Étude sur le disque ouvert de convergence, p. 394 — **4** ► Série entière d'une variable réelle, p. 396 — **5** ► Développement en série entière, p. 399

Fiche de synthèse, p. 403

Méthode pas à pas, p. 405

Exercices, p. 407

Corrigés, p. 415

Chapitre 11. Fonctions vectorielles **429**

Cours, p. 430

1 ► Dérivation des fonctions vectorielles, p. 430 — **2** ► Fonctions de classe $\mathscr{C}^k$, p. 434 — **3** ► Intégration sur un segment, p. 435 — **4** ► Formules de Taylor, p. 442

Fiche de synthèse, p. 446

Méthode pas à pas, p. 448

Exercices, p. 449

Corrigés, p. 455

Chapitre 12. Intégration sur un intervalle quelconque **467**

Cours, p. 468

1 ► Intégrale généralisée sur un intervalle de la forme $[a,+\infty[$, p. 468 — **2** ► Intégrabilité sur un intervalle de la forme $[a,+\infty[$, p. 470 — **3** ► Intégration sur un intervalle quelconque, p. 474 — **4** ► Suites et séries de fonctions intégrables, p. 483 — **5** ► Intégrales dépendant d'un paramètre, p. 488

Fiche de synthèse, p. 496

Méthode pas à pas, p. 498

Exercices, p. 500

Corrigés, p. 508

Chapitre 13. Probabilités **525**

Cours, p. 526

1 ► Dénombrabilité, p. 526 — **2** ► Espace probabilisable, p. 529 — **3** ► Espace probabilisé, p. 533 — **4** ► Conditionnement, p. 541 — **5** ► Indépendance, p. 547

Fiche de synthèse, p. 550

Méthode pas à pas, p. 552

Exercices, p. 554

Corrigés, p. 559

Chapitre 14. Variables aléatoires discrètes **571**

Cours, p. 572

1 ► Variables aléatoires discrètes, p. 572 — **2** ► Espérance d'une variable aléatoire réelle ou complexe, p. 583 — **3** ► Lois usuelles, p. 594 — **4** ► Loi faible des grands nombres, p. 600 — **5** ► Fonctions génératrices, p. 602

Fiche de synthèse, p. 607

Méthode pas à pas, p. 610

Exercices, p. 613

Corrigés, p. 619

Chapitre 15. Équations différentielles linéaires **633**

Cours, p. 634

1 ► Équations différentielles linéaires d'ordre 1, p. 634 — **2** ► Résolution de l'équation homogène, p. 640 — **3** ► Résolution de l'équation complète, p. 644 — **4** ► Équations linéaires à coefficients constants, p. 646 — **5** ► Équations différentielles scalaires, p. 650

Fiche de synthèse, p. 656

Méthode pas à pas, p. 658

Exercices, p. 660

Corrigés, p. 666

Chapitre 16. Calcul différentiel **679**

Cours, p. 680

1 ► Dérivée selon un vecteur, p. 680 — **2** ► Applications différentiables, p. 681 — **3** ► Opérations sur les applications différentiables, p. 685 — **4** ► Vecteurs tangents à une partie de $\boldsymbol{E}$, p. 691 — **5** ► Optimisation : étude au premier ordre, p. 694 — **6** ► Fonctions de classe $\mathscr{C}^1$, p. 700 — **7** ► Dérivées partielles d'ordre supérieur, p. 702 — **8** ► Optimisation : étude au second ordre, p. 706

Fiche de synthèse, p. 709

Méthode pas à pas, p. 711

Exercices, p. 712

Corrigés, p. 720

Chapitre 17. Problèmes de concours **737**

1 ► CCINP MP 2017, Maths 2, p. 738 — **2** ► Centrale-Supélec PSI 2018, Maths 2, p. 750 — **3** ► X MP 2017, épreuve B, p. 767 — **4** ► Centrale Supelec MP 2021, Maths 1 (extrait), p. 786

Index **805**

CHAPITRE 1
Compléments sur les groupes

Plan du chapitre

Cours, p. 8 ☐
- **1** ▶ Sous-groupe engendré par une partie, p. 8 ☐
- **2** ▶ Groupe monogène, p. 10 ☐
- **3** ▶ Groupes $\mathbb{Z}/n\mathbb{Z}$, p. 11 ☐
- **4** ▶ Groupe cyclique, p. 12 ☐
- **5** ▶ Ordre d'un élément d'un groupe, p. 13 ☐
- **6** ▶ Produit de deux groupes, p. 16 ☐

Fiche synthèse, p. 17 ☐
Méthodes pas à pas, p. 18 ☐
Exercices, p. 19 ☐
Corrigés, p. 24 ☐

Objectifs et compétences du programme

Capacités principales à maîtriser	Méthodes associées	Exercices associés
Trouver le sous-groupe engendré par une partie.	Méthode 1	Exercices 7, 8, C
Trouver l'ordre d'un élément d'un groupe.	Méthode 2	Exercices 1, 2, 3, D
Reconnaître un groupe cyclique.	Méthode 3	Exercices 1, 4
Connaître les éléments générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$.	Méthode 4	Exercices 5, 6

RETROUVEZ ICI LES FLASHCARDS INTERACTIVES POUR SE TESTER

www.lienmini.fr/212891-FLASH-01

COURS

Histoire des mathématiques

Évariste Galois, mathématicien français (1811-1832)
Génie très précoce, Évariste Galois échoue au concours de l'École polytechnique pour avoir jeté l'éponge à la figure de l'examinateur qui ne comprenait pas sa démonstration. Admis contre son gré à l'École royale (future ENS), il en est exclu en 1831 pour avoir levé son poignard à la santé du roi Louis-Philippe. Il meurt tragiquement le 31 mai 1832 dans un duel au pistolet contre un mari jaloux.
Galois, dans son *Mémoire sur les conditions de résolubilité des équations par radicaux* paru en 1830, généralise des idées de Joseph-Louis Lagrange (1736-1813). Il étudie un certain sous-groupe du groupe des permutations des racines d'une équation polynomiale pour décider de sa résolubilité par radicaux. C'est du moins la lecture moderne que nous pouvons faire d'un texte assez abscons mais bouillonnant d'idées nouvelles. Proposé pour le « Prix de l'Académie des sciences », le mémoire est égaré par Siméon Denis Poisson qui ne l'a même pas lu. Ce n'est que vingt ans plus tard qu'Arthur Cayley (1821-1895) énonce la définition générale d'un groupe, indépendamment de la notion de permutation. En 1872, dans son *Programme d'Erlangen*, Félix Klein refonde toute la géométrie sur le concept de groupe de transformations.

1 Sous-groupe engendré par une partie

1.1. Intersection de sous-groupes

Proposition 1.1. Intersection d'une famille de sous-groupes

Soit $(G,*)$ un groupe. L'intersection d'une famille de sous-groupes de G est un sous-groupe de G.

Démonstration
Utilisons la notation multiplicative. Soit $(H_i)_{i\in I}$ une famille de sous-groupes de G et $H=\bigcap_{i\in I} H_i$. Désignons par e l'élément neutre de G. Pour tout $i\in I$, $e\in H_i$, donc $e\in H$ et, par conséquent, $H\neq\varnothing$. De plus, pour tout $(x,y)\in H^2$, quel que soit $i\in I$, $(x,y)\in H_i^2$, donc $xy^{-1}\in H_i$; par conséquent, $xy^{-1}\in H$. H vérifie la caractérisation d'un sous-groupe. ■

1.2. Sous-groupe engendré par une partie

Définition 1.2. Sous-groupe engendré par une partie

Soit $(G,*)$ un groupe et A une partie quelconque de G. On appelle sous-groupe engendré par A l'intersection de la famille des sous-groupes de G contenant A.
On le note $<A>$ ou $\mathrm{gr}(A)$.

Exemples

- Si a est un élément de G, alors le sous-groupe engendré par le singleton $\{a\}$ est l'ensemble des itérés de a : $a\mathbb{Z} = \{na,\ n \in \mathbb{Z}\}$ en notation additive, $\{a^n,\ n \in \mathbb{Z}\}$ en multiplicative.
- Dans le groupe multiplicatif $\mathbb{C}^*$, le sous-groupe engendré par le singleton $\{e^{\frac{2i\pi}{n}}\}$ est l'ensemble des racines n-ièmes de l'unité $\mathscr{U}_n$.
- Dans le groupe des bijections du plan affine, le sous-groupe engendré par les symétries centrales est l'ensemble des symétries centrales et des translations.
- Dans le groupe symétrique $\mathscr{S}_n$, le sous-groupe engendré par les cycles de longueur 3 est le groupe alterné $\mathscr{A}_n$, ensemble des permutations de signature $+1$.

Proposition 1.3. Caractérisation du sous-groupe engendré par une partie

Soit $(G,*)$ un groupe et A une partie de G. Alors $< A >$ est, au sens de l'inclusion, le plus petit sous-groupe de G contenant A.

Démonstration

1. D'après la proposition 1.1., $< A >$ est est bien un sous-groupe de G et il contient A par construction.
2. Soit H un sous-groupe de G contenant A. Puisque $< A >$ est l'intersection de tous les sous-groupes de G contenant A, on a $< A > \subset H$. Ainsi $< A >$ est contenu dans tout sous-groupe contenant A, c'est donc bien le plus petit au sens de l'inclusion.

■

Proposition 1.4. Description du sous-groupe engendré par une partie

Soit $(G,*)$ un groupe d'élément neutre e et A une partie de G.

1. $< \emptyset >= \{e\}$.
2. Si A est non-vide alors :

$$< A > = \left\{x \in G\ ;\ \exists n \in \mathbb{N}^*,\ \exists(\alpha_1,\dots,\alpha_n) \in (A \cup A^{-1})^n,\ x = \alpha_1 * \cdots * \alpha_n\right\}.$$

En d'autres termes $< A >$ est l'ensemble des éléments de G qui sont des produits finis d'éléments de A ou d'inverses d'éléments de A.

Démonstration

1. Il est clair que $\{e\}$ est le plus petit sous-groupe de G contenant $\emptyset$!
2. Posons $H = \left\{x \in G\ ;\ \exists n \in \mathbb{N}^*,\ \exists(\alpha_1,\dots,\alpha_n) \in (A \cup A^{-1})^n,\ x = \alpha_1 * \cdots * \alpha_n\right\}$ et démontrons que H est le plus petit sous-groupe de G contenant A.
   - Prouvons tout d'abord que H est un sous-groupe de G. L'ensemble A étant non-vide, il existe $a \in A$ donc $a * a^{-1} \in H$ c'est-à-dire $e \in H$.
     Soit maintenant $x = \alpha_1 * \cdots * \alpha_n \in H$ et $y = \beta_1 * \cdots * \beta_m \in H$. Alors $x * y^{-1} = \alpha_1 * \cdots * \alpha_n * \beta_m^{-1} * \cdots \beta_1^{-1}$ est bien un produit fini d'éléments de $A \cup A^{-1}$, donc $x * y^{-1}$ est bien dans H.
   - Prouvons ensuite que $A \subset H$. En fait $A \subset A \cup A^{-1} \subset H$.
   - Prouvons enfin que H est le plus petit sous-groupe de G contenant A. Soit L un sous-groupe de G contenant A. Pour tout $x \in A$ on a $x \in L$ et $x^{-1} \in L$, donc $A \cup A^{-1} \subset L$. Puis par stabilité de L par produit on obtient $H \subset L$.

■

1.3. Partie génératrice d'un groupe

Définition 1.5. Partie génératrice d'un groupe

Une partie A d'un groupe G est dite génératrice de G si le sous-groupe engendré par A est G tout entier.

Exemples

- Le singleton $\{-1\}$ est une partie génératrice du groupe $(\mathbb{Z},+)$.
- L'ensemble des transpositions est une partie génératrice du groupe symétrique $\mathscr{S}_n$.

2 Groupe monogène

2.1. Définition et exemples

Définition 1.6. Groupe monogène

Un groupe G est dit monogène s'il est engendré par un singleton $\{a\}$. Un tel élément a est dit générateur de G. On dit indifféremment que G est engendré par $\{a\}$ ou par a.

Exemples

- Le groupe $(\mathbb{Z},+)$ est monogène, de générateur 1 ou -1.
- Le groupe $(\mathscr{U}_4,\times)$ des racines quatrièmes de l'unité est monogène, de générateur i ou $-i$.

2.2. Sous-groupes de $(\mathbb{Z},+)$

Théorème 1.7. Sous-groupes de $(\mathbb{Z},+)$

Tout sous-groupe du groupe $(\mathbb{Z},+)$ est monogène, autrement dit pour tout sous-groupe H de $\mathbb{Z}$, il existe $n\in\mathbb{N}$ tel que $H=n\mathbb{Z}$.

Démonstration

Si $H=\{0\}$, alors $H=0\mathbb{Z}$. Sinon, H contient au moins un entier non nul et son opposé. L'ensemble $H\cap\mathbb{N}^*$ est une partie non vide de $\mathbb{N}^*$, qui possède donc un plus petit élément, que nous noterons n. Il est clair que $n\mathbb{Z}\subset H$. Réciproquement, soit m un élément quelconque de H. Effectuons la division euclidienne de m par n : il existe $(q,r)\in\mathbb{Z}^2$ tel que $m=nq+r$ et $0\leqslant r<n$. Comme m et nq appartiennent à H, il en est de même de r. Mais r est positif et strictement inférieur au plus petit élément *strictement* positif de H ; il ne peut être que nul. Ainsi, $m=nq\in n\mathbb{Z}$, donc $H\subset n\mathbb{Z}$ et, en définitive, $H=n\mathbb{Z}$. ■

3 Groupes $\mathbb{Z}/n\mathbb{Z}$

3.1. Congruence modulo n

Définition 1.8. Congruence modulo n

Soit $n \in \mathbb{N}$. Deux entiers relatifs a et b sont dits congrus modulo n lorsque $a - b \in n\mathbb{Z}$.
On écrit $a \equiv b\,[n]$.

Proposition 1.9. Une relation d'équivalence

La relation de congruence modulo n est une relation d'équivalence.

Démonstration
Le lecteur vérifiera soigneusement la réflexivité, la symétrie et la transitivité de cette relation. ■

Si $n > 0$, alors a et b sont congrus modulo n si et seulement si ils ont le même reste dans la division euclidienne par n. Il y a donc exactement n classes d'équivalence.

La classe d'un entier k est le plus souvent notée $\overline{k}$ ou $\overline{k}^{(n)}$ s'il y a une ambiguïté sur n. Elle est parfois notée $\dot{k}$ ou $\mathrm{Cl}_n(k)$.

Définition 1.10. Ensemble $\mathbb{Z}/n\mathbb{Z}$

On désigne par $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence modulo n :

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}.$$

3.2. Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Proposition 1.11. Addition des classes

Soit $n \in \mathbb{N}^*$. Pour tout $(a, b) \in \mathbb{Z}^2$, la classe modulo n de $a+b$ ne dépend que des classes de a et de b, et non de représentants particuliers de ces classes. On a ainsi une addition dans $\mathbb{Z}/n\mathbb{Z}$:

$$\forall (\overline{a}, \overline{b}) \in (\mathbb{Z}/n\mathbb{Z})^2, \quad \overline{a} + \overline{b} = \overline{a+b}.$$

$\mathbb{Z}/n\mathbb{Z}$ muni de cette addition est un groupe abélien.

Démonstration
Soit $(a', b') \in \overline{a} \times \overline{b}$: $a' - a \in n\mathbb{Z}$ et $b' - b \in n\mathbb{Z}$.

$$(a' + b') - (a + b) = (a' - a) + (b' - b) \in n\mathbb{Z},$$

donc $a' + b' \in \overline{a+b}$. On vérifie que l'addition ainsi définie dans $\mathbb{Z}/n\mathbb{Z}$ est associative, commutative, qu'elle admet un élément neutre $\overline{0}$ et que toute classe $\overline{a}$ possède une opposée, $\overline{-a}$. ■

Exemple

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Les éléments $\overline{1}$ et $\overline{3}$ sont symétriques (opposés) ; $\overline{0}$ et $\overline{2}$ sont chacun leur propre symétrique.

Figure 1.1. Table du groupe $(\mathbb{Z}/4\mathbb{Z},+)$.

3.3. Éléments générateurs de $\mathbb{Z}/n\mathbb{Z}$

Théorème 1.12. Éléments générateurs de $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$. Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est monogène. Un élément $\overline{k}$ est générateur de ce groupe si et seulement si l'entier k est premier avec n.

Démonstration
Si $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$, alors il existe un entier p tel que $p\overline{k} = \overline{1}$, c'est-à-dire $pk \equiv 1\,[n]$. Il existe donc un entier q tel que $pk = 1 + qn$, d'où, d'après le théorème de Bezout, $k \wedge n = 1$.
Réciproquement, si k est premier avec n, alors il existe des entiers p et q tels que $pk + qn = 1$, d'où $pk \equiv 1\,[n]$ et $p\overline{k} = \overline{1}$. Pour tout $r \in [\![0, n-1]\!]$, $\overline{r} = p\,r\overline{k} : \overline{k}$ engendre le groupe $\mathbb{Z}/n\mathbb{Z}$. ■

Remarque
Le nombre d'éléments générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire le nombre d'entiers de $[\![1, n-1]\!]$ premiers avec n est appelé *indicatrice d'Euler* de l'entier n et noté $\varphi(n)$. Le calcul de ce nombre sera étudié dans le chapitre suivant, page 43.

4 Groupe cyclique

Définition 1.13. Groupe cyclique

On appelle groupe cyclique un groupe monogène fini.

Exemples
Pour tout $n \in \mathbb{N}$:
- Le groupe $(\mathscr{U}_n, \times)$ des racines n-ièmes de l'unité est cyclique, engendré par $e^{\frac{2i\pi}{n}}$.
- Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est cyclique, engendré par $\overline{1}^{(n)}$.

Théorème 1.14. Classification des groupes monogènes

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

Démonstration

Soit G un groupe monogène, que nous noterons multiplicativement. Soit a un générateur de G. L'application $\varphi : k \mapsto a^k$ est un morphisme de $(\mathbb{Z},+)$ dans $(G,\times)$, surjectif par hypothèse.

Le noyau de ce morphisme est un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$ d'après le théorème 1.7. Deux cas peuvent se présenter :

- si $n = 0$, Ker $\varphi = \{0\}$, alors le morphisme est aussi injectif, donc bijectif. Le groupe G est ainsi isomorphe à $\mathbb{Z}$;
- si $n > 0$, alors $a^k = e$ équivaut à $k \in n\mathbb{Z}$: ainsi n est le plus petit entier strictement positif tel que $a^n = e$. Le sous-groupe engendré par a est par conséquent :

$$< a >= \{e, a, a^2, \cdots, a^{n-1}\}.$$

  De plus, pour tout $(k,k') \in \mathbb{Z}^2$, $a^k = a^{k'}$ équivaut à $a^{k-k'} = e$, donc à $k \equiv k'\,[n]$ ou encore $\overline{k}^{(n)} = \overline{k'}^{(n)}$.
  L'application : $\overline{k}^{(n)} \mapsto a^k$ est un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ dans G.

L'entier n est appelé *ordre* de l'élément a. ■

Exemples

- $(\mathscr{U}_n,\times)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$, *via* l'isomorphisme $\overline{k}^{(n)} \mapsto \mathrm{e}^{2ik\pi/n}$.
- $(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},+)$ est isomorphe à $(\mathbb{Z}/6\mathbb{Z},+)$, *via* l'isomorphisme $\overline{k}^{(6)} \mapsto (\overline{k}^{(3)}, \overline{k}^{(2)})$.
- $(\{\mathrm{e}^{\mathrm{i}k\alpha},\ k\in\mathbb{Z}\},\times)$, où $\alpha \notin \pi\mathbb{Q}$ est un groupe isomorphe à $(\mathbb{Z},+)$, *via* l'isomorphisme $k \mapsto \mathrm{e}^{\mathrm{i}k\alpha}$.

5 Ordre d'un élément d'un groupe

5.1. Théorème de Lagrange

Théorème 1.15. Théorème de Lagrange

Dans un groupe fini, le cardinal d'un sous-groupe est un diviseur du cardinal du groupe.

Démonstration

Soit G un groupe fini et H un sous-groupe de G. La relation $\mathscr{R}$, définie dans G par $x\mathscr{R}y$ si et seulement si $xy^{-1} \in H$, est une relation d'équivalence :

- réflexive : $\forall x \in G,\ xx^{-1} = e \in H$;
- symétrique : $\forall (x,y) \in G^2,\ xy^{-1} \in H \Rightarrow yx^{-1} = (xy^{-1})^{-1} \in H$;
- transitive : $\forall (x,y,z) \in G^3,\ xy^{-1} \in H$ et $yz^{-1} \in H \Rightarrow xz^{-1} = (xy^{-1})(yz^{-1}) \in H$.

Pour tout $x \in G$, l'application $y \mapsto xy^{-1}$ de $\overline{x}$ dans H est une bijection car, pour tout $z \in H$, il existe un et un seul $y = z^{-1}x \in \overline{x}$ tel que $xy^{-1} = z$. Toutes les classes d'équivalence ont donc le même cardinal que H. Comme ces classes forment une partition de G, on en déduit que $|G| = p\,|H|$, où p est le nombre de classes d'équivalence. ■

5.2. Ordre d'un élément d'un groupe

Définition 1.16. Ordre d'un élément

Soit a un élément d'un groupe G. Si le sous-groupe engendré par a est fini, le cardinal de ce sous-groupe est appelé ordre de l'élément a. Sinon, l'élément a est dit d'ordre infini.

Exemples

- i est un élément d'ordre 4 du groupe $(\mathbb{C}^*, \times)$.
- Une réflexion de l'espace euclidien E est un élément d'ordre 2 du groupe $\mathrm{O}(E)$.
- Un cycle de longueur k est un élément d'ordre k du groupe symétrique $\mathscr{S}_n$.
- 2 est un élément d'ordre infini du groupe $(\mathbb{R}^*, \times)$.

Proposition 1.17. Ordre et divisibilité dans $\mathbb{Z}$

Soit a un élément d'un groupe G d'élément neutre e. Si a est d'ordre d fini, alors :

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

(En notation additive : $\forall n \in \mathbb{Z}, \quad n \cdot a = e \iff d|n.$).

Démonstration

Si a est d'ordre d, le groupe engendré par a est de cardinal d, donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$.
Donc $a^n = e$ équivaut à $\overline{n} = \overline{0}$ dans $\mathbb{Z}/d\mathbb{Z}$, c'est-à-dire $n \in d\mathbb{Z}$, soit d divise n. ■

Proposition 1.18. Caractérisation de l'ordre d'un élément

Soit a un élément d'un groupe G. L'ordre de a est le plus petit entier p strictement positif, s'il existe, tel que $a^p = e$ (en notation additive : $pa = 0$).

Démonstration

En notation multiplicative, le sous-groupe engendré par a est l'image du morphisme $\varphi : k \mapsto a^k$ de $(\mathbb{Z}, +)$ dans $(G, \times)$. Le noyau de φ est un sous-groupe de $(\mathbb{Z}, +)$, donc de la forme $p\mathbb{Z}$, avec $p \in \mathbb{N}$.

- Si $p = 0$, alors φ est injectif, le sous-groupe engendré par a est isomorphe à $(\mathbb{Z}, +)$ et l'élément a est donc d'ordre infini.
- Si $p \in \mathbb{N}^*$, alors $a^k = e \iff k \in p\mathbb{Z}$. Ainsi p est le plus petit entier strictement positif tel que $a^p = e$. Le sous-groupe engendré par a est $\{e, a, a^2, \ldots, a^{p-1}\}$: l'ordre de a est le cardinal de ce sous-groupe, c'est-à-dire p. ■

Proposition 1.19. L'ordre d'un élément divise le cardinal du groupe

Si G est un groupe fini de cardinal n, alors tout élément de G est d'ordre fini et son ordre est un diviseur de n.

Démonstration

Si G est fini, alors tout sous-groupe engendré par un élément de G est fini et, d'après le théorème de Lagrange (1.15), son cardinal est un diviseur de n. ■

Théorème 1.20. Un des nombreux théorèmes d'Euler

Soit G un groupe fini de cardinal n. Pour tout élément a de G : $a^n = e$.

Démonstration

Si a est d'ordre p, alors $n \in p\mathbb{Z}$, donc $a^n = e$. ■

5.3. Groupe cyclique et ordre d'un élément

Soit G un groupe fini de cardinal n. Un élément de G est générateur de G si et seulement si son ordre est n. Par conséquent :
Un groupe fini de cardinal n est cyclique si et seulement si il contient au moins un élément d'ordre n, générateur du groupe.

Exemples

- Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est fini et engendré (entre autres) par $\overline{1}$: il est cyclique.
- Le groupe produit $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ est fini et engendré (entre autres) par $(\overline{1}^{(3)}, \overline{1}^{(2)})$: il est cyclique.
- Le groupe $(\mathscr{U}_n, \times)$ des racines n-ièmes de l'unité est fini et engendré (entre autres) par $e^{2i\pi/n}$: il est cyclique.
- Le groupe alterné $\mathscr{A}_3$, de cardinal 3 est engendré (entre autres) par le cycle $(1, 2, 3)$: il est cyclique.

Conseils méthodologiques

Pour justifier qu'un groupe fini de cardinal n n'est pas cyclique, il faut montrer que les ordres de tous ses éléments sont des diviseurs stricts de n.
Par exemple, le groupe symétrique $\mathscr{S}_3$, de cardinal 6, n'est pas cyclique car l'ordre de chacun de ses éléments est $1, 2$ ou 3, mais jamais 6.

5.4. Groupe de cardinal premier

Proposition 1.21. Groupe de cardinal premier

Soit p un nombre premier. Tout groupe de cardinal p est cyclique.

Démonstration

L'ordre d'un élément divise p : c'est 1 ou p. Tous les éléments distincts de l'élément neutre e ont pour ordre p. Le groupe est donc cyclique et engendré par n'importe quel élément distinct de e. ■

6 Produit de deux groupes

Définition 1.22. Groupe produit

Soit $(G,*)$ et $(G',\circ)$ deux groupes. On munit le produit cartésien $G\times G'$ de la loi $(x,x')\square(y,y')=(x*y,x'\circ y')$. Alors, $(G\times G',\square)$ est un groupe, appelé groupe produit de G et G'.

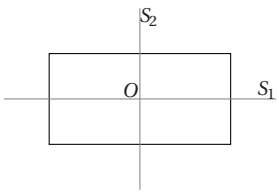
Exemple

Le groupe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ est appelé *groupe de Klein*. Il possède un élément d'ordre 1 et trois éléments d'ordre 2. Il n'est donc pas cyclique et n'est pas isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

$+$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$
$(\bar{0},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$
$(\bar{0},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{0})$
$(\bar{1},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$
$(\bar{1},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{0})$

Figure 1.2. Table du groupe de Klein $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

On rencontre fréquemment des groupes isomorphes au groupe de Klein ; par exemple, en géométrie, le groupe des isométries conservant un rectangle : l'identité, deux symétries axiales d'axes perpendiculaires en un point O et la symétrie centrale de centre O.



$\circ$	Id	S_1	S_2	S_O
Id	Id	S_1	S_2	S_O
S_1	S_1	Id	S_O	S_2
S_2	S_2	S_O	Id	S_1
S_O	S_O	S_2	S_1	Id

Figure 1.3. Le groupe des isométries du rectangle.

FICHE SYNTHÈSE

Sous-groupe engendré par une partie

Soit G un groupe.

- L'intersection d'une famille de sous-groupes de G est un sous-groupe de G.
- Le sous-groupe engendré par une partie A de G est l'intersection de la famille des sous-groupes de G contenant A. C'est le plus petit sous-groupe de G contenant A.
- On dit que la partie A est génératrice de G si le sous-groupe engendré par A est G.
- Le groupe G est dit monogène s'il est engendré par un singleton $\{a\}$. On dit indifféremment que G est engendré par a ou que a est un élément générateur de G.
- Un groupe est dit cyclique s'il est monogène et fini.

Groupes $\mathbb{Z}/n\mathbb{Z}$

- Les sous-groupes du groupe $(\mathbb{Z},+)$ sont monogènes, c'est-à-dire de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$.
- La relation de congruence modulo n, définie sur $\mathbb{Z}$ par : $a \equiv b\ [n] \iff a - b \in n\mathbb{Z}$ est une relation d'équivalence.
- L'ensemble des classes d'équivalence, noté $\mathbb{Z}/n\mathbb{Z}$ peut être muni d'une structure de groupe. Pour tout $n \in \mathbb{N}$, le groupe $\mathbb{Z}/n\mathbb{Z}$ est monogène.
- La classe d'un entier k modulo n est génératrice de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier avec n.
- Tout groupe monogène est isomorphe à :
  - $\mathbb{Z}$, s'il est infini ;
  - $\mathbb{Z}/n\mathbb{Z}$, s'il est fini de cardinal n.

Ordre d'un élément

- Dans un groupe fini, le cardinal d'un sous-groupe divise celui du groupe.
- Un élément $a \in G$ est dit d'ordre $m \in \mathbb{N}^*$ si le sous-groupe engendré par a est fini de cardinal m.
- Si G est un groupe d'élément neutre e, l'ordre d'un élément $a \in G$ est le plus petit entier $m \in \mathbb{N}^*$, s'il existe, tel que $a^m = e$.
- Pour tout $a \in G$, si a est d'ordre m, alors : $\forall n \in \mathbb{Z},\ a^n = e \iff m|n$.
- Si le groupe G est fini de cardinal n, pour tout $a \in G$, $a^n = e$.
- Si p est un nombre premier, tout groupe de cardinal p est cyclique.

RETROUVEZ ICI LA SYNTHÈSE DE CE CHAPITRE À TÉLÉCHARGER

www.lienmini.fr/212891-SYNTH-01

MÉTHODES PAS À PAS

Méthode 1 : Sous-groupe engendré par une partie

► Pour montrer que H est le sous-groupe de G engendré par une partie A, vous devez montrer :
- que H est un sous-groupe de G ;
- que $A \subset H$;
- que pour tout sous-groupe H' de G, si $A \subset H'$, alors $H \subset H'$.

► Pour montrer qu'une partie A est génératrice de G, vous pouvez montrer que tout élément de G est un produit d'éléments de A et d'inverses d'éléments de A.

Application de la méthode : voir les exercices 7, 8, C.

Méthode 2 : Ordre d'un élément d'un groupe

► Pour montrer qu'un élément a d'un groupe (noté multiplicativement) est d'ordre p, démontrez que $a^p = e$ et que, pour tout diviseur q de p distinct de p, $a^q \neq e$.

Application de la méthode : voir les exercices 1, 2, 3, D.

Méthode 3 : Groupe cyclique

► Pour montrer qu'un groupe G de cardinal n est cyclique, vous pouvez :
- trouver un élément d'ordre n dans G ;
- trouver un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et G ;
- conclure immédiatement si n est un nombre premier.

Application de la méthode : voir les exercices 1, 4.

Méthode 4 : Éléments générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$

► Pour montrer que la classe d'un entier k modulo n est d'ordre n dans le groupe Z/nZ, démontrez que k est premier avec n.

Application de la méthode : voir les exercices 5, 6.

EXERCICES

Vrai ou Faux

		Vrai	Faux
a)	L'ensemble des transpositions est une partie génératrice du groupe symétrique $\mathscr{S}_n$.	☐	☐
b)	La réunion d'une famille de sous-groupes de G est un sous-groupe de G.	☐	☐
c)	Dans le groupe $(\mathbb{R},+)$, le sous-groupe $\mathbb{Q}$ est monogène.	☐	☐
d)	Dans le groupe $\mathbb{Z}/p\mathbb{Z}$ où p est premier, tous les éléments sauf $\overline{0}$ sont générateurs.	☐	☐
e)	Si p est un nombre premier, le groupe $\mathbb{Z}/p\mathbb{Z}$ n'a que deux sous-groupes : $\{\overline{0}\}$ et lui-même.	☐	☐
f)	Un élément x d'un groupe $(G,\times)$ est d'ordre m si et seulement si $x^m = e$.	☐	☐
g)	Tout groupe monogène est isomorphe à $(\mathbb{Z},+)$ ou à un groupe $(\mathbb{Z}/n\mathbb{Z},+)$ avec $n \in \mathbb{N}^*$.	☐	☐
h)	Tout groupe de cardinal 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.	☐	☐

Exercices d'application du chapitre 1

Si vous êtes bloqué pour démarrer un exercice d'application, rendez-vous à la fin de la partie Exercices, rubrique « Aides à la résolution des exercices ».

●○○ **EXERCICE 1**

Soit G et H deux groupes, g un élément d'ordre p de G et h un élément d'ordre q de H. Que peut-on dire de l'ordre de (g,h) dans le groupe $G \times H$?
Montrer que si G et H sont cycliques de cardinaux premiers entre eux, alors $G \times H$ est cyclique.

●○○ **EXERCICE 2**

Soit G un groupe abélien, x et y deux éléments de G dont les ordres respectifs p et q sont premiers entre eux. Montrer que xy est d'ordre pq.

●○○ **EXERCICE 3**

Soit f un morphisme de groupes de G dans G' et x un élément de G d'ordre fini p.
Que peut-on dire de l'ordre de $f(x)$ dans G' ?
Application : trouver tous les morphismes de groupes de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/15\mathbb{Z}$, puis de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$.

●○○ **EXERCICE 4**

Un groupe abélien G d'élément neutre 0_G est dit *simple* s'il n'est pas réduit à $\{0_G\}$ et s'il ne possède pas d'autre sous-groupe que $\{0_G\}$ et G.

1) À quelle condition le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est-il simple ?
2) Montrer qu'un groupe abélien fini est simple si et seulement si il est cyclique de cardinal premier.

●●○ **EXERCICE 5**

Soit $n \in \mathbb{N}^*$ et H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Soit G l'ensemble des entiers relatifs dont la classe modulo n appartient à H. Montrer que G est un sous-groupe de $\mathbb{Z}$, donc de la forme $m\mathbb{Z}$ avec $m \in \mathbb{N}^*$. Montrer que m est un diviseur de n et que H est engendré par la classe de m.
Déterminer tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$. Exemples : sous-groupes de $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$.

●●○ **EXERCICE 6**

Un polygone à n côtés (n entier supérieur ou égal à 3) est dit régulier s'il est inscrit dans un cercle et que tous ses côtés ont la même longueur. Il peut être convexe ou croisé (ses côtés peuvent se croiser en dehors de leurs extrémités). On peut supposer sans nuire à la généralité que ce cercle est de centre O, de rayon 1 et que le point d'affixe 1 est l'un des sommets du polygone.
Combien de formes distinctes peut prendre un polygone régulier à n côtés ?
Dessinez, par exemple, toutes les formes de carré ($n = 4$), de pentagone régulier ($n = 5$), d'hexagone régulier ($n = 6$) et d'heptagone régulier ($n = 7$).

●●○ **EXERCICE 7**

Considérons les applications de $\mathbb{R} \setminus \{0, 1\}$ dans lui-même :

$$f_1 : x \mapsto x,\ \ f_2 : x \mapsto 1-x,\ \ f_3 : x \mapsto \frac{1}{1-x},\ \ f_4 : x \mapsto \frac{1}{x},\ \ f_5 : x \mapsto \frac{x}{x-1},\ \ f_6 : x \mapsto \frac{x-1}{x}.$$

1) Démontrer que $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ est un groupe pour la composition.
2) Déterminer tous ses sous-groupes.
3) Déterminer le sous-groupe de G engendré par les parties suivantes : $\{f_2\}$; $\{f_3\}$; $\{f_2, f_3\}$.

●●○ **EXERCICE 8**

On appelle matrice de transvection d'ordre 2 une matrice de la forme $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ ou $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, avec $a \in \mathbb{R}$.
Montrer que l'ensemble des matrices de transvection d'ordre 2 engendrent le *groupe spécial linéaire* $\mathrm{SL}_2(\mathbb{R})$, composé des matrices de $\mathscr{M}_2(\mathbb{R})$ de déterminant 1.

Exercices d'approfondissement du chapitre 1

Si vous êtes bloqué pour démarrer un exercice d'approfondissement, rendez-vous à la fin de la partie Exercices, rubrique « Aides à la résolution des exercices ».

●○○ **EXERCICE A**

Soit G un groupe fini et f un morphisme non constant de G dans le groupe multiplicatif $\mathbb{C}^*$. Déterminer la somme $\displaystyle\sum_{x \in G} f(x)$.

●○○ **EXERCICE B**

Soit $G, \cdot)$ un groupe abélien, d'élément neutre e, et H un sous-groupe de G.

1) Montrer que la relation $\mathscr{R}$ définie dans G par :

$$\forall (x, y) \in G^2, \qquad x \mathscr{R} y \quad \Longleftrightarrow \quad x \cdot y^{-1} \in H$$

est une relation d'équivalence.

2) On note $\overline{x}$ la classe d'équivalence d'un élément x de G et G/H l'ensemble des classes d'équivalence. Pour tout $(x,y)\in G^2$, on pose $\overline{x}*\overline{y} = \overline{x\cdot y}$.
   a) Quelle hypothèse est faite implicitement par cette définition ? Est-elle vérifiée ?
   b) Montrer que $(G/H,*)$ est un groupe abélien.
   On l'appelle groupe quotient de G par H.

●●○ **EXERCICE C**

Soit A et B deux sous-groupes d'un groupe G. On pose $AB=\{ab\in G,\ a\in A,\ b\in B\}$. Montrer que AB est un sous-groupe de G si et seulement si $AB=BA$. Montrer que c'est alors le sous-groupe de G engendré par $A\cup B$.

●●● **EXERCICE D**

Soit G un groupe de cardinal 35. Démontrer que G contient au moins un élément d'ordre 7 et un élément d'ordre 5.

●●● **EXERCICE E**

Soit G un groupe, noté multiplicativement, d'élément neutre e. On suppose qu'il existe dans G deux éléments a et b distincts de e tels que $aba=b$.

1) Montrer que $ab=ba^{-1}$ et $ba=a^{-1}b$.
2) a) Montrer que : $\forall j\in\mathbb{Z},\quad a^jb=ba^{-j}$.
   b) Montrer que : $\forall (j,k)\in\mathbb{Z}^2,\quad a^jb^k=b^ka^{(-1)^kj}$.
3) Soit $H=\{a^jb^k,\ (j,k)\in\mathbb{Z}^2\}$. Montrer que H est le sous-groupe de G engendré par $\{a,b\}$.
4) On suppose que a est d'ordre n et b d'ordre m, où n et m sont deux entiers naturels premiers entre eux.
   a) Montrer que : $\forall (j,k)\in\mathbb{Z}^2,\quad a^j=b^k \Rightarrow j\in n\mathbb{Z}$ et $k\in m\mathbb{Z}$.
   b) En déduire que tout élément de H s'écrit de façon unique sous la forme $a^{j_0}b^{k_0}$, où $j_0\in[\![0,n-1]\!]$ et $k_0\in[\![0,m-1]\!]$.
   c) En déduire le cardinal de H.
5) Soit G le groupe des bijections de $\mathbb{C}$ dans $\mathbb{C}$. Déterminer le cardinal du sous-groupe H de G, engendré par les applications r et s définies par :
$$\begin{cases} r: & z\mapsto jz \quad \text{où} \quad j=e^{\frac{2i\pi}{3}} \\ s: & z\mapsto\overline{z}\end{cases}.$$
   Interpréter géométriquement chaque élément de H.

EXERCICES

Sujets de concours

●○○ **SUJET I** **Oral Mines-Telecom**

Les groupes $(\mathbb{Z}/8\mathbb{Z},+)$ et $(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z},+)$ sont-ils isomorphes ?

●○○ **SUJET II** **Oral CCINP**

Pour $\theta\in\mathbb{R}$, on définit les matrices :
$$A(\theta)=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\quad\text{et}\quad A'(\theta)=\begin{pmatrix}\mathrm{ch}\theta & \mathrm{sh}\theta\\ \mathrm{sh}\theta & \mathrm{ch}\theta\end{pmatrix}.$$
Montrer que les ensembles $G=\{A(\theta),\ \theta\in\mathbb{R}\}$ et $G'=\{A'(\theta),\ \theta\in\mathbb{R}\}$, munis de la multiplication matricielle, sont des groupes. Sont-ils isomorphes ?
Indication : résoudre l'équation $X^2=\mathrm{I}_2$ dans G et dans G'.

●○○ **SUJET III** **Oral Mines-Ponts**

Soit p un nombre premier supérieur ou égal à 3. Soit G l'ensemble des matrices de la forme :

$$M(a,b,c) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{où } (a,b,c) \in \left(\mathbb{Z}/p\mathbb{Z}\right)^3.$$

1) Montrer que G est un groupe multiplicatif.
2) Quel est le cardinal de G ?
3) Déterminer l'ordre de chaque élément de G.

●●○ **SUJET IV** **Oral Mines-Ponts**

1) Soit G un groupe fini tel que, pour tout $x \in G$, $x^2 = e$.
   a) Montrer que G est abélien.

   On suppose que $G \neq \{e\}$; soit a un élément de G distinct de e.
   b) Montrer que $H = \{e, a\}$ est un sous-groupe de G.
   c) En déduire que le cardinal de G est pair.
   d) On définit dans G la relation $x \mathscr{R} y \iff x y^{-1} \in H$. Montrer que $\mathscr{R}$ est une relation d'équivalence et que l'ensemble des classes d'équivalence, noté G/H, peut être muni d'une structure de groupe.
   e) Quel est le cardinal du groupe quotient G/H ?
   f) En déduire que le cardinal de G est une puissance de 2.
2) Soit G un groupe de cardinal $2p$, où p est un nombre premier. Montrer que G contient au moins un élément d'ordre p.

●●○ **SUJET V** **Oral Centrale MP**

Soit p un nombre premier. On pose $G_p = \{z \in \mathbb{C},\ \exists k \in \mathbb{N},\ z^{p^k} = 1\}$.

1) Montrer que G_p est un sous-groupe de $(\mathbb{C}^*, \times)$. On l'appelle *p-groupe de Prüfer*.
2) Décrire G_p à l'aide des groupes cycliques U_{p^k} des racines p^k-ièmes de l'unité.
3) Montrer que les sous-groupes stricts de G_p sont cycliques et qu'aucun d'eux n'est maximal pour l'inclusion.
4) Montrer que G_p n'est pas engendré par un système fini d'éléments.

●●● **SUJET VI** **Oral X MP**

Soit G un groupe abélien de cardinal pq où p et q sont deux nombres premiers distincts. Montrer que G est cyclique.

●●● **SUJET VII** **Oral X MP**

1) Soit G un groupe abélien fini. Montrer qu'il existe un élément z de G dont l'ordre est le PPCM des ordres de tous les éléments de G.
2) Soit $\mathbb{K}$ un corps (commutatif). Démontrer que tout sous-groupe fini du groupe multiplicatif $\mathbb{K}^*$ est cyclique.

Aides à la résolution des exercices

Exercices d'application du chapitre 1

Exercice 1. Que peut-on dire de l'ordre du couple (g,h) où g et h sont des éléments générateurs respectifs de G et H ?

Exercice 2. Montrez que r et pq se divisent mutuellement.

Exercice 3.
Montrez que l'ordre de $f(x)$ divise celui de x.
Dans chaque exemple, cherchez les images possibles d'un élément générateur du groupe de départ.

Exercice 4. Montrez que $(\mathbb{Z}/n\mathbb{Z},+)$ est simple si et seulement si n est premier.

Exercice 5. Que peut-on dire de l'image réciproque d'un sous-groupe par un morphisme de groupes ?

Exercice 6. Décrivez la suite des affixes des sommets du polygone.

Exercice 7.
1) De quel groupe $(G,\circ)$ pourrait-il bien être un sous-groupe ? Calculez toutes les composées des éléments de G deux à deux. Que pouvez-vous en déduire ?
2) Cherchez les sous-groupes de G à $1,2,\ldots,6$ éléments. Y a-t-il des sous-groupes à 4 ou 5 éléments ? Pourquoi ?
3) Souvenez-vous de la caractérisation du sous-groupe engendré par une partie.

Exercice 8. Cherchez la forme que peut prendre un produit de matrices de transvection et montrez que toute matrice de $\mathrm{SL}_2(\mathbb{R})$ peut s'écrire sous cette forme.

Exercices d'approfondissement du chapitre 1

Exercice A. Pour tout $a \in G$, l'application $x \mapsto ax$ est une bijection de G dans G.

Exercice B. On peut s'inspirer de la construction du groupe $\mathbb{Z}/n\mathbb{Z}$ (paragraphe 3.2.).

Exercice C. En supposant que AB est un sous-groupe de G, montrez que $AB \subset BA$ et $BA \subset AB$.

Exercice D. Le cas où G est cyclique est très simple. Si G n'est pas cyclique, supposez qu'il n'existe aucun élément d'ordre 5 ; faites un dessin.

Exercice E.
3) a) Commencez par le cas $j \in \mathbb{N}$, par récurrence.
   b) De même pour k.
4) Montrez que H est un sous-groupe de G et que tout sous-groupe de G qui contient a et b contient H.
5) a) Montrez que $a^{mj} = e$ et $b^{nk} = e$.
   b) Pensez à la division euclidienne.
   c) Combien y a-t-il de couples (j_0, k_0) ?
6) Montrez que $rsr = s$.

EXERCICES

CORRIGÉS

Corrigés des Vrai/Faux

a) Vrai.
b) Faux, en général. Par exemple, $2\mathbb{Z}\cup 3\mathbb{Z}$ n'est pas stable par addition ($2+3\notin 2\mathbb{Z}\cup 3\mathbb{Z}$).
c) Faux. Il n'existe aucun rationnel r_0 tel que tout rationnel r s'écrive sous la forme $r = n\,r_0$, avec $n\in\mathbb{Z}$.
d) Vrai.
e) Vrai.
f) Faux. Il faut qu'il n'y ait pas d'entier $k\in[\![1, m-1]\!]$ tel que $x^k = e$.
g) Vrai.
h) Faux. Le groupe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

Corrigés des exercices d'application

EXERCICE 1

L'ordre de (g,h) est le PPCM des ordres de g et de h. Si G et H sont cycliques d'ordres a et b premiers entre eux, alors G possède au moins un élément g d'ordre a, et H un élément h d'ordre b. L'élément (g,h) est d'ordre ab dans $G\times H$, qui est donc cyclique.

EXERCICE 2

Soit r l'ordre de xy. Il vient $(xy)^{pq} = (x^p)^q(y^q)^p = e$, donc r divise pq.
Réciproquement, $(xy)^r = x^r y^r = e$ implique $x^r = y^{-r}$. D'où, $x^{qr} = y^{-qr} = e$. On en déduit que p divise qr ; comme il est premier avec q, il divise r. On montre de même que q divise r. Comme $p\wedge q = 1$, le produit pq divise r.
En définitive, $r = pq$.

EXERCICE 3

Si $x^p = e$, alors $f(x)^p = e'$: l'ordre de $f(x)$ est un diviseur de p.
Le groupe $\mathbb{Z}/7\mathbb{Z}$ possède un élément d'ordre 1 et six éléments d'ordre 7 : leurs images ne peuvent être que d'ordre 1 dans $\mathbb{Z}/15\mathbb{Z}$; le seul morphisme possible est l'application nulle.
Le groupe $\mathbb{Z}/4\mathbb{Z}$ possède deux éléments d'ordre 4, à savoir $\overline{1}$ et $\overline{3}$. Leurs images dans $\mathbb{Z}/12\mathbb{Z}$ ne peuvent être que $\overline{0}$, $\overline{3}$, $\overline{6}$, $\overline{9}$, d'où quatre morphismes possibles (chacun étant entièrement défini par l'image de $\overline{1}$).

EXERCICE 4

1) Si n est premier, alors le cardinal d'un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ ne peut être que 1 ou n : il est simple. Réciproquement, si $\mathbb{Z}/n\mathbb{Z}$ est simple, soit p un diviseur de n ; l'élément $\overline{p}$ engendre un sous-groupe de cardinal n/p, donc $n/p = 1$ ou $n/p = n$, soit $p = n$ ou $p = 1$: n est premier.
2) Si G est un groupe cyclique de cardinal n premier, il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ donc simple. Réciproquement, soit G un groupe fini simple de cardinal n. Tout élément distinct de 0_G est d'ordre n, donc engendre G. On en déduit que G est cyclique, donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$: n est premier.

EXERCICE 5

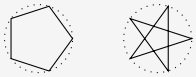
G est l'image réciproque du sous-groupe H par le morphisme $k \mapsto \overline{k}$, surjection canonique de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$; c'est donc un sous-groupe de $\mathbb{Z}$, de la forme $m\mathbb{Z}$. Comme $\overline{n} = \overline{0} \in H$, il vient $n \in m\mathbb{Z}$: ainsi m divise n.
Pour tout $\overline{x} \in H$, nous avons $x \in m\mathbb{Z}$, c'est-à-dire qu'il existe un entier k tel que $x = km$, d'où $\overline{x} = k\overline{m}$: $\overline{m}$ engendre H.
Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont donc les groupes cycliques engendrés par les diviseurs de n.

- Sous-groupes de $\mathbb{Z}/4\mathbb{Z}$: $<\overline{1}>=\mathbb{Z}/4\mathbb{Z}$; $<\overline{2}>=\{\overline{0},\overline{2}\}$; $<\overline{4}>=\{\overline{0}\}$.
- Sous-groupes de $\mathbb{Z}/6\mathbb{Z}$: $<\overline{1}>=\mathbb{Z}/6\mathbb{Z}$; $<\overline{2}>=\{\overline{0},\overline{2},\overline{4}\}$; $<\overline{3}>=\{\overline{0},\overline{3}\}$; $<\overline{6}>=\{\overline{0}\}$.
- Sous-groupes de $\mathbb{Z}/12\mathbb{Z}$: $<\overline{1}>=\mathbb{Z}/12\mathbb{Z}$; $<\overline{2}>=\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10}\}$; $<\overline{3}>=\{\overline{0},\overline{3},\overline{6},\overline{9}\}$;

$<\overline{4}>=\{\overline{0},\overline{4},\overline{8}\}$; $<\overline{6}>=\{\overline{0},\overline{6}\}$; $<\overline{12}>=\{\overline{0}\}$.

EXERCICE 6

Un polygone régulier à n côtés est invariant par la rotation de centre O qui permet de passer d'un sommet au suivant. Par conséquent, l'ensemble des affixes des sommets est de la forme $(1, e^{i\theta}, e^{2i\theta}, \ldots, e^{(n-1)i\theta})$ où $e^{i\theta}$ est un élément d'ordre n du groupe $(\mathbb{C}^*, \times)$, c'est-à-dire un élément générateur du groupe $\mathscr{U}_n$ des racines n-ièmes de l'unité. Ce qui signifie que $\theta = k(2\pi/n)$, où k est un entier premier avec n. Le nombre de valeurs correspondantes de $e^{i\theta}$ est donc $\varphi(n)$, où φ est l'indicatrice d'Euler. On remarque que les valeurs $e^{i\theta}$ et $e^{-i\theta}$ définissent le même polygone régulier, parcouru dans un sens ou dans l'autre. Le nombre de polygones réguliers à n côtés est donc $\dfrac{\varphi(n)}{2}$.

- $\dfrac{\varphi(4)}{2} = 1$: il n'existe qu'une seule forme de carré :
- $\dfrac{\varphi(5)}{2} = 2$: il existe deux formes de pentagones réguliers : 
- $\dfrac{\varphi(6)}{2} = 1$: il n'existe qu'une seule forme d'hexagone régulier :
- $\dfrac{\varphi(4)}{2} = 3$: il existe trois formes d'heptagones réguliers :

EXERCICE 7

1) Construisons la table de G :

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_6	f_5	f_2	f_1
f_4	f_4	f_3	f_2	f_1	f_6	f_5
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_1	f_2	f_4	f_3

L'ensemble G est non vide, stable par composition et il contient les inverses de ses éléments : c'est donc un sous-groupe du groupe des bijections de $\mathbb{R} \setminus \{0, 1\}$ dans lui-même.

CORRIGÉS

2) Cherchons les sous-groupes de G par nombre d'éléments :
- seul sous-groupe de G à un élément : $\{f_1\}$;
- sous-groupes de G à deux éléments : $\{f_1, f_2\}$, $\{f_1, f_4\}$, $\{f_1, f_5\}$;
- seul sous-groupe de G à trois éléments : $\{f_1, f_3, f_6\}$;
- tout sous-groupe contenant au moins quatre éléments est G tout entier.

3) Le sous-groupe engendré par $\{f_2\}$ (plus petit sous-groupe contenant f_2) est $\{f_1, f_2\}$.
Le sous-groupe engendré par $\{f_3\}$ (plus petit sous-groupe contenant f_3) est $\{f_1, f_3, f_6\}$.
Le sous-groupe engendré par $\{f_2, f_3\}$ (plus petit sous-groupe contenant f_2 et f_3) est G.

EXERCICE 8

On montre d'abord très facilement que toute matrice de transvection d'ordre 2 a pour déterminant 1 et que l'ensemble $\mathrm{SL}_2(\mathbb{R})$ des matrices carrées de taille 2 de déterminant 1 est bien un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.
On s'aperçoit ensuite que l'ensemble des matrices de la forme $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ est un sous-groupe de $\mathrm{SL}_2(\mathbb{R})$, de même que l'ensemble des matrices de la forme $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$. Pour espérer obtenir une matrice quelconque de $\mathrm{SL}_2(\mathbb{R})$, il faut donc effectuer un produit de matrices de ces deux ensembles. Essayons le produit :

$$M(x, y, z) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}.$$

Tous calculs faits, on obtient :

$$M(x, y, z) = \begin{pmatrix} 1+xy & x+z+xyz \\ y & yz+1 \end{pmatrix}.$$

Soit maintenant une matrice quelconque de $\mathrm{SL}_2(\mathbb{R})$: $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, avec $ad - bc = 1$.
On aura $M(x, y, z) = A$ si et seulement si :

$$\left\{\begin{array}{rcl} 1+xy & = & a \\ x+z+xyz & = & b \\ y & = & c \\ yz+1 & = & d \end{array}\right. .$$

Supposons $c \neq 0$. D'où : $y = c$, $x = \dfrac{a-1}{c}$, $z = \dfrac{d-1}{c}$. Réciproquement, ce triplet (x, y, z) vérifie le système, donc l'égalité $M(x, y, z) = A$.
Dans le cas où $b \neq 0$, il suffit d'examiner le produit :

$$M(x, y, z) = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}.$$

On conclut de la même façon.
Dans le cas où $b = c = 0$, on a :

$$A = \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & -1/a \\ 0 & 1/a \end{pmatrix}.$$

On est ramené à une matrice de la forme $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ avec $ad = 1$ et $b \neq 0$, dont on a vu plus haut qu'elle est un produit de matrices de transvection.
Conclusion : toute matrice du groupe $\mathrm{SL}_2(\mathbb{R})$ est un produit de matrices de transvection. D'après la proposition 1.4, ce groupe est engendré par les matrices de transvection.

Corrigés des exercices d'approfondissement

EXERCICE A

Comme f n'est pas constant, il existe $a \in G$ tel que $f(a) \neq 1$. L'application $x \mapsto ax$ est une bijection de G dans G, donc :

$$\sum_{x\in G} f(x) = \sum_{x\in G} f(ax) = f(a)\sum_{x\in G} f(x).$$

Or $f(a) \neq 1$, on en déduit : $\displaystyle\sum_{x\in G} f(x) = 0$.

EXERCICE B

1) La relation $\mathscr{R}$ est :
- réflexive, car pour tout $x \in G$, $x \cdot x^{-1} = e \in H$;
- symétrique, car pour tout $(x, y) \in G^2$, si $x \cdot y^{-1} \in H$, alors $(x \cdot y^{-1})^{-1} = x \cdot y^{-1}) \in H$;
- transitive, car pour tout $(x, y) \in G^3$, si $x \cdot y^{-1} \in H$ et $y \cdot z^{-1} \in H$, alors :

$$(x \cdot y^{-1})^{-1} \cdot y \cdot z^{-1} = x \cdot z^{-1} \in H.$$

2) a) Pour que cette définition ait un sens, il faut s'assurer que la classe de $x \cdot y$ ne dépend que des classes de x et de y et non de représentants particuliers de ces classes.
Soit (x, x') et (y, y') dans G^2 tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$. Montrons que $\overline{x \cdot y} = \overline{x' \cdot y'}$.
Si $x \cdot x'^{-1} \in H$ et $y \cdot y'^{-1} \in H$, alors :

$$(x \cdot y)\cdot(x' \cdot y')^{-1} = x \cdot y \cdot y'^{-1} \cdot x'^{-1} = (x \cdot x'^{-1})\cdot(y \cdot y'^{-1}) \in H.$$

La définition de la loi $*$ dans G/H est bien validée.
On remarquera que dans la dernière égalité, on a utilisé la commutativité du groupe G. Dans un groupe non abélien, cette construction n'est plus valide pour un sous-groupe quelconque, mais uniquement pour certains d'entre eux appelés sous-groupes distingués. Cette notion n'est pas au programme.

b) On montre alors sans difficulté que la loi $*$ est associative, qu'elle possède un élément neutre qui est $\overline{e}$, et que tout élément $\overline{x}$ possède un inverse, qui est $\overline{x^{-1}}$. Ainsi $(G/H, *)$ est un groupe.

EXERCICE C

Supposons que $AB = BA$. L'ensemble AB est non vide, car il contient $e = ee$. Soit $x = ab$ et $y = a'b'$ deux éléments de AB (avec $(a, a') \in A^2$ et $(b, b') \in B^2$). Alors $xy^{-1} = abb'^{-1}a'^{-1}$. Or abb'^{-1} appartient à AB, donc à BA : il existe $a'' \in A$, $b'' \in B$ tels que $abb'^{-1} = b''a''$. On en déduit que $xy^{-1} = b''a''a'^{-1}$, qui appartient à BA donc à AB. AB est un sous-groupe de G.

Supposons maintenant que AB soit un sous-groupe de G :
• soit $x = ab$ un élément de AB (avec $(a, b) \in A \times B$). x^{-1} est encore élément de AB, c'est-à-dire qu'il existe $(a', b') \in A \times B$ tel que $x^{-1} = a'b'$, d'où $x = b'^{-1}a'^{-1}$, qui est élément de BA : $AB \subset BA$;
• soit $x = ba$ un élément de BA (avec $(a, b) \in A \times B$). Puisque $b = e \cdot b$ et $a = a \cdot e$ sont des éléments de AB, qui est stable par la loi de G, il vient $x \in AB$: $BA \subset AB$. En définitive, $AB = BA$.

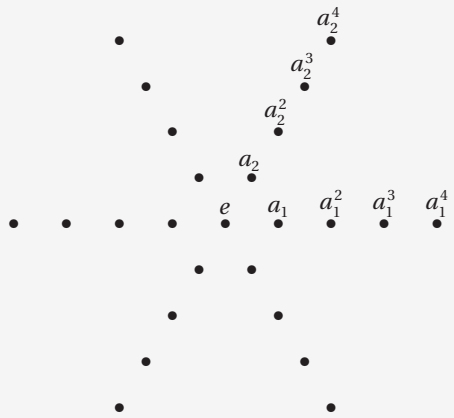
Dans ce cas, le sous-groupe AB contient A et B, et tout sous-groupe contenant A et B contient AB : AB est le plus petit sous-groupe de G contenant A et B.

CORRIGÉS

EXERCICE D

Tous les éléments de G ont pour ordre 1, 5, 7 ou 35.
• Si G est cyclique, il possède un élément a d'ordre 35, donc $a^{35} = e$, c'est-à-dire $(a^7)^5 = e$. L'entier 5 est le plus petit entier $n > 0$ tel que $(a^7)^n = e$, car sinon on aurait $a^{7n} = e$ avec $7n < 35$, ce qui est absurde. Donc l'élément a^7 est d'ordre 5. On montre de même que a^5 est d'ordre 7.
• Supposons maintenant que G n'est pas cyclique et qu'il ne possède aucun élément d'ordre 7. Alors tous les éléments distincts de e sont d'ordre 5.
Soit $a_1 \neq e$, le groupe engendré par a_1 est $< a_1 >= \{e, a_1, a_1^2, a_1^3, a_1^4\}$.
Pour tout élément $a_2 \notin < a_1 >$, $< a_2 >= \{e, a_2, a_2^2, a_2^3, a_2^4\}$ et $< a_1 > \cap < a_2 >= \{e\}$. Si on réitère cette opération ; on obtient une suite finie $(a_1, a_2, \ldots, a_p)$ telle que pour tout $k \in [\![2, p]\!]$, $a_k \notin \bigcup_{1 \leqslant i < k} < a_i >$.

On a alors $\left| \bigcup_{1 \leqslant i \leqslant p} < a_i > \right| = 4p + 1$.



Cette réunion ne peut pas être égale à G puisque 35 n'est pas congru à 1 modulo 4. Donc il existe bien au moins un élément d'ordre 7.
On peut montrer de même qu'il existe dans G au moins un élément d'ordre 5, puisque 35 n'est pas congru à 1 modulo 6.

EXERCICE E

1) En multipliant l'égalité $aba = b$, respectivement à droite ou à gauche, par a^{-1}, on obtient :

$$ab = ba^{-1} \quad ; \quad ba = a^{-1}b.$$

2) a) Montrons d'abord la proposition par récurrence pour j entier naturel :
• L'égalité est évidente pour $j = 0$.
• Soit $j \in \mathbb{N}$ tel que $a^j b = ba^{-j}$. Par associativité de la loi et d'après l'hypothèse de récurrence :

$$a^{j+1}b = a(a^j b) = a(ba^{-j}) = (ab)a^{-j} = (ba^{-1})a^{-j} = ba^{-(j+1)}.$$

L'égalité $a^j b = ba^{-j}$ est donc établie pour tout entier j positif.
En multipliant l'égalité $a^j b = ba^{-j}$ à gauche par a^{-j} et à droite par a^j, il vient :

$$a^{-j}b = ba^j,$$

ce qui prouve la proposition pour l'entier négatif $-j$ et, par conséquent, pour tout entier relatif.

b) De la même façon, commençons par démontrer la proposition par récurrence pour k entier naturel.
- L'égalité est évidente pour $k=0$.
- Soit $k \in \mathbb{N}$ tel que, pour tout $j \in \mathbb{Z}$, $a^j b^k = b^k a^{(-1)^k j}$. On a alors :

$$a^j b^{k+1} = a^j b^k \cdot b = b^k a^{(-1)^k j} b = b^k b a^{-(-1)^k j} = b^{k+1} a^{(-1)^{k+1} j}.$$

L'égalité $a^j b^k = b^k a^{(-1)^k j}$ est donc établie pour tout entier k positif.
En multipliant cette égalité à gauche et à droite par b^{-k}, nous obtenons :

$$b^{-k} a^j = a^{(-1)^k j} b^{-k} \quad \text{pour tout } j \in \mathbb{Z}.$$

En remplaçant j par $(-1)^k j$, il vient :

$$a^j b^{-k} = b^{-k} a^{(-1)^k j},$$

ce qui prouve la proposition pour l'entier négatif $-k$ et, par conséquent, pour tout entier relatif.
3) L'ensemble H est non vide, car il contient a et b.
Montrons qu'il est stable par la loi de G : soit $x = a^j b^k$ et $y = a^{j'} b^{k'}$ deux éléments de H.

$$x y = a^j b^k a^{j'} b^{k'} = a^j a^{(-1)^k j'} b^k b^{k'} = a^{j+(-1)^k j'} b^{k+k'}.$$

Donc $x y \in H$.

Montrons que H contient les inverses de tous ses éléments. Soit $x = a^j b^k \in H$:

$$x^{-1} = b^{-k} a^{-j} = a^{(-1)^{k+1} j} b^{-k} \in H.$$

L'ensemble H est donc un sous-groupe de G contenant a et b. Or tout sous-groupe de G contenant a et b contient nécessairement $a^j b^k$ pour tout $(j,k) \in \mathbb{Z}^2$. H est donc le plus petit sous-groupe contenant a et b, c'est-à-dire le sous-groupe engendré par $\{a, b\}$.
4) a) Soit j et k deux entiers tels que $a^j = b^k$. On a alors :

$$a^{mj} = b^{mk} = (b^m)^k = e.$$

L'entier mj est donc un multiple de l'ordre de a : n divise mj. D'après le théorème de Gauss, comme n est premier avec m, n divise j.
De même :

$$b^{nk} = a^{nj} = (a^n)^j = e.$$

L'entier nk est donc un multiple de l'ordre de b : m divise nk. D'après le théorème de Gauss, comme m est premier avec n, m divise k.
b) Soit $x = a^j b^k \in H$, avec $(j,k) \in \mathbb{Z}^2$. Effectuons les divisions euclidiennes de j par n et de k par m :

$$\begin{array}{rcll} j & = & qn + j_0 & \text{où} \quad j_0 \in [\![0, n-1]\!]; \\ k & = & q'm + k_0 & \text{où} \quad k_0 \in [\![0, m-1]\!]. \end{array}$$

$$x = a^{qn+j_0} b^{q'm+k_0} = a^{j_0} b^{k_0}.$$

Montrons que cette écriture est unique ; supposons qu'il existe des entiers $j_1 \in [\![0, n-1]\!]$ et $k_1 \in [\![0, m-1]\!]$ tels que :

$$x = a^{j_0} b^{k_0} = a^{j_1} b^{k_1}.$$

On a alors : $a^{j_0 - j_1} = b^{k_1 - k_0}$. D'après le résultat de la question 4) a) :

$$j_0 - j_1 \in n\mathbb{Z} \quad \text{et} \quad k_1 - k_0 \in m\mathbb{Z},$$

ce qui implique : $j_0 = j_1$ et $k_0 = k_1$.
Tout élément x de H s'écrit donc de façon unique sous la forme $a^{j_0} b^{k_0}$ avec $j_0 \in [\![0, n-1]\!]$ et $k_0 \in [\![0, m-1]\!]$.
c) Par conséquent :

$$|H| = \left|[\![0, n-1]\!] \times [\![0, m-1]\!]\right| = nm.$$

CORRIGÉS

5) Déterminons l'application rsr :

$$\forall z \in \mathbb{C}, \quad rsr(z) = j(\overline{jz}) = j\overline{j}\overline{z} = \overline{z} = s(z).$$

Donc $rsr = s$. De plus, $r^3 = \mathrm{Id}_{\mathbb{C}}$ et $s^2 = \mathrm{Id}_{\mathbb{C}}$. On peut appliquer les résultats des questions précédentes : le sous-groupe H est de cardinal 6 et :

$$H = \{\mathrm{Id}_{\mathbb{C}}, r, r^2, s, rs, r^2 s\}.$$

Géométriquement :
- r est la rotation de centre O d'angle $\frac{2\pi}{3}$;
- r^2 est la rotation de centre O d'angle $\frac{4\pi}{3}$;
- s est la symétrie par rapport à l'axe des réels ;
- rs est la symétrie par rapport à la droite passant par O et d'angle polaire $\frac{\pi}{3}$;
- $r^2 s$ est la symétrie par rapport à la droite passant par O et d'angle polaire $\frac{2\pi}{3}$.

Corrigés des sujets de concours

SUJET I

Le groupe $(\mathbb{Z}/8\mathbb{Z}, +)$ est cyclique, tandis que pour tout $(x, y) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$: $4(x, y) = (4x, 4y) = (0, 0)$; tous les éléments du groupe $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, +)$ ont un ordre au plus égal à 4. Ce groupe n'est pas cyclique. Les deux groupes ne sont pas isomorphes.

SUJET II

Pour tout $\theta \in \mathbb{R}$, $\det A(\theta) = \det A'(\theta) = 1 \neq 0$, donc $A(\theta)$ et $A'(\theta)$ appartiennent à $\mathrm{GL}_2(\mathbb{R})$. Montrons que les applications $\theta \mapsto A(\theta)$ et $\theta \mapsto A'(\theta)$ sont des morphismes du groupe $(\mathbb{R}, +)$ dans le groupe $\mathrm{GL}_2(\mathbb{R})$.

$$\begin{aligned} A(\theta)A(\theta') &= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} \cos\theta' & -\sin\theta' \\ \sin\theta' & \cos\theta' \end{pmatrix} = \begin{pmatrix} \cos(\theta+\theta') & -\sin(\theta+\theta') \\ \sin(\theta+\theta') & \cos(\theta+\theta') \end{pmatrix}, \\ A'(\theta)A'(\theta') &= \begin{pmatrix} \mathrm{ch}\theta & \mathrm{sh}\theta \\ \mathrm{sh}\theta & \mathrm{ch}\theta \end{pmatrix}\begin{pmatrix} \mathrm{ch}\theta' & \mathrm{sh}\theta' \\ \mathrm{sh}\theta' & \mathrm{ch}\theta' \end{pmatrix} = \begin{pmatrix} \mathrm{ch}(\theta+\theta') & \mathrm{sh}(\theta+\theta') \\ \mathrm{sh}(\theta+\theta') & \mathrm{ch}(\theta+\theta') \end{pmatrix}, \end{aligned}$$

ce qui prouve que $A(\theta)A(\theta') = A(\theta+\theta')$ et $A'(\theta)A'(\theta') = A'(\theta+\theta')$. Les ensembles G et G' sont les images des morphismes A et A' ; ce sont donc des sous-groupes de $\left(\mathrm{GL}_2(\mathbb{R}), \times\right)$. Le groupe G est bien connu : c'est le *groupe spécial orthogonal* $\mathrm{SO}_2(\mathbb{R})$, constitué des matrices de rotation du plan.

Soit $X = A(\theta) \in G$. Alors $X^2 = A(2\theta) = \begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}$. Donc $X^2 = \mathrm{I}_2$ équivaut à $\theta = k\pi$, avec $k \in \mathbb{Z}$.

Finalement, il y a deux solutions à $X^2 = \mathrm{I}_2$ dans G : $X = \mathrm{I}_2$ ou $X = -\mathrm{I}_2$.

De même, soit $X = A'(\theta) \in G'$. Alors, $X^2 = A'(2\theta) = \begin{pmatrix} \mathrm{ch}2\theta & \mathrm{sh}2\theta \\ \mathrm{sh}2\theta & \mathrm{ch}2\theta \end{pmatrix}$. Donc $X^2 = \mathrm{I}_2$ équivaut à $\theta = 0$. Il y a une seule solution à $X^2 = \mathrm{I}_2$ dans G : $X = \mathrm{I}_2$.

Supposons qu'il existe un isomorphisme φ de G dans G'. Alors : $\varphi(-\mathrm{I}_2)^2 = \varphi(\mathrm{I}_2) = \mathrm{I}_2$, ce qui implique, puisque $\varphi(-\mathrm{I}_2) \in G'$, que $\varphi(-\mathrm{I}_2) = \mathrm{I}_2$. L'égalité $\varphi(\mathrm{I}_2) = \varphi(-\mathrm{I}_2)$ contredit l'injectivité de φ. Finalement les groupes G et G' ne sont pas isomorphes.

SUJET III

1) On sait que $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ est un corps. Les éléments de G ont pour déterminant 1 : ils sont inversibles. Montrons que G est un sous-groupe du groupe $\mathrm{GL}_n(\mathbb{K})$.

- $M(\overline{0},\overline{0},\overline{0}) = \mathrm{I}_3$, élément neutre de $\mathrm{GL}_n(\mathbb{K})$.
- Pour tous (a,b,c) et (a',b',c') dans $\left(\mathbb{Z}/p\mathbb{Z}\right)^3$,

$$M(a,b,c) * M(a',b',c') = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix} = M(a+a', b+b'+ac', c+c') \in G.$$

- Pour tout (a,b,c) dans $\left(\mathbb{Z}/p\mathbb{Z}\right)^3$,

$$M(a,b,c)^{-1} = \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} = M(-a,-b+ac,-c) \in G.$$

Donc G est bien un groupe.

2) Sans détour : $\mathrm{Card}(G) = \mathrm{Card}\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^3\right) = p^3$.

3) L'ordre d'un élément de G est un diviseur de p^3 ; il ne peut donc être que 1, p, p^2 ou p^3. Par définition, seule la matrice I_3 est d'ordre 1. Soit $M(a,b,c)$ un élément de G distinct de I_3. Par récurrence sur n (à faire le jour J !), il vient pour tout $n \in \mathbb{N}$:

$$M(a,b,c)^n = \begin{pmatrix} 1 & na & nb + \dfrac{n(n-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix} = M\left(na, nb + \frac{n(n-1)}{2}ac, nc\right).$$

En particulier, comme p est un nombre premier impair, $\dfrac{p-1}{2} \in \mathbb{N}$ et $\dfrac{p(p-1)}{2}$ est un multiple de p. Ainsi, pa, $pb + \dfrac{p(p-1)}{2}ac$ et pc sont des multiples de p : leur classe dans $\mathbb{Z}/p\mathbb{Z}$ est nulle et par conséquent $M(a,b,c)^p = \mathrm{I}_3$. Tout élément de G distinct de I_3 est d'ordre p.

SUJET IV

1) a) Pour tout $(a,b) \in G^2$: $(ab)^{-1} = ab$, d'où $ba = ab$: G est abélien.

b) H est non vide, stable et contient les inverses de ses éléments : c'est un sous-groupe de G.

c) D'après le théorème de Lagrange, le cardinal de G est multiple de celui de H, donc pair.

d) On peut faire une construction analogue à celle du groupe $\mathbb{Z}/n\mathbb{Z}$ (paragraphe 3.2. et exercice d'approfondissement B).

e) Pour tout $x \in G$, $\overline{x} = \{x, ax\}$. Le cardinal de G/H est donc $|G|/2$.

f) Pour tout $\overline{x} \in G/H$, $\overline{x}^2 = \overline{e}$. Le groupe G/H a donc la même propriété que le groupe G : son cardinal est soit 1, soit pair. En itérant ce procédé, on obtient une suite de groupes dont les cardinaux sont en progression géométrique de raison 1/2. Cette suite est nécessairement finie et le cardinal de chacun de ces groupes, dont G, est une puissance de 2.

2) Pour $p = 2$, le groupe G est de cardinal 4 ; il est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dans les deux cas il possède un élément d'ordre 2.

Si $p > 2$, les ordres possibles des éléments de G sont 1, 2, p et $2p$.

- S'il existe un élément d'ordre p, alors le résultat est acquis.
- S'il existe un élément a d'ordre $2p$, alors a^2 est d'ordre p (d'ailleurs, G est cyclique).
- Supposons enfin que tous les éléments de G distincts de e soient d'ordre 2 : d'après I.6), le cardinal du groupe G est une puissance de 2, ce qui est absurde.

SUJET V

1) $G_p \subset \mathbb{C}^*$; $1 \in G_p$ donc $G_p \neq \varnothing$.

Soit $(z, z') \in G_p^2$: il existe deux entiers k et k' tels que $z^{p^k} = 1$ et $z'^{p^{k'}} = 1$. Alors :

$$\left(zz'^{-1}\right)^{p^{k+k'}} = \left(z^{p^k}\right)^{p^{k'}} \left(z'^{p^{k'}}\right)^{-p^k} = 1.$$

donc $zz'^{-1} \in G_p$. Il s'ensuit que G_p est un sous-groupe de $\mathbb{C}^*$.

2) Le groupe G_p est la réunion de la famille $(U_{p^k})_{k\in\mathbb{N}}$, croissante pour l'inclusion.

3) Soit H un sous-groupe de G_p.

S'il existe des entiers k tels que $U_{p^k} \not\subset H$, soit k_0 le plus grand entier $k \in \mathbb{N}$ tel que $U_{p^k} \subset H$.

- Si $U_{p^{k_0}} = H$, alors H est un sous-groupe cyclique de G_p.

Si H était maximal pour l'inclusion, il serait égal à la réunion G_p, ce qui est exclu.

- Si l'inclusion $U_{p^{k_0}} \subset H$ est stricte, soit z un élément de $H \backslash U_{p^{k_0}}$. Comme il existe $k_1 \in \mathbb{N}$ tel que $z \in U_{p^{k_1}}$, avec $k_1 > k_0$, alors le sous-groupe de H engendré par z est de la forme U_{p^k}, avec $k_0 < k \leqslant k_1$, donc $U_{p^k} \subset H$, ce qui est contraire à la définition de k_0. Dans ce cas, on conclut que pour tout $k \in \mathbb{N}$, $U_{p^k} \subset H$, d'où par réunion $G_p \subset H$ et donc $H = G_p$.

Conclusion : tous les sous-groupes stricts de G_p sont cycliques et non maximaux.

4) Si G_p était engendré par un nombre fini d'éléments, il existerait un entier maximal k_0 tel que $U_{p^{k_0}}$ contienne tous ces éléments et, par conséquent, $G_p \subset U_{p^{k_0}}$, ce qui est absurde.

SUJET VI

Supposons que G ne soit pas cyclique, c'est-à-dire qu'il ne contienne aucun élément d'ordre pq. Soit x un élément de $G\backslash\{e\}$. Son ordre ne peut être que p ou q, disons p pour fixer les idées. Soit y un élément de G n'appartenant pas au sous-groupe engendré par x.

Supposons que y soit aussi d'ordre p. Soit H le sous-groupe de G engendré par $\{x, y\}$. L'application $\varphi : (\overline{i}, \overline{j}) \mapsto x^i y^j$ de $(\mathbb{Z}/p\mathbb{Z})^2$ dans H est un morphisme de groupes, surjectif puisque G est abélien et $H =< x, y >$; cherchons son noyau. Remarquons que $(\overline{i}, \overline{j}) \in \operatorname{Ker} \varphi$ si et seulement si $x^i y^j = e$, c'est-à-dire $x^i = y^{-j}$. Cet élément appartient à $< x > \cap < y >$, qui est un sous-groupe strict de $< x >$, donc d'ordre 1, c'est-à-dire $\{e\}$. D'où $x^i = y^{-j} = e$, soit $(i, j) \in (p\mathbb{Z})^2$ et $(\overline{i}, \overline{j}) = (\overline{0}, \overline{0})$. Le morphisme φ est injectif ; étant déjà surjectif, il est bijectif. On en déduit que $|H| = p^2$, ce qui est absurde car p^2 ne divise pas pq. En définitive, y est d'ordre q.

Comme G est abélien et p et q premiers entre eux, l'élément xy est d'ordre pq (voir exercice 2), ce qui est contraire à l'hypothèse. Nous avons démontré par l'absurde que G était cyclique.

SUJET VII

1) Désignons par $\omega(x)$ l'ordre d'un élément x de G. Soit n le PPCM des ordres des éléments de G. Décomposons n en facteurs premiers : $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Pour tout $i \in [\![1, k]\!]$, α_i est le plus grand exposant de p_i figurant dans les décompositions en facteurs premiers des ordres des éléments de G. Il existe donc un élément y_i de G tel que α_i soit l'exposant de p_i dans la décomposition en facteurs premiers de son ordre, soit : $\omega(y_i) = p_i^{\alpha_i} m_i$, avec $m_i \wedge p_i = 1$. On a alors $\left(y_i^{m_i}\right)^{p_i^{\alpha_i}} = e$. L'ordre de $y_i^{m_i}$ divise $p_i^{\alpha_i}$, il est donc de la forme p_i^{β} avec $\beta \leqslant \alpha_i$. Si β était strictement inférieur à α_i, on aurait $\left(y_i^{m_i}\right)^{p_i^{\beta}} = e$, d'où $y_i^{p_i^{\beta} m_i} = e$, ce qui contredit la définition de l'ordre de y_i. Donc $\omega(y_i^{m_i}) = p_i^{\alpha_i}$. Les ordres des différents $y_i^{m_i}$ étant premiers entre eux deux à deux, l'ordre de leur produit $y = \prod_{i=1}^{k} y_i^{m_i}$ est n.

2) Considérons un sous-groupe fini G de cardinal N de $(\mathbb{K}^*, \cdot)$. Soit n le PPCM des ordres des éléments de G. D'après le résultat de la question précédente, il existe un élément x de G d'ordre n. D'après le théorème de Lagrange, n divise N et, par conséquent, $N \geqslant n$.
De plus, tout élément de G a pour ordre un diviseur de n et est par conséquent racine du polynôme $X^n - 1$ de $\mathbb{K}[X]$. Comme ce polynôme possède au plus n racines, on en déduit que $N \leqslant n$.
En définitive, $N = n$. L'élément x a pour ordre N : le groupe G est cyclique.

CHAPITRE 2
Compléments sur les anneaux

Plan du chapitre

Cours, p. 36 ☐
- **1** ▶ Idéaux d'un anneau commutatif, p. 36 ☐
- **2** ▶ L'anneau $\mathbb{Z}$, p. 39 ☐
- **3** ▶ Anneaux $\mathbb{Z}/n\mathbb{Z}$, p. 40 ☐
- **4** ▶ Anneaux $\mathbb{K}[X]$, p. 46 ☐
- **5** ▶ Algèbres, p. 50 ☐

Fiche synthèse, p. 53 ☐
Méthodes pas à pas, p. 55 ☐
Exercices, p. 57 ☐
Corrigés, p. 65 ☐

Objectifs et compétences du programme

Capacités principales à maîtriser	Méthodes associées	Exercices associés
Reconnaître un idéal d'un anneau.	Méthode 1	Exercices 1, 2, 3
Calculer dans Z/nZ.	Méthode 2	Exercices 4, 5, A, B, E
Raisonner dans l'anneau $\mathbb{K}[X]$.	Méthode 3	Exercices 7, F
Raisonner sur une algèbre	Méthode 4	Exercices 6, F

RETROUVEZ ICI LES FLASHCARDS INTERACTIVES POUR SE TESTER

www.lienmini.fr/212891-FLASH-02

COURS

Histoire des mathématiques

Emmy Noether, mathématicienne allemande (1882-1935)
Emmy Noether naît dans une famille juive d'Erlangen dans le royaume de Bavière. En 1915, elle est invitée par David Hilbert et Felix Klein à rejoindre le renommé département de mathématiques de l'université de Göttingen. Cependant, en raison de l'opposition de la faculté – qui refuse qu'une femme soit nommée professeur – elle doit pendant quatre ans donner des cours sous le nom de Hilbert. En 1934, chassée de l'université par les nazis, elle émigre aux États-Unis où elle rencontre Albert Einstein qui la décrit comme un « génie créatif considérable ».
Paru en 1921, son article *Idealtheorie in Ringbereichen (Théorie des idéaux dans les anneaux)* pose les fondations de la théorie générale des anneaux commutatifs, qui généralise l'étude classique de l'arithmétique des entiers et des polynômes. En son honneur, un anneau dont tous les idéaux sont engendrés par une partie finie est appelé « noetherien ».

1 Idéaux d'un anneau commutatif

1.1. Idéal d'un anneau commutatif

Définition 2.1. Idéal d'un anneau commutatif

Soit A un anneau commutatif. On appelle idéal de A une partie I de A telle que :
- $(I,+)$ est un sous-groupe de $(A,+)$;
- I est stable par la multiplication par un élément quelconque de A : $\forall x \in I$, $\forall a \in A$, $ax \in I$.

Exemples

- L'ensemble $2\mathbb{Z}$ des entiers pairs est un idéal de l'anneau $\mathbb{Z}$ des entiers.
- L'ensemble des suites convergeant vers 0 est un idéal de l'anneau des suites bornées.

Remarque
Si un idéal de l'anneau A contient l'élément unité 1_A, alors il est égal à A tout entier.

Proposition 2.2. Image directe ou réciproque d'un idéal par un morphisme

Soit A et A' deux anneaux commutatifs et f un morphisme d'anneaux de A dans A'.
- L'image directe d'un idéal de A est un idéal du sous-anneau $f(A)$.
- L'image réciproque d'un idéal de A' est un idéal de A. En particulier, $\operatorname{Ker} f$ est un idéal de A.

Démonstration

- Soit I un idéal de A. Le morphisme d'anneaux f de A dans A' est d'abord un morphisme de groupes de $(A,+)$ dans $\big(f(A),+\big)$, donc $f(I)$, image d'un sous-groupe de $(A,+)$, est un sous-groupe de $\big(f(A),+\big)$.
  De plus, pour tout $x \in f(I)$ et tout $a \in f(A)$, il existe $\xi \in I$ et $\alpha \in A$ tels que $x = f(\xi)$ et $a = f(\alpha)$.
  Alors :
  $$a\,x = f(\alpha)f(\xi) = f(\alpha\xi).$$
  Comme α appartient à A et ξ à I qui est un idéal de A, $\alpha\xi$ appartient à I et par conséquent $a\,x$ appartient à $f(I)$.
  Nous avons bien démontré que $f(I)$ est un idéal de $f(A)$ (qui est un sous-anneau de A, mais pas nécessairement un idéal de A!).
- De même, soit J un idéal de A'. L'image réciproque de J, sous-groupe de $(A',+)$, par le morphisme de groupes f est un sous-groupe de $(A,+)$. De plus, pour tout $x \in f^{-1}(J)$ et tout $a \in A$, $f(x) \in J$ et $f(a) \in A'$. Comme J est un idéal de A', $f(a)f(x) \in J$, c'est-à-dire $f(a\,x) \in J$, donc $a\,x \in f^{-1}(J)$.
  Nous avons bien démontré que $f^{-1}(J)$ est un idéal de A.
  En particulier, $\operatorname{Ker} f = f^{-1}\big(\{0_{A'}\}\big)$ et $\{0_{A'}\}$ est un idéal de A', donc $\operatorname{Ker} f$ est un idéal de A. ■

Proposition 2.3. Intersection et somme d'idéaux

Soit A un anneau commutatif :

- toute intersection d'idéaux de A est un idéal de A ;
- toute somme d'idéaux de A est un idéal de A.

Démonstration

Soit $(I_j)_{j\in J}$ une famille d'idéaux de A.

- L'intersection de cette famille est une intersection de sous-groupes de $(A,+)$; c'est donc est un sous-groupe de $(A,+)$. De plus, soit $x \in \bigcap_{j\in J} I_j$ et $a \in A$. Pour tout $j \in J$, $x \in I_j$ et comme I_j est un idéal de A, $a\,x \in I_j$. En définitive, $a\,x \in \bigcap_{j\in J} I_j$.
  Nous avons bien démontré que $\bigcap_{j\in J} I_j$ est un idéal de A.
- De même, $\sum_{j\in J} I_j$ est une somme de sous-groupes de $(A,+)$; c'est donc est un sous-groupe de $(A,+)$.
  Soit $x \in \sum_{j\in J} I_j$ et $a \in A$. Pour tout $j \in J$, il existe $x_j \in I_j$ tel que $x = \sum_{j\in J} x_j$, d'où :
  $$a\,x = a\sum_{j\in J} x_j = \sum_{j\in J} a\,x_j.$$
  Comme pour tout $j \in J$, I_j est un idéal de A, $a\,x_j \in I_j$. En définitive, $a\,x \in \sum_{j\in J} I_j$.
  Nous avons bien démontré que $\sum_{j\in J} I_j$ est un idéal de A. ■

1.2. Idéal engendré par un élément

Définition 2.4. Idéal engendré par un élément

Soit A un anneau commutatif et x un élément de A. L'ensemble des éléments de A de la forme xa, où a est un élément quelconque de A, est un idéal de A appelé idéal engendré par x. C'est le plus petit idéal de A contenant x. On le note xA.

$$xA = \big\{y \in A\ ,\ \exists a \in A\ ,\ y = xa\big\}.$$

Exemples

1. L'ensemble des entiers relatifs pairs est l'idéal de $\mathbb{Z}$ engendré par l'entier 2 :
$$2\mathbb{Z} = \{y \in \mathbb{Z}\ ,\ \exists a \in \mathbb{Z}\ ,\ y = 2a\}.$$
2. L'ensemble des polynômes à coefficients réels admettant 0 pour racine est l'idéal de $\mathbb{R}[X]$ engendré par le polynôme X :
$$X\mathbb{R}[X] = \{P \in \mathbb{R}[X]\ ,\ \exists Q \in \mathbb{R}[X]\ ,\ P = XQ\}.$$

Définition 2.5. Idéal principal, anneau principal

Soit A un anneau commutatif. Un idéal de A est dit principal s'il est engendré par un seul élément. L'anneau A est dit principal s'il est intègre et si tous ses idéaux sont principaux.

Exemples

1. Un idéal de l'anneau $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$, or nous avons vu dans le chapitre précédent (théorème 1.7) que tout sous-groupe de $\mathbb{Z}$ est monogène, c'est-à-dire de la forme $n\mathbb{Z}$; c'est donc un idéal principal. Comme l'anneau $\mathbb{Z}$ est intègre, c'est un anneau principal.
2. Soit $\mathbb{Z}[X]$ l'ensemble des polynômes à coefficients entiers et A l'ensemble des éléments de cet anneau de la forme $P = \sum_{k=0}^{n} a_n X^n$, où pour tout $k \in [\![1, n]\!]$ $a_k \in \mathbb{Z}$ et $a_0 \in 2\mathbb{Z}$ (le coefficient constant est pair). On montre facilement que A est un idéal de $\mathbb{Z}[X]$, mais cet idéal n'est pas principal car par exemple les éléments 2 et X ne sont pas multiples l'un de l'autre. L'anneau $\mathbb{Z}[X]$ n'est donc pas principal.

1.3. Divisibilité dans un anneau intègre

Définition 2.6. Divisibilité

Soit A un anneau intègre.

- On dit que a divise b s'il existe un élément c de A tel que $b = ac$. On écrit $a|b$.
- Si $a|b$, on dit que a est un diviseur de b ou que b est un multiple de a.
- Deux éléments a et b sont dits associés si a divise b et b divise a.
- Un élément est dit irréductible si ses seuls diviseurs sont les éléments inversibles et les éléments qui lui sont associés.

Remarque

La relation « divise » dans l'anneau A se ramène à une inclusion des idéaux engendrés :
$$a \mid b \iff bA \subset aA.$$

2 L'anneau $\mathbb{Z}$

2.1. Idéaux de $\mathbb{Z}$

Rappelons le résultat déjà démontré dans l'exemple 1 du paragraphe 1.2. :

Théorème 2.7. Idéaux de $\mathbb{Z}$

$\mathbb{Z}$ est un anneau principal. Tout idéal de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, avec $n \in \mathbb{Z}$.

Démonstration

L'anneau $\mathbb{Z}$ est intègre. Si I est un idéal de $\mathbb{Z}$, alors $(I,+)$ est un sous-groupe de $(\mathbb{Z},+)$, donc il existe $n \in \mathbb{Z}$ tel que $I = n\mathbb{Z}$. Tout idéal de $\mathbb{Z}$ est principal. L'anneau $\mathbb{Z}$ est principal. ■

Remarque

Dans l'anneau $\mathbb{Z}$, il n'y a pas de différence entre sous-groupe et idéal, mais cette situation est tout à fait exceptionnelle.

Définition 2.8. PGCD et PPCM de n entiers en termes d'idéaux

Soit $(x_1,\dots,x_n)$ une famille de n entiers relatifs, avec $n \geqslant 2$. On appelle :

- PGCD de cette famille l'unique générateur positif de l'idéal $\sum_{i=1}^{n} x_i\mathbb{Z}$:
$$(x_1 \wedge \cdots \wedge x_n)\mathbb{Z} = x_1\mathbb{Z} + \cdots + x_n\mathbb{Z};$$
- PPCM de cette famille l'unique générateur positif de l'idéal $\bigcap_{i=1}^{n} x_i\mathbb{Z}$:
$$(x_1 \vee \cdots \vee x_n)\mathbb{Z} = x_1\mathbb{Z} \cap \cdots \cap x_n\mathbb{Z}.$$

On retrouve bien les définitions étudiées en première année.

- Soit d le PGCD de $(x_1,\dots,x_n)$: $d\mathbb{Z} = x_1\mathbb{Z} + \cdots + x_n\mathbb{Z}$, donc pour tout $i \in [\![1,n]\!]$, $x_i\mathbb{Z} \subset d\mathbb{Z}$, c'est-à-dire : $d|x_i$: d est un diviseur commun à tous les x_i. Réciproquement, si δ est un diviseur commun à tous les x_i, alors pour tout i, $\delta|x_i$, c'est-à-dire $x_i\mathbb{Z} \subset \delta\mathbb{Z}$, d'où $d\mathbb{Z} \subset \delta\mathbb{Z}$, ou encore : $\delta|d$. Tout diviseur commun à tous les x_i divise d.
  En définitive, d est le plus grand (au sens de la divisibilité) des diviseurs communs à tous les x_i.
- Soit m le PPCM de $(x_1,\dots,x_n)$: $m\mathbb{Z} = x_1\mathbb{Z} \cap \cdots \cap x_n\mathbb{Z}$. Alors pour tout $i \in [\![1,n]\!]$, $m\mathbb{Z} \subset x_i\mathbb{Z}$, c'est-à-dire : $x_i|m$: m est un multiple commun à tous les x_i. Réciproquement, si μ est un multiple commun à tous les x_i, alors pour tout i, $x_i|\mu$, c'est-à-dire $\mu\mathbb{Z} \subset x_i\mathbb{Z}$, d'où $\mu\mathbb{Z} \subset m\mathbb{Z}$, ou encore : $m|\mu$. Tout multiple commun à tous les x_i est un multiple de m.
  En définitive, m est le plus petit (au sens de la divisibilité) des multiples communs à tous les x_i.

Algorithme 2.9. Exemple de calcul avec Python du PGCD de deux entiers

```
def pgcd(a,b):
    while b<>0:
        r=a%b
        a,b=b,r
    return a
```

2.2. Entiers premiers entre eux

Définition 2.10. Entiers premiers entre eux

Soit $(x_1, \dots, x_n)$ une famille de n entiers relatifs, avec $n \geqslant 2$. Ces entiers sont dits premiers entre eux si leur PGCD est 1, c'est-à-dire si : $x_1\mathbb{Z} + \cdots + x_n\mathbb{Z} = \mathbb{Z}$.

Théorème 2.11. Théorème de Bezout

Les entiers $(x_1, \dots, x_n)$ sont premiers entre eux si et seulement si il existe des entiers relatifs $(u_1, \dots, u_n)$ tels que : $x_1 u_1 + \cdots + x_n u_n = 1$.

Démonstration

Soit d le PGCD des x_i. Si ces entiers sont premiers entre eux, alors $d = 1$, donc $1 \in x_1\mathbb{Z} + \cdots + x_n\mathbb{Z}$, d'où la relation de Bezout.

Réciproquement, si cette relation est réalisée, alors $1 \in d\mathbb{Z}$, donc $d|1$. Comme un PGCD est par définition positif, il vient $d = 1$: les entiers x_i sont premiers entre eux. ■

3 Anneaux $\mathbb{Z}/n\mathbb{Z}$

3.1. Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$

Proposition 2.12. Multiplication dans $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$. Pour tout $(a, b) \in \mathbb{Z}^2$, la classe modulo n de ab ne dépend que des classes de a et de b, et non de représentants particuliers de ces classes. On peut ainsi définir une multiplication dans $\mathbb{Z}/n\mathbb{Z}$: $\forall(\overline{a}, \overline{b}) \in (\mathbb{Z}/n\mathbb{Z})^2, \quad \overline{a}\,\overline{b} = \overline{ab}$.

Alors, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

Démonstration

Nous savons déjà que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.

Soit $(a', b') \in \overline{a} \times \overline{b}$: $a' - a \in n\mathbb{Z}$ et $b' - b \in n\mathbb{Z}$. Nous avons :

$$a'b' - ab = (a' - a)b + a'(b' - b) \in n\mathbb{Z},$$

donc $a'b' \in \overline{ab}$.

On vérifie aisément que la multiplication ainsi définie dans $\mathbb{Z}/n\mathbb{Z}$ est associative, commutative, distributive par rapport à $+$ et qu'elle admet un élément neutre $\overline{1}$.

Finalement $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est bien un anneau commutatif. ■

Exemple : anneau $(\mathbb{Z}/6\mathbb{Z}, +, \times)$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Figure 2.1. Tables de l'anneau $(\mathbb{Z}/6\mathbb{Z}, +, \times)$.

On remarque que $\overline{2} \times \overline{3} = \overline{0}$: $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre. Ses éléments inversibles sont $\overline{1}$ et $\overline{5}$, qui sont chacun leur propre inverse.

3.2. Inversibles de $\mathbb{Z}/n\mathbb{Z}$

Théorème 2.13. Inversibles de $\mathbb{Z}/n\mathbb{Z}$

L'élément $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier avec n.

Démonstration

Si $\overline{k}$ est inversible, alors il existe un entier k' tel que $\overline{kk'} = \overline{1}$, c'est-à-dire $kk' \equiv 1\,[n]$. Ainsi il existe $q \in \mathbb{Z}$ tel que $kk' - qn = 1$. D'après le théorème de Bezout : $k \wedge n = 1$.
Réciproquement, si $k \wedge n = 1$, alors il existe des entiers p et q tels que $kp + nq = 1$, soit $kp \equiv 1\,[n]$, d'où $\overline{k}\overline{p} = \overline{1}$: ainsi, $\overline{k}$ est inversible. ■

Remarque

Le calcul de l'inverse de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ se ramène à l'algorithme d'Euclide.

Exemple

Puisque $5 \wedge 18 = 1$, la classe $\overline{5}$ est inversible dans $\mathbb{Z}/18\mathbb{Z}$. Or $18 = 3\times5+3$; $5 = 1\times3+2$; $3 = 1\times2+1$, d'où : $1 = 3-2 = 3-(5-3) = -5+2\times3 = -5+2(18-3\times5) = 2\times18-7\times5$.
Ainsi, $(\overline{5})^{-1} = \overline{(-7)} = \overline{11}$ dans $\mathbb{Z}/18\mathbb{Z}$.

Théorème 2.14. Corps $\mathbb{Z}/p\mathbb{Z}$

L'anneau $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps si et seulement si p est un nombre premier.
On le note alors $\mathbb{F}_p$.

Démonstration

$(\mathbb{Z}/p\mathbb{Z},+,\times)$ est un corps si et seulement si il possède $p-1$ éléments inversibles, c'est-à-dire si et seulement si p est premier avec tous les entiers de 1 à $p-1$: c'est une caractérisation d'un nombre premier. ■

3.3. Produit fini d'anneaux

Nous avons besoin pour le paragraphe suivant d'étendre aux anneaux la notion de structure produit déjà étudiée dans le premier chapitre pour les groupes.

Définition 2.15. Anneau produit

Soit $(A_i)_{i\in[\![1,n]\!]}$ une famille finie d'anneaux. On peut munir le produit cartésien $A=\prod_{i=1}^{n} A_i$ des opérations internes :

- $+$: si $x=(x_i)_{i\in[\![1,n]\!]}$ et $y=(y_i)_{i\in[\![1,n]\!]}$, alors $x+y=(x_i+y_i)_{i\in[\![1,n]\!]}$;
- $\times$: si $x=(x_i)_{i\in[\![1,n]\!]}$ et $y=(y_i)_{i\in[\![1,n]\!]}$, alors $x\,y=(x_i\,y_i)_{i\in[\![1,n]\!]}$.

On vérifie aisément que A muni de ces deux lois est un anneau.

3.4. Théorème chinois

Théorème 2.16. Théorème chinois

Soit $(n,m)\in\mathbb{N}^{*2}$. Si $n\wedge m=1$, alors les anneaux $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$ sont isomorphes.

Remarque

Ce théorème est ainsi nommé en hommage au mathématicien chinois Qin Jiushao (1202-1261), qui démontra un énoncé équivalent en termes de restes de divisions euclidiennes.

Démonstration

L'application f de $\mathbb{Z}/nm\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ qui, à une classe $\overline{k}$ modulo nm associe le couple des classes de k modulo n et m, est un morphisme d'anneaux. Son noyau est l'ensemble des $\overline{k}$ modulo nm tels que $k\equiv 0[n]$ et $k\equiv 0[m]$, c'est-à-dire k divisible par n et m ; comme n et m sont premiers entre eux, cela équivaut à k divisible par nm, c'est-à-dire $k\equiv 0\,[nm]$, ou encore $\overline{k}=\overline{0}$ dans $\mathbb{Z}/nm\mathbb{Z}$. Donc $\operatorname{Ker} f=\{\overline{0}\}$, le morphisme f est injectif. Comme les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ ont le même cardinal nm, f est bijectif. C'est un isomorphisme. ■

Application : systèmes de congruence

Le théorème chinois signifie que, si n et m sont deux entiers premiers entre eux, un système de congruences de modulo respectifs n et m équivaut à une seule congruence modulo nm.

$$\forall(a,b)\in\mathbb{Z}^2,\ \exists c\in\mathbb{Z}\ /\quad \begin{cases} x\equiv a\,[n] \\ x\equiv b\,[m]\end{cases} \iff x\equiv c\,[nm].$$

Exemple Tiré du traité *Shùshū Jiǔzhāng, neuf chapitres de l'art mathématique*, de Qin Jiushao, publié en 1247

Le général Han Xin a entre 900 et 1 000 soldats. Si on les range par 3, il en reste 2. Si on les range par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien sont-ils ?
Le nombre x de soldats vérifie le système de congruences :

$$\begin{cases} x \equiv 2\,[3] \\ x \equiv 3\,[5] \\ x \equiv 2\,[7] \end{cases} \qquad \text{avec } x \in [\![900, 1\,000]\!].$$

Comme 3, 5 et 7 sont premiers entre eux deux à deux, ce système équivaut à une seule congruence modulo $3\times5\times7=105$. Il existe $(p,q,r)\in\mathbb{Z}^3$ tel que $x=3p+2=5q+3=7r+2$. Il vient $3p-5q=1$, dont une solution particulière est $(p,q)=(2,1)$ et l'ensemble des solutions $(p,q)=(5s+2,3s+1)$, avec $s\in\mathbb{Z}$. On a donc $x=15s+8=7r+2$. On en déduit $7r-15s=6$. Or $15-2\times7=1$, donc $6\times15-12\times7=6$. Une solution particulière est $(r,s)=(-12,-6)$ et l'ensemble des solutions $(r,s)=(15t-12,7t-6)$, avec $t\in\mathbb{Z}$. En définitive, $x=105t-82$. Le système équivaut à l'unique congruence $x\equiv-82\ [105]$. La seule solution comprise entre 900 et 1 000 est obtenue pour $t=10$. Le général a 968 soldats.

3.5. Indicatrice d'Euler

Définition 2.17. Indicatrice d'Euler

On appelle indicatrice d'Euler de l'entier $n\in\mathbb{N}^*$ le nombre $\varphi(n)$ d'entiers de $[\![1,n]\!]$ premiers avec n.

Remarque

Nous avons rencontré ce nombre à deux reprises :

- $\varphi(n)$ est le nombre d'éléments générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z},+)$;
- $\varphi(n)$ est le nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$.

Nous savons déjà que, si p est un nombre premier, alors $\varphi(p)=p-1$.

Algorithme 2.18. Calcul de l'indicatrice d'Euler

On peut écrire un algorithme qui calcule $\varphi(n)$, pour des petites valeurs de n, en parcourant tous les entiers de 1 à n et en incrémentant un compteur chaque fois que l'on en rencontre un qui est premier avec n. Bien entendu, cet algorithme devient vite inefficace pour de grandes valeurs de n.

Calcul en Python de l'indicatrice d'Euler d'un entier (voir au paragraphe 2.9 la fonction PGCD) :

```python
def phi(n):
    compteur = 0
    for d in range(1,n+1):
        if pgcd(d,n) == 1:
            compteur += 1
    return compteur
```

Proposition 2.19. Indicatrice d'Euler d'un produit d'entiers premiers entre eux

Si n et m sont deux entiers premiers entre eux, alors $\varphi(nm) = \varphi(n)\varphi(m)$.

Démonstration

D'après le théorème chinois, si $n \wedge m = 1$, alors les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes. Leurs éléments inversibles se correspondent dans cet isomorphisme. Or $(\overline{a}, \overline{b})$ est inversible dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ si et seulement si $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et $\overline{b}$ est inversible dans $\mathbb{Z}/m\mathbb{Z}$, ce qui donne $\varphi(n)\varphi(m)$ éléments inversibles dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ pour $\varphi(nm)$ dans $\mathbb{Z}/nm\mathbb{Z}$. On en déduit l'égalité. ■

Proposition 2.20. Indicatrice d'Euler d'une puissance d'un nombre premier

Soit p un nombre premier et k un entier naturel non nul, alors $\varphi(p^k) = p^k\left(1 - \frac{1}{p}\right)$.

Démonstration

Les entiers premiers avec p^k sont ceux qui sont premiers avec p, c'est-à-dire tous les entiers qui ne sont pas multiples de p. Dans l'intervalle $[\![1, p^k]\!]$, on compte p^{k-1} multiples de p, donc $p^k - p^{k-1}$ entiers qui ne le sont pas. On a donc $\varphi\left(p^k\right) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$. ■

Proposition 2.21. Indicatrice d'Euler et diviseurs premiers

Si les diviseurs premiers de l'entier n sont $(p_1, p_2, \ldots, p_k)$, alors :

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Démonstration

L'entier n admet une décomposition en produit de facteurs premiers de la forme :

$$n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_k}^{\alpha_k},$$

où $p_1, p_2, \ldots, p_k$ sont des nombres premiers distincts deux à deux et $\alpha_1, \alpha_2, \ldots, \alpha_k$ des entiers naturels non nuls. Les ${p_i}^{\alpha_i}$, pour $i \in [\![1, k]\!]$, sont premiers entre eux deux à deux. On en déduit que :

$$\begin{aligned}
\varphi(n) &= \varphi\left({p_1}^{\alpha_1}\right)\varphi\left({p_2}^{\alpha_2}\right)\cdots\varphi\left({p_k}^{\alpha_k}\right) \\
&= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right)p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right)\cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).
\end{aligned}$$

■

Exemple

Calculons l'indicatrice d'Euler de 3 600. Les diviseurs premiers de 3 600 sont 2, 3, 5, d'où :

$$\varphi(3\,600) = 3\,600\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 960.$$

Remarque

L'avantage de cette formule est qu'elle ne nécessite pas de connaître les exposants apparaissant dans la décomposition en produit de facteurs premiers de n, mais seulement les facteurs premiers eux-mêmes. Cependant, cette méthode devient elle-même trop complexe pour des nombres géants (une centaine de chiffres décimaux). Nous verrons ci-après que c'est sur cette complexité que repose la sécurité de certaines méthodes utilisées en cryptographie.

3.6. Théorème d'Euler

Théorème 2.22. Théorème d'Euler

Soit $n \in \mathbb{N}^*$. Pour tout entier a premier avec n :

$$a^{\varphi(n)} \equiv 1\,[n].$$

Démonstration

Si $a \wedge n = 1$, alors la classe de a modulo n appartient au groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Son ordre divise le cardinal du groupe, qui est $\varphi(n)$: $\overline{a}^{\varphi(n)} = \overline{1}$, c'est-à-dire $a^{\varphi(n)} \equiv 1\,[n]$. ■

Corollaire 2.23. Petit théorème de Fermat

Si p est un nombre premier, alors pour tout entier a : $a^p \equiv a\ [p]$.

Démonstration

Si $a \in p\mathbb{Z}$, alors $a \equiv 0\,[p]$ et $a^p \equiv 0\,[p]$, d'où le résultat.
Si $a \notin p\mathbb{Z}$, alors $a \wedge p = 1$. D'après le théorème d'Euler, $a^{\varphi(p)} \equiv 1\,[p]$ avec $\varphi(p) = p - 1$.
D'où $a^{p-1} \equiv 1\,[p]$ puis $a^p \equiv a\,[p]$. ■

Remarque

Ne pas confondre ce théorème avec le « grand théorème de Fermat-Wiles » affirmant que, si n est un entier supérieur ou égal à 3, il n'existe aucun triplet $(a, b, c) \in \mathbb{N}^{*3}$ tel que $a^n + b^n = c^n$. Sous son apparente simplicité, ce résultat, dont Pierre de Fermat prétendait disposer d'une démonstration « merveilleuse », ne fut démontré qu'en 1994 par Andrew Wiles à l'aide de méthodes extrêmement complexes.

Application : principe du cryptage RSA (voir exercice G)

Il s'agit d'une méthode de cryptage inventée par Ron Rivest, Adi Shamir et Léonard Adleman en 1978. Elle utilise des *clés asymétriques* : une clé publique, permettant librement de crypter des messages pour un destinataire, et une clé privée, que celui-ci est seul à détenir et qui lui permet de décrypter les messages qu'il reçoit.
La sécurité du système repose sur la difficulté de calculer l'indicatrice d'Euler d'un très grand entier. Le RSA est encore utilisé aujourd'hui pour échanger en toute sécurité des *clés symétriques* utilisées pour crypter et décrypter beaucoup plus rapidement.

4 Anneaux $\mathbb{K}[X]$

Dans ce paragraphe, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, le plus souvent $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. Cette mention nous garantit que l'application de $\mathbb{Z}$ dans $\mathbb{K}$ définie par $n \mapsto n \cdot 1_{\mathbb{K}}$ est injective. Ce ne serait pas le cas pour un corps tel que $\mathbb{Z}/p\mathbb{Z}$ avec p premier, dans lequel $p \cdot \overline{1} = \overline{0}$. Dans $\mathbb{Z}/2\mathbb{Z}$, par exemple, $\overline{1}+\overline{1} = \overline{0}$. De telles égalités compliquent la théorie des polynômes et restreignent la validité de certains résultats. Par exemple, dans $\mathbb{Z}/2\mathbb{Z}[X]$, le polynôme X^2+X est de degré 2 mais de fonction polynomiale nulle.
Rappelons qu'un polynôme est dit *unitaire* si son coefficient dominant est égal à 1.

4.1. Idéaux de $\mathbb{K}[X]$

Théorème 2.24. Idéaux de $\mathbb{K}[X]$

L'anneau $\mathbb{K}[X]$ est principal, c'est-à-dire qu'il est intègre et que tout idéal de $\mathbb{K}[X]$ est de la forme $P_0\,\mathbb{K}[X]$, où P_0 est un polynôme, que l'on peut choisir unitaire (il est alors unique).

Démonstration

On sait déjà que $\mathbb{K}[X]$ est intègre : $\forall (P,Q) \in \mathbb{K}[X]^2, \quad PQ = 0 \Rightarrow (P = 0 \text{ ou } Q = 0)$.
Soit I un idéal de $\mathbb{K}[X]$.
Si $I = \{0\}$, alors I est l'idéal engendré par le polynôme nul.
Si $I \neq \{0\}$, considérons l'ensemble D des degrés des polynômes non nuls de I. Comme D est une partie non vide de $\mathbb{N}$, elle possède un plus petit élément n_0. Soit P_0 un élément de I de degré p_0. L'idéal $P_0\,\mathbb{K}[X]$ engendré par P_0 est inclus dans I.
Réciproquement, soit P un élément quelconque de I. Par division euclidienne de P par P_0 :

$$P = P_0 Q + R \qquad \text{avec } \deg(R) < p_0.$$

Comme P et $P_0 Q$ appartiennent à I, R appartient aussi à I. Or son degré est strictement inférieur au plus petit degré des éléments non nuls de I, donc $R = 0$. Le polynôme P est donc un multiple de P_0, c'est-à-dire que I est inclus dans l'idéal engendré par P_0.
En définitive, I est l'idéal engendré par le polynôme P_0, ou par tout polynôme associé à P_0. Parmi ceux-ci, il en existe un et un seul qui soit unitaire. ■

On peut étendre sans difficulté à $\mathbb{K}[X]$ les notions de PGCD, PPCM, éléments premiers entre eux, ainsi que le théorème de Bezout.

4.2. PGCD de n polynômes

Définition 2.25. PGCD d'une famille finie de polynômes

Soit $(A_1, \ldots, A_n)$ une famille de n polynômes à coefficients dans $\mathbb{K}$. On appelle plus grand commun diviseur ou PGCD de cette famille l'unique générateur unitaire de l'idéal $\sum_{k=1}^{n} \left(A_k\,\mathbb{K}[X]\right)$.

4.3. Polynômes premiers entre eux

Définition 2.26. Polynômes premiers entre eux

Soit $(A_k)_{k\in[\![1,n]\!]} \in \mathbb{K}[X]^n$. Les polynômes A_k sont dits premiers entre eux si leur PGCD est 1 :

$$\sum_{k=1}^{n} (A_k\,\mathbb{K}[X]) = \mathbb{K}[X].$$

Théorème 2.27. Théorème de Bezout

Soit $(A_k)_{k\in[\![1,n]\!]} \in \mathbb{K}[X]^n$. Les polynômes A_k sont premiers entre eux si et seulement si il existe une famille $(U_1,\dots,U_n) \in \mathbb{K}[X]^n$ telle que :

$$\sum_{k=1}^{n} A_k U_k = 1.$$

Conseils méthodologiques

Comme pour les entiers, la recherche d'un couple $(U,V) \in \mathbb{K}[X]^2$ tel que $AU+BV=1$ peut utiliser l'algorithme d'Euclide.

Exemple Pour $A = X^3+1, B = X^2+1$, il vient par divisions euclidiennes successives :

$$\begin{cases} X^3+1 = (X^2+1)X-(X-1) \\ X^2+1 = (X-1)(X+1)+2 \end{cases}.$$

d'où :

$$\begin{aligned} 2 &= (X^2+1)-(X-1)(X+1) = (X^2+1)-\big((X^2+1)X-(X^3+1)\big)(X+1) \\ &= (X^3+1)(X+1)-(X^2+1)(X^2+X-1). \end{aligned}$$

Une solution particulière de l'équation $AU+BV=1$ est donc :

$$(U_0,V_0) = \left(\frac{1}{2}(X+1),\ \frac{1}{2}(-X^2-X+1)\right).$$

La solution générale est :

$$(U,V) = \Big(U_0+(X^2+1)Q,\ V_0-(X^3+1)Q\Big), \text{ avec } Q \in \mathbb{K}[X].$$

On retrouve également le théorème de Gauss :

Corollaire 2.28. Théorème de Gauss

Si un polynôme divise un produit de deux polynômes et qu'il est premier avec l'un des facteurs, alors il divise l'autre.

$$\forall (A,B,C) \in \mathbb{K}[X]^3, \quad \big(A|BC \text{ et } A\wedge B = 1\big) \implies A|C.$$

Démonstration
Puisque $A \wedge B = 1$, il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$, d'où $ACU + BCV = C$.
Puisque $A|BC$, il existe $D \in \mathbb{K}[X]$ tel que $BC = AD$. On en déduit que $A(CU + DV) = C$ et donc que A divise C. ■

4.4. Polynômes irréductibles de $\mathbb{K}[X]$

Définition 2.29. Polynôme irréductible sur un corps

Un polynôme de $\mathbb{K}[X]$ est dit irréductible s'il est non constant et si ses seuls diviseurs sont les polynômes qui lui sont associés et les polynômes constants.

Remarques
- Les polynômes irréductibles jouent le même rôle dans $\mathbb{K}[X]$ que les nombres premiers dans $\mathbb{Z}$.
- Le caractère irréductible d'un polynôme dépend du corps $\mathbb{K}$ considéré. Par exemple, $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, mais pas dans $\mathbb{C}[X]$.

Proposition 2.30. Existence d'un diviseur irréductible

Tout polynôme non constant de $\mathbb{K}[X]$ possède au moins un diviseur irréductible.

Démonstration
Soit P un polynôme non constant. L'ensemble des degrés des diviseurs non constants de P est une partie non vide de $\mathbb{N}^*$, qui possède donc un plus petit élément n_0. Soit D_0 un diviseur de P de degré n_0. Un diviseur de D_0 non constant et non associé à D_0 serait un diviseur de P de degré strictement inférieur à n_0, ce qui contredirait la définition de n_0. Donc D_0 est irréductible. ■

Théorème 2.31. Décomposition en produit de facteurs irréductibles

Tout polynôme non constant de $\mathbb{K}[X]$ est un produit de facteurs irréductibles. Cette décomposition est unique, sauf à changer un facteur en un facteur associé ou à modifier l'ordre des facteurs.

Démonstration
La démonstration est exactement la même que celle de la décomposition d'un entier en produit de facteurs premiers. ■

4.5. Irréductibles de $\mathbb{C}[X]$

Conformément au programme, nous admettrons sans démonstration le théorème suivant, parfois appelé *théorème fondamental de l'algèbre*.

Théorème 2.32. Théorème de d'Alembert-Gauss

Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine dans $\mathbb{C}$.

Corollaire 2.33. Polynômes irréductibles de $\mathbb{C}[X]$

- Les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
- Tout polynôme de degré $n \geqslant 0$ de $\mathbb{C}[X]$ possède exactement n racines, comptées avec leur ordre de multiplicité.
- Tout polynôme non constant de $\mathbb{C}[X]$ est scindé, c'est-à-dire produit de polynômes de degré 1.

$$P = \lambda(X-a_1)^{m_1}(X-a_2)^{m_2}\cdots(X-a_k)^{m_k}.$$

4.6. Irréductibles de $\mathbb{R}[X]$

Soit $P \in \mathbb{R}[X]$, de degré $n \geqslant 0$. P possède n racines complexes, comptées avec leur ordre de multiplicité. Si z est une racine d'ordre m :

$$P(z) = P'(z) = \cdots = P^{(m-1)}(z) = 0 \quad \text{et} \quad P^{(m)}(z) \neq 0.$$

En conjuguant, on obtient :

$$P(\overline{z}) = P'(\overline{z}) = \cdots = P^{(m-1)}(\overline{z}) = 0 \quad \text{et} \quad P^{(m)}(\overline{z}) \neq 0.$$

$\overline{z}$ est donc aussi racine de P avec le même ordre de multiplicité que z. Les racines de P sont donc soit réelles, soit non réelles conjuguées deux à deux, avec le même ordre de multiplicité. Dans la décomposition en produit de facteurs irréductibles de P dans $\mathbb{C}[X]$, on peut regrouper les facteurs correspondant à deux racines non réelles conjuguées :

$$(X-z)^m(X-\overline{z})^m = (X^2+bX+c)^m,$$

avec $b = -2\mathfrak{Re}(z) \in \mathbb{R}$ et $c = |z|^2 \in \mathbb{R}$. Le trinôme X^2+bX+c n'a pas de racine réelle : son discriminant est strictement négatif, $b^2-4c<0$. Le polynôme P peut se décomposer dans $\mathbb{R}[X]$ sous la forme :

$$P = \lambda(X-a_1)^{m_1}(X-a_2)^{m_2}\cdots(X-a_k)^{m_k}(X^2+b_1X+c_1)^{\mu_1}\cdots(X^2+b_\ell X+c_\ell)^{\mu_\ell}.$$

On en déduit le résultat suivant :

Proposition 2.34. Polynômes irréductibles de $\mathbb{R}[X]$

Les seuls polynômes irréductibles de $\mathbb{R}[X]$ sont :

- les polynômes de degré 1 ;
- les polynômes de degré 2 de discriminant strictement négatif.

Remarque

Un polynôme de $\mathbb{R}[X]$ de degré strictement supérieur à 2 n'est certainement pas irréductible, même s'il n'a pas de racine réelle. Par exemple :

$$X^4+1 = (X^2+1)^2-2X^2 = (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1).$$

Les racines complexes d'un polynôme sans racine réelle sont conjuguées deux à deux, si bien que son degré est nécessairement pair. Autrement dit, un polynôme de $\mathbb{R}[X]$ de degré impair a toujours au moins une racine réelle.

L'étude des polynômes irréductibles de $\mathbb{Q}[X]$ est hors programme, mais il faut savoir qu'il en existe de n'importe quel degré.

5 Algèbres

Dans ce paragraphe comme dans le précédent, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, le plus souvent $\mathbb{R}$ ou $\mathbb{C}$.

5.1. Structure d'algèbre

Définition 2.35. Algèbre sur un corps

On appelle algèbre sur le corps $\mathbb{K}$ ou $\mathbb{K}$-algèbre un ensemble $\mathscr{A}$ muni de deux lois internes notées $+$ et $\times$ et d'une loi externe de multiplication par les éléments de $\mathbb{K}$, notée $\cdot$, telles que :

- $(\mathscr{A},+,\cdot)$ est un $\mathbb{K}$-espace vectoriel ;
- $(\mathscr{A},+,\times)$ est un anneau ; son élément unité est noté $1_{\mathscr{A}}$;
- $\forall (x,y)\in A^2,\ \forall(\alpha,\beta)\in\mathbb{K}^2,\ (\alpha\cdot x)\times(\beta\cdot y)=(\alpha\beta)\cdot(x\times y)$.

Si, de plus, $\times$ est commutative, on dit que l'algèbre est commutative.

Exemples

- Le $\mathbb{R}$-espace vectoriel $\mathbb{C}$ est une $\mathbb{R}$-algèbre.
- Si E est un $\mathbb{K}$-espace vectoriel, l'ensemble de ses endomorphismes $\mathscr{L}(E)$ est une $\mathbb{K}$-algèbre pour la composition des applications. Son élément unité est Id_E.
- L'ensemble des matrices carrées $\mathscr{M}_n(\mathbb{K})$ est une $\mathbb{K}$-algèbre, d'élément unité I_n.
- L'ensemble des polynômes $\mathbb{K}[X]$ est une $\mathbb{K}$-algèbre, dont l'élément unité est le polynôme constant 1.
- L'ensemble des applications d'un ensemble X quelconque dans $\mathbb{K}$, $\mathscr{F}(X,\mathbb{K})$ est une $\mathbb{K}$-algèbre, dont l'élément unité est la fonction constante égale à 1.

5.2. Sous-algèbre

Définition 2.36. Sous-algèbre

Soit $\mathscr{A}$ une $\mathbb{K}$-algèbre. On appelle sous-algèbre de $\mathscr{A}$ une partie $\mathscr{B}$ de $\mathscr{A}$ qui est à la fois un sous-espace vectoriel et un sous-anneau de $\mathscr{A}$.

Proposition 2.37. Caractérisation d'une sous-algèbre

Soit $\mathscr{A}$ une $\mathbb{K}$-algèbre. Une partie $\mathscr{B}$ de $\mathscr{A}$ est une sous-algèbre de $\mathscr{A}$ si et seulement si :

- $1_{\mathscr{A}}\in\mathscr{B}$;
- $\forall(\alpha,\beta)\in\mathbb{K}^2,\ \forall(x,y)\in\mathscr{B}^2,\ \alpha x+\beta y\in\mathscr{B}$;
- $\forall(x,y)\in\mathscr{B}^2,\ x\times y\in\mathscr{B}$.

Démonstration

Il suffit de cumuler les caractérisations d'un sous-espace vectoriel et d'un sous-anneau. On remarque que la condition $\mathscr{B}\neq\varnothing$ est satisfaite par la première hypothèse et que la condition $\forall(x,y)\in\mathscr{B}^2,\ x-y\in\mathscr{B}$ est un cas particulier de la seconde, avec $\alpha=1$ et $\beta=-1$. ■

Exemples

- $\mathbb{R}$ est une sous-algèbre de la $\mathbb{R}$-algèbre $\mathbb{C}$.
- Si E est un $\mathbb{K}$-espace vectoriel, l'ensemble des homothéties $k\mathrm{Id}_E$ est une sous-algèbre de $\mathscr{L}(E)$.
- L'ensemble des matrices diagonales de taille n est une sous-algèbre de $\mathscr{M}_n(\mathbb{K})$.
- L'ensemble des polynômes pairs est une sous-algèbre de $\mathbb{K}[X]$.
- L'ensemble des applications continues d'un intervalle I de $\mathbb{R}$ dans $\mathbb{K}$ est une sous-algèbre de $\mathbb{K}^I$.

5.3. Morphismes d'algèbres

Définition 2.38. Morphisme d'algèbres

Soit $\mathscr{A}$ et $\mathscr{A}'$ deux $\mathbb{K}$-algèbres. On appelle morphisme de $\mathscr{A}$ dans $\mathscr{A}'$ une application f de $\mathscr{A}$ dans $\mathscr{A}'$ qui est à la fois un morphisme d'espaces vectoriels (c'est-à-dire linéaire) et un morphisme d'anneaux, c'est-à-dire telle que :

- $f(1_{\mathscr{A}}) = 1_{\mathscr{A}'}$;
- $\forall(\alpha,\beta)\in\mathbb{K}^2,\ \forall(x,y)\in\mathscr{A}^2,\ f(\alpha x+\beta y)=\alpha f(x)+\beta f(y)$;
- $\forall(x,y)\in\mathscr{A}^2,\ f(x\times y)=f(x)\times f(y)$.

Exemples

- L'application $(u_n)_{n\in\mathbb{N}} \mapsto \lim\limits_{n\in\mathbb{N}} u_n$ est un morphisme de la $\mathbb{R}$-algèbre des suites réelles convergentes dans l'algèbre $\mathbb{R}$.
- L'application $f \mapsto f(0)$ est un morphisme de la $\mathbb{R}$-algèbre des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, dans l'algèbre $\mathbb{R}$.

5.4. Substitution de l'indéterminée d'un polynôme par un élément d'une algèbre

Soit $P = \sum\limits_{k=0}^{n} a_k X^k$ un polynôme à coefficients dans $\mathbb{K}$. Rappelons que X n'est rien d'autre qu'un polynôme particulier, appelé *indéterminée* de $\mathbb{K}[X]$. On peut lui substituer un élément x d'un ensemble E, à condition de disposer d'une :

- multiplication interne dans E, pour définir x^k pour tout $k\in\mathbb{N}$;
- multiplication externe par les éléments de $\mathbb{K}$, pour définir $a_k x^k$;
- addition interne dans E, pour ajouter les termes précédents.

Ces conditions sont réalisées si E est une K-algèbre.

Définition 2.39. Substitution de l'indéterminée d'un polynôme

Soit $\mathscr{A}$ une $\mathbb{K}$-algèbre. On appelle substitution l'application $(P,x)\mapsto P(x)$ de $\mathbb{K}[X]\times\mathscr{A}$ dans $\mathscr{A}$ définie de la façon suivante : si $P = \sum\limits_{k=0}^{n} a_k X^k$ et $x\in\mathscr{A}$, alors $P(x) = \sum\limits_{k=0}^{n} a_k x^k$ avec la convention $x^0 = 1_{\mathscr{A}}$.

Exemple

Si $P = X^2 - X + 2 \in \mathbb{R}[X]$:

- pour $i \in \mathbb{C}$, $P(i) = 1 - i \in \mathbb{C}$;
- pour $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathscr{M}_2(\mathbb{R})$, $P(A) = A^2 - A + 2\mathrm{I}_2 = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \in \mathscr{M}_2(\mathbb{R})$;
- pour $X^2 \in \mathbb{R}[X]$, $P(X^2) = X^4 - X^2 + 2 \in \mathbb{R}[X]$.

Proposition 2.40. Polynômes annulateurs ; polynôme minimal

Soit $\mathscr{A}$ une $\mathbb{K}$-algèbre et $x \in \mathscr{A}$. L'application $P \mapsto P(x)$ est un morphisme d'algèbres de $\mathbb{K}[X]$ dans $\mathscr{A}$. Le noyau de ce morphisme est un idéal de $\mathbb{K}[X]$, appelé idéal des polynômes annulateurs de x. Comme $\mathbb{K}[X]$ est principal, cet idéal est engendré par un seul élément. Si cet élément est non nul, il est unique si on le choisit unitaire, donc appelé polynôme minimal de x.

Conseils méthodologiques

P est le polynôme minimal de l'élément x de $\mathscr{A}$ si et seulement si $P(x) = 0$ et si, pour tout diviseur Q de P non associé à P, $Q(x) \neq 0$.

Exemples

- L'élément i de la $\mathbb{R}$-algèbre $\mathbb{C}$ a pour polynôme minimal $X^2 + 1$.
- L'élément $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ de la $\mathbb{R}$-algèbre $\mathscr{M}_2(\mathbb{R})$ a pour polynôme minimal $(X-1)^2$.
- Soit E un espace vectoriel. Un projecteur p de $\mathscr{L}(E)$, non nul et distinct de Id_E, admet pour polynôme minimal $X^2 - X$.

FICHE SYNTHÈSE

Idéal d'un anneau commutatif

Soit A un anneau commutatif.

- Un idéal de A est un sous-groupe de $(A,+)$ stable par multiplication par un élément quelconque de A.
- L'intersection et la somme de deux idéaux de A sont des idéaux de A.
- L'idéal engendré par un élément x de A est l'ensemble noté xA des éléments de A de la forme xa, où $a \in A$. C'est le plus petit idéal de A contenant x.
- Un idéal de A est dit principal s'il est engendré par un seul élément. L'anneau A est dit principal s'il est intègre et si tous ses idéaux sont principaux.

Arithmétique dans $\mathbb{Z}$

- L'anneau $\mathbb{Z}$ est principal ; tout sous-groupe de $\mathbb{Z}$ est principal.
- Le PGCD (resp. PPCM) d'une famille finie d'entiers est le générateurs de la somme (resp. l'intersection) des idéaux engendrés par les éléments de cette famille.
- Les entiers d'une famille finie sont premiers entre eux si leur PGCD est 1.
- Théorème de Bezout : les entiers $(x_1,\dots,x_n)$ sont premiers entre eux si et seulement si il existe des entiers relatifs $(u_1,\dots,u_n)$ tels que : $x_1u_1+\cdots+x_nu_n=1$.

Anneau $\mathbb{Z}/n\mathbb{Z}$

- $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un anneau commutatif.
- L'élément $\overline{k}$ de cet anneau est inversible si et seulement si $k \wedge n = 1$.
- L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si l'entier p est premier.
- Théorème chinois : si n et m sont deux entiers premiers entre eux, les anneaux $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$ sont isomorphes.
- L'indicatrice d'Euler d'un entier $n \in \mathbb{N}^*$ est le nombre $\varphi(n)$ d'entiers de $[\![1,n]\!]$ premiers avec n. C'est donc le nombre d'éléments générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z},+)$ ou d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$.
- Si n et m sont deux entiers premiers entre eux, $\varphi(nm)=\varphi(n)\varphi(m)$.
- Si les diviseurs premiers de n sont $(p_1,\dots,p_k)$, alors $\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$.
- Théorème d'Euler : soit $n \in \mathbb{N}^*$. Pour tout entier a premier avec n, $a^{\varphi(n)} \equiv 1\,[n]$.
- Théorème de Fermat : si p est un nombre premier, alors pour tout entier a : $a^p \equiv a\,[p]$.

Anneau $\mathbb{K}[X]$

- L'anneau $\mathbb{K}[X]$ est principal.
- Les notions d'arithmétique (PGCD, PPCM, éléments premiers entre eux, théorème de Bezout) s'étendent de $\mathbb{Z}$ à $\mathbb{K}[X]$.
- Un polynôme de $\mathbb{K}[X]$ est dit irréductible s'il est non constant et si ses seuls diviseurs sont les polynômes qui lui sont associés et les polynômes constants. • Théorème de d'Alembert Gauss : tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine dans $\mathbb{C}$. • Les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1. Tout polynôme non constant de $\mathbb{C}[X]$ est scindé.
- Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.

Structure d'algèbre

- Une $\mathbb{K}$-algèbre A est à la fois un $\mathbb{K}$-espace vectoriel et un anneau avec la relation :

$$\forall (x,y)\in A^2,\ \forall(\alpha,\beta)\in\mathbb{K}^2,\ (\alpha\cdot x)\times(\beta\cdot y)=(\alpha\beta)\cdot(x\times y).$$

- Une sous-algèbre de A est à la fois un sous-espace vectoriel et un sous-anneau.
- Un morphisme d'algèbres est à la fois un morphisme d'espaces vectoriels (=linéaire) et un morphisme d'anneaux.
- Si A est une algèbre et $x\in A$, un polynôme P est annulateur de x si $P(x)=0$. L'ensemble des polynômes annulateurs de x est un idéal de $\mathbb{K}[X]$. Si cet idéal est engendré par un polynôme non nul, ce polynôme (unique si unitaire) est appelé polynôme minimal de x.

RETROUVEZ ICI LA SYNTHÈSE DE CE CHAPITRE À TÉLÉCHARGER

www.lienmini.fr/212891-SYNTH-02

MÉTHODES PAS À PAS

Méthode 1 : Idéal d'un anneau commutatif

► Pour montrer qu'une partie d'un anneau commutatif est un idéal, vous pouvez démontrer que :
- c'est un sous-groupe pour l'addition et il est stable par la multiplication par un élément quelconque de l'anneau ;
- c'est l'image réciproque d'un idéal par un morphisme d'anneaux (en particulier, le noyau de ce morphisme) ;
- c'est l'image directe d'un idéal par un morphisme *surjectif* d'anneaux.

► Pour montrer qu'un anneau A est principal, vous pouvez :
- démontrer que A est intègre et que tout idéal de A est l'ensemble des multiples d'un élément donné ;
- trouver un isomorphisme entre A et $\mathbb{Z}$ ou $\mathbb{K}[X]$.

Application de la méthode : voir les exercices 1, 2, 3.

Méthode 2 : Calcul dans $\mathbb{Z}/n\mathbb{Z}$

► Pour montrer que la classe d'un entier k modulo n est inversible dans $\mathbb{Z}/n\mathbb{Z}$, démontrez que k est premier avec n.

► Pour trouver l'inverse de $\overline{k}$, utilisez l'algorithme d'Euclide pour calculer les coefficients de l'égalité de Bezout entre k et n.

► Pour calculer l'indicatrice d'Euler d'un entier n, comptez les entiers de 1 à n qui sont premiers avec n, ou utilisez la formule :

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right),$$

où $(p_1, p_2, \ldots, p_k)$ sont les diviseurs premiers de l'entier n.

► Dans des questions de congruences, pensez aux théorèmes suivants :
- théorème chinois : si $n \wedge m = 1$, alors un système de congruences modulos n et m est équivalent à une seule congruence modulo nm ;
- théorème d'Euler : si $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1\,[n]$;
- petit théorème de Fermat : si p est premier, alors $a^p \equiv a\ [p]$ pour tout $a \in \mathbb{Z}$.

Application de la méthode : voir les exercices 4, 5, A, B, E.

Méthode 3 : Calcul dans l'anneau $\mathbb{K}[X]$

($\mathbb{K}$ est un sous-corps de $\mathbb{C}$.)

► Pour calculer le PGCD de deux polynômes, utilisez l'algorithme d'Euclide.

► Pour montrer qu'un polynôme P de $\mathbb{K}[X]$ est irréductible :
- si $\mathbb{K}=\mathbb{C}$, montrez que P est de degré 1 ;
- si $\mathbb{K}=\mathbb{R}$, montrez que P est de degré 1, ou de degré 2 avec un discriminant strictement négatif;
- les autres cas sont difficiles et hors programme (par exemple, $\mathbb{K}=\mathbb{Q}$).

► Pour décomposer un polynôme P de $\mathbb{K}[X]$ en produit de facteurs irréductibles, avec $\mathbb{K}$ égal à $\mathbb{R}$ ou $\mathbb{C}$, cherchez les racines complexes de P (il n'y a pas de méthode systématique).

Application de la méthode : voir les exercices 7, F.

Méthode 4 : Structure d'algèbre

► Pour montrer qu'une partie d'une algèbre $\mathscr{A}$ est une sous-algèbre de $\mathscr{A}$, montrez que c'est un sous-espace vectoriel et un sous-anneau de $\mathscr{A}$.

► Pour montrer que P est le polynôme minimal d'un élément a d'une algèbre, montrez que $P(a)=0$ et que, pour tout diviseur Q de P non associé à P, $Q(a)\neq 0$.

Application de la méthode : voir les exercices 6, F.

EXERCICES

Vrai ou Faux

		Vrai	Faux
a)	L'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ s'annulant en 0 est un idéal de l'anneau de toutes les fonctions de $\mathbb{R}$ dans $\mathbb{R}$.	☐	☐
b)	L'ensemble des fonctions dérivables de $\mathbb{R}$ dans $\mathbb{R}$ dont la dérivée s'annule en 0 est un idéal de l'anneau de toutes les fonctions dérivables de $\mathbb{R}$ dans $\mathbb{R}$.	☐	☐
c)	Soit A un anneau commutatif. A est le seul sous-anneau de A qui est aussi un idéal de A.	☐	☐
d)	L'anneau $\mathbb{Z}^2$ est intègre.	☐	☐
e)	Les anneaux $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ et $\mathbb{Z}/80\mathbb{Z}$ sont isomorphes.	☐	☐
f)	$\overline{6}$ est inversible dans l'anneau $\mathbb{Z}/25\mathbb{Z}$.	☐	☐
g)	Pour tout $(p,q) \in \mathbb{N}^2$, $\varphi(pq) = \varphi(p)\varphi(q)$.	☐	☐
h)	Deux polynômes qui n'ont pas de racine commune sont premiers entre eux.	☐	☐
i)	Le polynôme $X^6 + 1$ est irréductible dans $\mathbb{R}[X]$.	☐	☐
j)	$\mathbb{R}$ est une sous-algèbre de la $\mathbb{C}$-algèbre $\mathbb{C}$.	☐	☐

Exercices d'application du chapitre 2

Si vous êtes bloqué pour démarrer un exercice d'application, rendez-vous à la fin de la partie Exercices, rubrique « Aides à la résolution des exercices ».

●○○ **EXERCICE 1**

Soit A un anneau commutatif et M une partie de A. On appelle *annulateur* de M l'ensemble des éléments a de A tels que $am = 0_A$ pour tout m de M. Montrer que l'annulateur de M est un idéal de A.

●○○ **EXERCICE 2**

Soit A un anneau commutatif et I un idéal de A. On dit que l'idéal I est *premier* si pour tout $(a,b) \in A^2$, $ab \in I \Rightarrow (a \in I)$ ou $(b \in I)$.

1) Trouver les idéaux premiers de $\mathbb{Z}$.
2) On construit l'*anneau-quotient* A/I comme on a construit dans le cours l'anneau $\mathbb{Z}/n\mathbb{Z}$. Montrer que l'idéal I est premier si et seulement si l'anneau A/I est intègre.
3) Montrer que, si f est un morphisme d'anneaux de A dans A', l'image réciproque d'un idéal premier de A' est un idéal premier de A.

●○○ **EXERCICE 3**

Soit A un anneau commutatif. Un élément x de A est dit *nilpotent* s'il existe un entier naturel non nul n tel que $x^n = 0_A$.

1) Montrer que l'ensemble des éléments nilpotents de A est un idéal de A.
2) Soit $x \in A$. Montrer que, si x est nilpotent, alors $1_A - x$ est inversible. Préciser son inverse.

●○○ **EXERCICE 4**

1) Soit n dont l'écriture en base 10 est donnée par $n = \sum_{i=0}^{k} b_i 10^i$.
   Donner une expression de $n \mod 11$ et en déduire que n est congru modulo 11 à la somme alternée de ses chiffres (par exemple, $1234 \equiv 4-3+2-1 \equiv 2\,[11]$).
2) Vérifier que 101 est un nombre premier et trouver un procédé similaire pour déterminer la classe d'un entier modulo 101. Calculer $1234 \mod 101$, puis $2^{22} \mod 101$.

●●○ **EXERCICE 5**

On considère le groupe $(G, \times)$ des éléments inversibles de l'anneau $\mathbb{Z}/32\mathbb{Z}$.

1) Quel est le cardinal de G ?
2) Quels sont les ordres des éléments $\overline{5}$ et $\overline{15}$?
3) Trouver un groupe additif isomorphe à G.

●○○ **EXERCICE 6**

Pour tout $(a, b) \in \mathbb{R}^2$, on définit la matrice $M(a, b) = \begin{pmatrix} a & b & b \\ b & a & b \\ b & b & a \end{pmatrix}$.

1) Montrer que l'ensemble E des matrices $M(a, b)$ est une sous-algèbre de l'algèbre $\mathscr{M}_3(\mathbb{R})$.
2) Trouver les éléments inversibles de l'algèbre E.

●●○ **EXERCICE 7**

Trouver l'ensemble des polynômes $P \in \mathbb{C}[X]$ tels que $P(X^2) = P(X-1)P(X+1)$.

Exercices d'approfondissement du chapitre 2

Si vous êtes bloqué pour démarrer un exercice d'approfondissement, rendez-vous à la fin de la partie Exercices, rubrique « Aides à la résolution des exercices ».

●●○ **EXERCICE A**

Soit n un entier supérieur ou égal à 3 et $(G, \times)$ le groupe des éléments inversibles de l'anneau $\mathbb{Z}/2^n\mathbb{Z}$.

1) Quel est le cardinal de G ?
2) Démontrer que : $5^{2^{n-3}} \equiv 2^{n-1} + 1 \quad [2^n]$.
3) En déduire l'ordre de l'élément $\overline{5}$ dans le groupe G.

●●○ **EXERCICE B** **Théorème de Wilson**

1) Montrer qu'un entier p est premier si et seulement si $(p-1)! \equiv -1\,[p]$.
2) Soit p un nombre premier de la forme $4n+1$. Montrer que, dans $\mathbb{Z}/p\mathbb{Z}$: $\overline{-1} = \overline{(2n)!}^2$.

●●○ **EXERCICE C**

1) Soit k un entier. Montrer que l'application $f_k : \overline{x} \mapsto \overline{k}\,\overline{x}$ est un morphisme du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ dans lui-même. À quelle condition ce morphisme est-il bijectif ?

2) On désigne par $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ le groupe des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ et par $(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ)$ le groupe des automorphismes du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
On considère l'application $\varphi : \overline{k} \mapsto f_k$ de $(\mathbb{Z}/n\mathbb{Z})^*$ dans $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. Montrer que φ est un morphisme du groupe $\big((\mathbb{Z}/n\mathbb{Z})^*, \times\big)$ dans le groupe $\big(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ\big)$. Déterminer son noyau et son image. Que peut-on en déduire ?

●●○

EXERCICE D

On appelle entier triangulaire un entier naturel qui peut s'écrire sous la forme de la somme des n premiers entiers strictement positifs :

$$N = 1+2+\cdots+n = \frac{n(n+1)}{2}.$$

Le but de l'exercice est de trouver l'ensemble des entiers qui sont à la fois triangulaires et carrés, c'est-à-dire pour lesquels il existe deux entiers strictement positifs n et p tels que :

$$N = \frac{n(n+1)}{2} = p^2. \qquad (1)$$

1) Soit $(n,p) \in \mathbb{N}^{*2}$ vérifiant l'équation (1). On pose : $r = 2n+1$; $s = 2p$. Montrer que :

$$r^2 - 2s^2 = 1. \qquad (2)$$

Cette équation est appelée équation de Pell-Fermat.

2) On considère l'ensemble $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ (a,b) \in \mathbb{Z}^2\}$.
   a) Montrer que $\mathbb{Z}[\sqrt{2}]$ est un anneau commutatif.
   b) On désigne par G le groupe des éléments inversibles de cet anneau. Soit $(a,b) \in \mathbb{Z}^2$. Montrer que $a + b\sqrt{2} \in G$ si et seulement si $a^2 - 2b^2 = \pm 1$.
   c) Soit $(a,b) \in \mathbb{N}^{*2}$ tel que $a + b\sqrt{2} \in G$.
      i. Montrer que $b \leqslant a < 2b$.
      ii. On pose $\dfrac{a+b\sqrt{2}}{1+\sqrt{2}} = a_1 + b_1\sqrt{2}$, avec $(a_1, b_1) \in \mathbb{Z}^2$. Montrer que $a_1 + b_1\sqrt{2} \in G$ et que $0 < a_1 \leqslant a$; $0 \leqslant b_1 < b$.
      iii. Montrer qu'il existe $q \in \mathbb{N}^*$ tel que $a + b\sqrt{2} = (1+\sqrt{2})^q$. Discuter la valeur de $a^2 - 2b^2$ en fonction de q.

3) En déduire l'ensemble des couples $(r,s) \in \mathbb{N}^{*2}$ vérifiant l'équation (2), puis l'ensemble des entiers triangulaires carrés.

●●●

EXERCICE E

Soit p un nombre premier supérieur ou égal à 3 et n un entier naturel supérieur ou égal à 2.
On veut montrer que le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$ des éléments inversibles de l'anneau $\mathbb{Z}/p^n\mathbb{Z}$ est cyclique.

1) Montrer que, pour tout $k \in \mathbb{N}^*$, $(1+p)^{p^k} \equiv 1\,[p^{k+1}]$ et $(1+p)^{p^k} \not\equiv 1\,[p^{k+2}]$.
2) En déduire l'ordre de la classe de $1+p$ dans le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$.
3) On admet que le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique ; soit x un entier tel que $\overline{x}$ soit un élément générateur de ce groupe. Montrer que la classe de x dans $(\mathbb{Z}/p^n\mathbb{Z})^*$ a pour ordre un multiple de $p-1$. En déduire qu'il existe dans ce groupe un élément y d'ordre $p-1$ et conclure.

●●●

EXERCICE F

Un réel α est dit *algébrique* s'il existe un polynôme P à coefficients entiers (relatifs) admettant α pour racine.

1) Montrer que tout nombre rationnel est algébrique. La réciproque est-elle vraie ?
2) Soit α un réel algébrique. Montrer que l'ensemble des polynômes à coefficients rationnels admettant α pour racine est un idéal de l'anneau $\mathbb{Q}[X]$. En déduire l'existence d'un polynôme P_0 à coefficients entiers premiers entre eux dans leur ensemble, qui engendre cet idéal. Montrer que P_0 est unique au signe près. Celui qui a un coefficient dominant positif est appelé *polynôme minimal* de α.

3) Déterminer le polynôme minimal de chacun des réels algébriques suivants :

$$\alpha = \frac{\sqrt{5}+1}{2}\,; \qquad \alpha = \sqrt{\sqrt{3}+\sqrt{2}} - \sqrt{\sqrt{3}-\sqrt{2}}\,; \qquad \alpha = \cos(\frac{2\pi}{5}).$$

●●● **EXERCICE G** **Principe du codage RSA**

Soit p et q deux nombres premiers distincts. On pose $n = pq$.

1) Déterminer $\varphi(n)$, indicatrice d'Euler de n.
2) Soit x un entier compris entre 1 et $n-1$. Montrer, à l'aide du petit théorème de Fermat, que p divise x ou $x^{p-1}-1$, et que q divise x ou $x^{q-1}-1$.
3) Montrer que, quel que soit l'entier naturel k, $x^{k\varphi(n)+1}$ est congru à x modulo n.
4) Soit c un entier premier avec $\varphi(n)$. Montrer qu'il existe un entier d tel que cd soit congru à 1 modulo $\varphi(n)$. En déduire que x^{cd} est congru à x modulo n.
5) Ce qui précède constitue le principe du cryptage RSA : un destinataire désirant se faire envoyer des messages cryptés diffuse librement une clé de codage c ; il conserve précieusement pour lui-même la clé de décodage correspondante d. L'expéditeur d'un message doit le numériser sous forme d'un entier x (opération facile à casser), puis calculer la classe de x^c modulo n, qui constituera le message crypté y.
   a) Comment le destinataire peut-il décrypter le message ? Pourquoi est-il le seul à pouvoir le faire ?
   b) Sur quoi repose la sécurité du système ?
   c) Exemple : On choisit $p = 397$, $q = 457$, $c = 1789$. Calculer la clé de décodage d. Crypter puis décrypter le message « RAS » (numérisé en représentant chaque lettre par son numéro alphabétique).

Sujets de concours

●○○ **SUJET I** **Oral CCINP MP**

Soit $\theta \in \mathbb{R}$ et $n \in \mathbb{N}^*$. Décomposer en produit de polynômes irréductibles sur $\mathbb{C}[X]$, puis sur $\mathbb{R}[X]$, le polynôme :

$$P = X^{2n} - 2X^n \cos(n\theta) + 1.$$

●●○ **SUJET II** **Oral Mines MP**

Soit p un nombre premier impair et q un diviseur premier de $2^p - 1$.
Montrer que $q \equiv 1\,[2p]$.

●●○ **SUJET III** **Oral Centrale MP**

Soit p et q deux entiers premiers entre eux.
On considère les polynômes $A = (1-X^p)(1-X^q)$ et $B = (1-X^{pq})(1-X)$. Montrer que A divise B et que le quotient $Q = \frac{B}{A}$ est à coefficients entiers. Calculer $Q(0)$ et $Q(1)$.

●●○ **SUJET IV** **Oral X MP**

1) Soit $P \in \mathbb{Z}[X]$, $n \in \mathbb{N}^*$, $m = P(n)$. Montrer que : $\forall k \in \mathbb{Z},\ m | P(n+km)$.
2) En déduire qu'il n'existe aucun polynôme P à coefficients entiers non constant tel que, pour tout entier $n \in \mathbb{Z}$, $P(n)$ soit un nombre premier.

●●○ **SUJET V** **Oral X MP**

Soit $P \in \mathbb{Z}[X]$ un polynôme à coefficients entiers et $\alpha \in \mathbb{Z}$ une racine entière de P.

1) On sait qu'il existe un polynôme $Q \in \mathbb{Q}[X]$ tel que $P(X) = (X-\alpha)Q(X)$.
Montrer que $Q \in \mathbb{Z}[X]$.
2) En déduire que si $x \in \mathbb{Z}$ est un entier non racine de P, alors $x-\alpha$ divise $P(x)$.
3) Donner une méthode pour trouver toutes les racines entières de P.
4) Exemple : trouver les racines entières de $P = X^4 - 8X^2 + 5X + 6$.

●●● **SUJET VI** **Oral Centrale MP**

Soit A un sous-anneau de $\mathbb{Q}$.

1) Soit $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$, premiers entre eux. Montrer que, si $p/q \in A$, alors $1/q \in A$.
2) Soit I un idéal de A distinct de $\{0\}$. Montrer qu'il existe $n \in \mathbb{N}^*$ tel que $I \cap \mathbb{Z} = n\mathbb{Z}$ et qu'alors $I = nA$.
3) Soit p un nombre premier. On pose : $Z_p = \{a/b;\ a \in \mathbb{Z},\ b \in \mathbb{N}^*,\ p \wedge b = 1\}$. Montrer que, si $x \in \mathbb{Q}^*$, alors x ou $1/x$ appartient à Z_p.
4) On suppose ici que, pour tout $x \in \mathbb{Q}^*$, x ou $1/x$ appartient à A. On note I l'ensemble des éléments non inversibles de A.
   a) Montrer que I est un idéal de A.
   b) Montrer que tout idéal strict de A est inclus dans I.
   c) En déduire que $A = \mathbb{Q}$ ou $A = Z_p$ pour un certain nombre premier p.

●●● **SUJET VII** **Oral ENS Lyon MP**

Soit A une $\mathbb{R}$-algèbre de dimension finie et intègre. On identifie $\mathbb{R}1_A$ à $\mathbb{R}$.

1) Montrer que A est un corps.
2) Montrer que pour tout $x \in A$, il existe $(\alpha, \beta) \in \mathbb{R}^2$ tel que $x^2 = \alpha x + \beta$.
3) Montrer que pour tout $x \in A$, $x^2 \in \mathbb{R}_+ \Rightarrow x \in \mathbb{R}$.
4) Soit $V = \{x \in A,\ x^2 \in \mathbb{R}_-\}$. Montrer que pour tout $x \in A$, il existe un unique $\xi \in \mathbb{R}$ tel que $(x-\xi) \in V$.
5) Soit $(x, y) \in V^2$, $(\alpha, \beta) \in \mathbb{R}^2$. Montrer que $\alpha x + \beta y \in \mathbb{R} \Rightarrow \alpha x + \beta y = 0$.
6) Montrer que V est un $\mathbb{R}$-espace vectoriel, supplémentaire de $\mathbb{R}$ dans A.
7) On suppose que $V \neq \{0\}$. Montrer qu'il existe un élément $v \in V$ tel que $v^2 = -1$. Quelle est la dimension de V ? Celle de A ?
8) Montrer que l'algèbre A est isomorphe à $\mathbb{R}$ ou $\mathbb{C}$.

●●● **SUJET VIII** **Oral Centrale MP**

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de $\mathbb{C}[X]$, unitaire, admettant pour racines $(\lambda_1, \ldots, \lambda_n)$ (comptées avec leur ordre de multiplicité). On note :

$$\|P\| = \sum_{k=0}^{n} |a_k| \,; \qquad L(P) = \left(\sum_{k=0}^{n} |a_k|^2\right)^{\frac{1}{2}} \,; \qquad M(P) = \prod_{k=1}^{n} \max(1, |\lambda_k|).$$

1) Montrer que $\forall k \in [\![0, n]\!],\ |a_k| \leqslant \binom{n}{k} M(P)$.
2) En déduire que $L(P) \leqslant 2^n M(P)$.
3) Montrer que $L(P)^2 = \frac{1}{2\pi} \int_0^{2\pi} |P(e^{i\theta})|^2 d\theta$.
4) En déduire que, si $P = (X-\lambda)Q$, alors : $L(P) = L\big((\overline{\lambda}X - 1)Q\big)$. En déduire une expression de $L(P)$, en distinguant les racines de module supérieur à 1 des autres.
5) Démontrer que : $L(P) \geqslant M(P)$ (inégalité de Landau).

EXERCICES

●●○ **SUJET IX** **Compilation de plusieurs sujets d'écrit CCINP et Centrale**

Partie A : Anneaux $\mathbb{Z}[\sqrt{n}]$

Soit n un entier naturel qui n'est pas le carré d'un entier. On désigne par $\mathbb{Z}[\sqrt{n}]$ l'ensemble des nombres réels de la forme $a+b\sqrt{n}$, où a et b sont des entiers relatifs quelconques.

1) Montrer que l'application de $\mathbb{Z}^2$ dans $\mathbb{Z}[\sqrt{n}]$: $(a,b)\mapsto a+b\sqrt{n}$ est bijective.
2) Montrer que $\mathbb{Z}[\sqrt{n}]$ est un sous-anneau de $\mathbb{R}$. Est-il intègre ?
3) Montrer que l'application φ de $\mathbb{Z}[\sqrt{n}]$ dans $\mathbb{Z}[\sqrt{n}]$: $a+b\sqrt{n}\mapsto a-b\sqrt{n}$ est un automorphisme involutif de $\mathbb{Z}[\sqrt{n}]$.
4) Pour tout élément x de $\mathbb{Z}[\sqrt{n}]$, on considère le produit $N(x)=x\varphi(x)$.
   a) Montrer que $\forall x\in\mathbb{Z}[\sqrt{n}],\quad N(x)=0 \iff x=0$.
   b) Montrer que $\forall (x,y)\in\mathbb{Z}[\sqrt{n}]^2,\quad N(xy)=N(x)N(y)$.
5) Montrer que x élément de $\mathbb{Z}[\sqrt{n}]$ est inversible dans $\mathbb{Z}[\sqrt{n}]$ si et seulement si $N(x)=\pm 1$.

Partie B : Étude de l'anneau $\mathbb{Z}[\sqrt{5}]$

On choisit dans cette partie $n=5$.

1) Donner quelques exemples d'éléments inversibles de l'anneau $\mathbb{Z}[\sqrt{5}]$. Démontrer qu'il en existe une infinité.
2) a) Démontrer qu'il n'existe pas d'entiers relatifs c et d tels que $c^2-5d^2=\pm 2$ (on pourra raisonner dans l'anneau $\mathbb{Z}/4\mathbb{Z}$).
   b) En déduire que l'élément 2 est premier (ou irréductible) dans l'anneau $\mathbb{Z}[\sqrt{5}]$, c'est-à-dire que, s'il existe deux éléments x et y de $\mathbb{Z}[\sqrt{5}]$ tels que $xy=2$, alors x ou y est inversible.
3) Soit I l'ensemble des éléments $x=a+b\sqrt{5}$ de $\mathbb{Z}[\sqrt{5}]$ tels que les entiers a et b soient de même parité. Démontrer que I est un idéal de l'anneau $\mathbb{Z}[\sqrt{5}]$.
4) On suppose que l'idéal I est engendré par un élément x. Il existe donc des éléments y et z de $\mathbb{Z}[\sqrt{5}]$ tels que $2=xy$ et $1+\sqrt{5}=xz$. Trouver une contradiction. Que peut-on dire de l'anneau $\mathbb{Z}[\sqrt{5}]$?

Partie C : Anneau des entiers de Gauss

On appelle *entier de Gauss* un nombre complexe dont la partie réelle et la partie imaginaire sont des entiers relatifs : $u=a+ib, (a,b)\in\mathbb{Z}^2$. On désigne par $\mathbb{Z}[i]$ l'ensemble des entiers de Gauss.

1) Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$. Est-il intègre ? Est-ce un corps ?
2) a) Montrer que, pour tout $u\in\mathbb{Z}[i]$, $|u|^2$ est un entier naturel.
   b) Montrer que u est inversible dans $\mathbb{Z}[i]$ si et seulement si $|u|=1$.
   c) En déduire l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}[i]$. Quel groupe connu reconnaît-on ?
3) Étant donné deux éléments non nuls u et v de $\mathbb{Z}[i]$, on dit que u *divise* v (ou que v est un *multiple* de u) s'il existe $w\in\mathbb{Z}[i]$ tel que : $v=uw$.
   a) Montrer que, si u divise v dans $\mathbb{Z}[i]$, alors $|u|^2$ divise $|v|^2$ dans $\mathbb{N}$.
   b) $2+i$ et $2-i$ sont-ils des diviseurs de $4+7i$? La réciproque de la question (a) est-elle vraie ?
   c) Deux entiers de Gauss sont dits *associés* si chacun divise l'autre. Montrer qu'il s'agit d'une relation d'équivalence. Quelle est la classe d'équivalence d'un élément $u=a+ib$ de $\mathbb{Z}[i]$?
4) a) Montrer que, pour tout nombre complexe z, il existe un entier de Gauss u tel que $|z-u|<1$.
   b) En déduire que, pour tout couple $(u,v)\in\mathbb{Z}[i]^2$, avec $v\neq 0$, il existe un couple $(q,r)\in\mathbb{Z}[i]^2$ tel que $u=vq+r$ et $|r|<|v|$.
   c) Le couple (q,r) est-il unique ? Déterminer toutes les solutions $(q,r)\in\mathbb{Z}[i]^2$ pour $u=1-i$ et $v=2i$.
5) Montrer que l'anneau $\mathbb{Z}[i]$ est principal.
6) Un entier de Gauss u, non nul et non inversible, est dit *premier* (ou *irréductible*) s'il n'admet pas d'autres diviseurs que les inversibles et les éléments qui lui sont associés.
   a) Montrer que, si $|u|^2$ est premier dans $\mathbb{N}$, alors u est premier dans $\mathbb{Z}[i]$.
   b) Les entiers 2 et 3 sont-ils premiers dans $\mathbb{Z}[i]$? La réciproque de la question a) est-elle vraie ?

c) Montrer que, si $u = a + ib$, avec $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}^*$, est premier dans $\mathbb{Z}[i]$, alors $|u|^2 = a^2 + b^2$ est premier dans $\mathbb{N}$.
d) Montrer que la somme de deux carrés d'entiers naturels n'est jamais congrue à 3 modulo 4. Montrer qu'un entier naturel congru à 3 modulo 4 premier dans $\mathbb{N}$ est premier dans $\mathbb{Z}[i]$.
e) On admet qu'un entier naturel congru à 1 modulo 4 premier dans $\mathbb{N}$ est toujours somme de deux carrés d'entiers naturels ; en déduire qu'il n'est pas premier dans $\mathbb{Z}[i]$.
f) Quel est l'ensemble des éléments premiers de $\mathbb{Z}[i]$?

Aides à la résolution des exercices

Exercices d'application du chapitre 2

Exercice 1. Vérifiez soigneusement toutes les conditions de la définition d'un idéal.

Exercice 2.
1) À quelle condition (n divise ab) implique (n divise a ou b) ?
2) Traduisez la condition (l'idéal I est premier) en termes de classes d'équivalence dans A/I.

Exercice 3. Calculez, à l'aide de la formule du binôme, $(x-y)^N$, avec N suffisamment grand pour que tous les termes soient nuls.

Exercice 4. Remarquez que $10 \equiv -1\ [11]$.

Exercice 5. L'ordre d'un élément x d'un groupe fini G est le plus petit diviseur d du cardinal du groupe tel que $x^d = 1_G$.

Exercice 6.
1) Écrivez $M(a,b)$ sous la forme $a\mathrm{I}_3 + bJ$.
2) Calculez le déterminant de $M(a,b)$.

Exercice 7. Si le polynôme P n'est pas constant, envisagez l'une de ses racines ayant le plus grand module.

Exercices d'approfondissement du chapitre 2

Exercice A. Même méthode que dans l'exercice 5. La deuxième question se résout par récurrence.

Exercice B. Quelle est la classe modulo p du produit de toutes les classes inversibles ?

Exercice C.
1) L'application f_k est injective si et seulement si $\overline{k}\,\overline{x} = \overline{0}$ implique $\overline{x} = \overline{0}$.
2) Pour montrer la surjectivité de φ, considérez un automorphisme f de $\mathbb{Z}/n\mathbb{Z}$ et calculez $\varphi(\overline{k})$, où $\overline{k} = f(\overline{1})$.

Exercice D. L'exercice est bien détaillé. Faites attention aux ensembles précis auxquels appartiennent chacune des variables.
L'anneau $\mathbb{Z}[\sqrt{2}]$ est un exemple d'anneau $\mathbb{Z}[\sqrt{n}]$ faisant l'objet du problème IX à la fin de ce chapitre.

Exercice E. 1) Raisonnez par récurrence.

Exercice F. Si un réel α est racine d'un polynôme irréductible P de $\mathbb{Z}[X]$, P est le polynôme minimal de α.

Exercice G.
2) Pensez au théorème de Fermat.
3) Pensez à la récurrence.
4) $\overline{c}$ est inversible dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$.

CORRIGÉS

Corrigés des Vrai/Faux

a) Vrai.
b) Faux, si $f'(0)=0$, $(fg)'(0)=f(0)g'(0)$.
c) Vrai. Un idéal qui contient 1_A est égal à A.
d) Faux. Par exemple, $(1,0)\times(0,1)=(0,0)$.
e) Faux. Par exemple, dans $\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$, $40(x,y)$ est toujours nul, alors que dans $\mathbb{Z}/80\mathbb{Z}$, $40\times\overline{1}\neq\overline{0}$.
f) Vrai, car 6 et 25 sont premiers entre eux.
g) Faux. Il faut supposer p et q premiers entre eux.
h) Faux. Dans $\mathbb{R}[X]$, les polynômes $(X-1)(X^2+1)$ et $(X+1)(X^2+1)$ n'ont pas de racine commune, mais leur PGCD est X^2+1. La propriété est vraie pour des polynômes scindés, donc en particulier dans $\mathbb{C}[X]$.
i) Faux, puisque $\deg(X^6+1)>2$.
j) Faux. $\mathbb{R}$ n'est pas stable par combinaisons linéaires à coefficients complexes.

Corrigés des exercices d'application

EXERCICE 1

Soit $\mathrm{Ann}(M)$ l'annulateur de M.
- $\mathrm{Ann}(M)\neq\varnothing$, car $0_A\in\mathrm{Ann}(M)$.
- Soit $(a,b)\in\mathrm{Ann}(M)^2$. Si $m\in M$ alors $am=bm=0_A$ d'où $(a-b)m=0_A$. Ainsi $a-b\in\mathrm{Ann}(M)$.

Par conséquent $(\mathrm{Ann}(M),+)$ est un sous-groupe de $(A,+)$.
- Soit $a\in\mathrm{Ann}(M)$ et $x\in A$. Si $m\in M$ alors $am=0_A$ d'où $xam=0_A$. Ainsi $xa\in\mathrm{Ann}(M)$.

Finalement $\mathrm{Ann}(M)$ est un idéal de A.

EXERCICE 2

1) L'idéal $n\mathbb{Z}$ de l'anneau $\mathbb{Z}$ est premier si et seulement si $ab\in n\mathbb{Z}$ implique $a\in\mathbb{Z}$ et $b\in\mathbb{Z}$, c'est-à-dire n divise ab implique n divise a ou b, ce qui caractérise un entier n premier.
2) Remarquons que $a\in I$ équivaut à $\overline{a}=\overline{0}$. Il s'ensuit que l'idéal I est premier si et seulement si dans A/I l'égalité $\overline{ab}=\overline{0}$ implique $\overline{a}=\overline{0}$ ou $\overline{b}=\overline{0}$. C'est la définition d'un anneau intègre.
3) Soit J un idéal premier de A' et $(a,b)\in A^2$ tel que $ab\in f^{-1}(J)$. Par définition, $f(ab)\in J$ soit $f(a)f(b)\in J$. Par hypothèse $f(a)\in J$ ou $f(b)\in J$, c'est-à-dire $a\in f^{-1}(J)$ ou $b\in f^{-1}(J)$. Ceci signifie que $f^{-1}(J)$ est un idéal premier.

EXERCICE 3

1) Soit $\mathcal{N}$ l'ensemble des éléments nilpotents de A.
- Tout d'abord $\mathcal{N}\neq\varnothing$, car 0_A est nilpotent.
- Soit $(x,y)\in\mathcal{N}^2$ et $(n,m)\in\mathbb{N}^{*2}$ tel que $x^n=y^m=0_A$. Alors :

$$(x-y)^{n+m-1}=\sum_{k=0}^{n+m-1}\binom{n+m-1}{k}x^k(-y)^{n+m-1-k}.$$

Si $k \geqslant n$, alors $x^k = 0_A$; si $k < n$, alors $n+m-1-k \geqslant m$ donc $(-y)^{n+m-1-k} = 0_A$.
Par conséquent $(x-y)^{n+m-1} = 0_A$ soit $x - y \in \mathcal{N}$. Finalement $(\mathcal{N}, +)$ est un sous-groupe de $(A, +)$.
• Soit $x \in \mathcal{N}$ et $a \in A$. Il existe $n \in \mathbb{N}$ tel que $x^n = 0_A$. Alors $(ax)^n = a^n x^n = 0_A$. Ainsi $ax \in \mathcal{N}$.
En conclusion $\mathcal{N}$ est un idéal de A.
2) Soit $x \in A$ tel que $x^n = 0_A$. Par télescopage, il vient :

$$(1_A - x)\sum_{k=0}^{n-1} x^k = \sum_{k=0}^{n-1} x^k - \sum_{k=1}^{n} x^k = 1_A - x^n = 1_A.$$

De même, $\left(\sum_{k=0}^{n-1} x^k\right)(1_A - x) = 1_A$. Finalement, $1_A - x$ est inversible et son inverse est :

$$(1_A - x)^{-1} = \sum_{k=0}^{n-1} x^k.$$

EXERCICE 4

1) $10 = 11 - 1$ donc $10 \equiv -1\ [11]$. Alors, $n \equiv \sum_{i=0}^{k} b_i 10^i \equiv \sum_{i=0}^{k} b_i (-1)^i\ [11]$.
2) *Idem* avec $100 = 101 - 1$, donc $100 \equiv -1\ [101]$.
Prendre la somme alternée des chiffres deux par deux modulo 101. Par exemple :

$$1234 \equiv 34 - 12 \equiv 22\ \ [101].$$

$$2^{22} = 4 \times 1024 \times 1024 \equiv 4 \times 14 \times 14 \equiv 56 \times 14 \equiv 784 \equiv 84 - 7 \equiv 77\ [101].$$

EXERCICE 5

1) Les inversibles de $\mathbb{Z}/32\mathbb{Z}$ sont les classes des entiers de 0 à 31 premiers avec 32, c'est-à-dire impairs. Donc $\mathrm{Card}(G) = 16$.
2) L'ordre de $\overline{5}$ est un diviseur de 16, soit 2, 4, 8 ou 16. Or $\overline{5}^2 = \overline{25} = -\overline{7}$; $\overline{5}^4 = \overline{49} = \overline{17} = -\overline{15}$; $\overline{5}^8 = \overline{225} = \overline{1}$.
L'élément $\overline{5}$ est donc d'ordre 8. On trouve de même que l'élément $\overline{15}$ est d'ordre 2.
3) Posons $G' = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ et définissons $\varphi : G' \to G$ par $\varphi(\overline{a}, \overline{b}) = \overline{15}^a \overline{5}^b$. On vérifie que φ est un morphisme de groupes de $(G', +)$ dans $(G, \cdot)$.
Soit $(\overline{a}, \overline{b}) \in \mathrm{Ker}\ \varphi$. Alors $\varphi(\overline{a}, \overline{b}) = \overline{15}^a \overline{5}^b = \overline{1}$, d'où $\overline{5}^b = \overline{15}^{2-a}$. D'après les calculs de 2), il vient $<\overline{5}> \cap <\overline{15}> = \{\overline{1}\}$, d'où $a = 0$ et $b = 0$. Le morphisme φ est ainsi injectif. Comme $\mathrm{Card}(G) = \mathrm{Card}(G')$, il est bijectif. Les groupes $(G, \cdot)$ et $(G', +)$ sont isomorphes.

EXERCICE 6

1) On peut écrire : $M(a, b) = a\mathrm{I}_3 + bJ$, avec $J = M(0, 1) = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$.
Ainsi, E est le sous-espace vectoriel de $\mathcal{M}_3(\mathbb{R})$ engendré par la famille (I_3, J). De plus, E contient la matrice unité I_3. Montrons que E est stable par multiplication :

$$\forall (a, b, a', b') \in \mathbb{R}^4, \quad M(a, b)M(a', b') = (a\mathrm{I}_3 + bJ)(a'\mathrm{I}_3 + b'J) = aa'\mathrm{I}_3 + (ab' + a'b)J + bb'J^2.$$

Or $J^2 = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix} = 2\mathrm{I}_3 + J$, qui appartient à E. Donc $M(a, b)M(a', b') \in E$. E est bien une sous-algèbre de $\mathcal{M}_3(\mathbb{R})$.

2) Une matrice carrée est inversible si et seulement si son déterminant est non nul.

$$\det\big(M(a,b)\big) = \begin{vmatrix} a & b & b \\ b & a & b \\ b & b & a \end{vmatrix} = \begin{vmatrix} a & b & a+2b \\ b & a & a+2b \\ b & b & a+2b \end{vmatrix} = \begin{vmatrix} a & b & a+2b \\ b-a & a-b & 0 \\ 0 & b-a & 0 \end{vmatrix} = (a+2b)(b-a)^2.$$

Les éléments inversibles de E sont les matrices $M(a,b)$ telles que $a \neq b$ et $a \neq -2b$.

EXERCICE 7

Supposons que le polynôme P ne soit pas constant. L'ensemble de ses racines est alors fini et non vide. L'ensemble des modules des racines est une partie finie non vide de $\mathbb{R}$, qui possède donc un plus grand élément M. Soit α une racine de P de module M. On a alors :

$$\begin{cases} P\big((\alpha+1)^2\big) = P(\alpha)P(\alpha+2) = 0 \\ P\big((\alpha-1)^2\big) = P(\alpha-2)P(\alpha) = 0 \end{cases}.$$

Donc $(\alpha+1)^2$ et $(\alpha-1)^2$ sont également racines de P. Il s'en suit qu'elles ont chacune un module inférieur ou égal à $|\alpha|$. or : $(\alpha+1)^2-(\alpha-1)^2 = 4\alpha$, d'où : $4|\alpha| \leqslant \big|(\alpha+1)^2\big| + \big|(\alpha-1)^2\big| \leqslant 2|\alpha|$. On en déduit $\alpha = 0$, or dans ce cas $(\alpha+1)^2 = \alpha-1)^2 = 1$, ce qui contredit le fait que α soit la racine de plus grand module.

On a donc démontré par l'absurde que le polynôme P est constant. Si $P(X) = C$, alors $C = C^2$, d'où $C \in \{0,1\}$: le polynôme P est soit nul (il a une infinité de racines) soit égal à 1 (il n'a aucune racine).

Corrigés des exercices d'approfondissement

EXERCICE A

1) Les inversibles de $\mathbb{Z}/2^n\mathbb{Z}$ sont les classes des entiers de 0 à 2^n-1 qui sont premiers avec 2^n, c'est-à-dire impairs. Il s'ensuit que $\mathrm{Card}(G) = 2^{n-1}$.

2) Récurrence :

- Pour $n = 3$: $5 \equiv 2^2+1\,[8]$.
- Soit $n \geqslant 3$ tel que $5^{2^{n-3}} \equiv 2^{n-1}+1\,[2^n]$.

$$5^{2^{n-2}} = \left(5^{2^{n-3}}\right)^2 = (2^{n-1}+1+k2^n)^2 = 2^{2n-2}+1+k^2 2^{2n}+2^n+k2^{n+1}+k2^{2n} \equiv 2^n+1\,[2^{n+1}].$$

3) L'ordre de $\overline{5}$ est un diviseur de l'ordre de G ; il est donc de la forme 2^p avec $p \leqslant n-1$. La question précédente fournit $5^{2^{n-3}} \not\equiv 1\,[2^n]$ ainsi que $5^{2^{n-2}} \equiv (5^{2^{n-3}})^2 \equiv (2^n+1)^2 \equiv 1\,[2^n]$. L'ordre de $\overline{5}$ est finalement 2^{n-2}.

EXERCICE B

1) Si $(p-1)! \equiv -1\,[p]$, alors p est premier avec $1, 2, \ldots, p-1$, donc p est un nombre premier. Réciproquement, si p est premier, alors toutes les classes $\overline{1}, \overline{2}, \ldots, \overline{(p-1)}$ sont inversibles dans $\mathbb{Z}/p\mathbb{Z}$.
Effectuons le produit de ces classes. Remarquons que pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, $x^2 = \overline{1}$ équivaut à $(x-\overline{1})(x+\overline{1}) = \overline{0}$; par intégrité de $\mathbb{Z}/p\mathbb{Z}$, on en déduit que seules deux classes sont leur propre inverse, à savoir $\overline{1}$ et $\overline{(-1)}$, qui est aussi $\overline{(p-1)}$. Ainsi dans le produit $\overline{1}\cdots\overline{(p-1)}$ on peut regrouper chaque classe avec son inverse, sauf celles qui sont leur propre inverse. Le produit est donc égal à $\overline{(-1)}$.

2) Ici, dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{(4n)!} = \overline{(-1)}\,[p]$. Mais : $\overline{(4n)!} = \overline{1}\cdot\overline{2}\cdots\overline{(2n)}\,\overline{(-2n)}\cdots\overline{(-2)}\,\overline{(-1)} = \overline{(2n)!}^2$.

CORRIGÉS

EXERCICE C

1) $\overline{k}(\overline{x}+\overline{y})=\overline{k}\overline{x}+\overline{k}\overline{y}$: f_k est un morphisme. Il est bijectif si et seulement si $k\wedge n=1$.
2) $\varphi(\overline{k})\circ\varphi(\overline{k'})=f_k\circ f_{k'}=f_{kk'}=\varphi(\overline{kk'})$: φ est un morphisme.
Ker $\varphi=\{\overline{k}\in(\mathbb{Z}/n\mathbb{Z})^*, f_k=\mathrm{Id}\}=\{\overline{1}\}$: φ est injectif.
Soit $f\in\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. Posons $\overline{k}=f(\overline{1})$. Il vient $f(\overline{2})=f(\overline{1}+\overline{1})=f(\overline{1})+f(\overline{1})=\overline{2}f(\overline{1})=\overline{2k}$, puis par récurrence pour tout $\overline{x}$: $f(\overline{x})=\overline{k}\overline{x}$, d'où $f=f_k=\varphi(\overline{k})$. Le morphisme φ est surjectif.
Finalement les groupes $((\mathbb{Z}/n\mathbb{Z})^*,\times)$ et $(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}),\circ)$ sont isomorphes.

EXERCICE D

1) Immédiat.
2) a) Il suffit de montrer que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$.
b) Si $a+b\sqrt{2}\in G$, il existe $(a',b')\in\mathbb{Z}^2$ tel que : $(a+b\sqrt{2})(a'+b'\sqrt{2})=1$, c'est-à-dire :

$$\begin{cases} aa'+2bb'=1 \\ ab'+a'b=0 \end{cases}.$$

On en déduit : $(a-b\sqrt{2})(a'-b'\sqrt{2})=1$, puis en multipliant membre à membre :

$$(a^2-2b^2)(a'^2-2b'^2)=1.$$

L'entier relatif a^2-2b^2 est inversible dans $\mathbb{Z}$, d'où : $a^2-2b^2=\pm1$.
Réciproquement :
- si $a^2-2b^2=1$, alors $(a+b\sqrt{2})(a-b\sqrt{2})=1$, donc $a+b\sqrt{2}\in G$;
- si $a^2-2b^2=-1$, alors $(a+b\sqrt{2})(-a+b\sqrt{2})=1$, donc $a+b\sqrt{2}\in G$.

c) Soit $(a,b)\in\mathbb{N}^{*2}$ tel que $a+b\sqrt{2}\in G$.
i. Distinguons deux cas :
- si $a^2-2b^2=1$, alors $a^2-b^2=b^2+1>0$, donc $a>b$; de plus $a^2-4b^2=1-2b^2$; or $b\geqslant1$ donc $a^2-4b^2\leqslant-1<0$ et $a<2b$;
- si $a^2-2b^2=-1$, alors $a^2-b^2=b^2-1\geqslant0$, donc $a\geqslant b$; de plus $a^2-4b^2=-1-2b^2<0$, donc $a<2b$.

ii. $a_1+b_1\sqrt{2}=\dfrac{a+b\sqrt{2}}{1+\sqrt{2}}=(a+b\sqrt{2})(\sqrt{2}-1)=(2b-a)+(a-b)\sqrt{2}$. D'où :

$$\begin{cases} a_1=2b-a \\ b_1=a-b \end{cases}.$$

$$a_1^2-2b_1^2=(2b-a)^2-2(a-b)^2=-a^2+2b^2=\pm1.$$

Donc $a_1+b_1\sqrt{2}\in G$. On a immédiatement $a_1>0$ et $b_1\geqslant0$.
De plus : $a_1-a=2b-2a\leqslant0$, d'où : $a_1\leqslant a$; et $b_1-b=a-2b<0$, d'où : $b_1<b$.

iii. En réitérant le procédé, on obtient des suites d'entiers naturels (a_i) décroissante et (b_i) strictement décroissante, donc finie. Il existe $q\in\mathbb{N}^*$ tel que $b_q=0$. On a alors :

$$a_q+b_q\sqrt{2}=1,\quad a_{q-1}+b_{q-1}\sqrt{2}=1+\sqrt{2},\quad a_{q-2}+b_{q-2}\sqrt{2}=(1+\sqrt{2})^2,\quad \text{jusqu'à}\quad a+b\sqrt{2}=(1+\sqrt{2})^q.$$

On remarque que si q est pair, $a^2-2b^2=1$ et si q est impair, $a^2-2b^2=-1$.

3) Considérons $(r,s)\in\mathbb{N}^{*2}$ vérifiant l'équation (2) : $r^2-2s^2=1$. D'après ce qui précède, $r+s\sqrt{2}\in G$ et donc il existe $q\in\mathbb{N}^*$ tel que $r+s\sqrt{2}=(1+\sqrt{2})^q$. Réciproquement, si $r+s\sqrt{2}=(1+\sqrt{2})^q$, $r^2-2s^2=(-1)^q$; le couple $(r,s)\in\mathbb{N}^{*2}$ vérifie l'équation (2) si et seulement si q est pair, de la forme $2k$. L'ensemble des solutions de l'équation (2) est l'ensemble des couples $(r,s)\in\mathbb{N}^{*2}$ tels que $r+s\sqrt{2}=(1+\sqrt{2})^{2k}$, avec $k\in\mathbb{N}^*$.

On a alors $r - s\sqrt{2} = (1-\sqrt{2})^{2k}$, d'où :

$$\begin{cases} r = \dfrac{(1+\sqrt{2})^{2k} + (1-\sqrt{2})^{2k}}{2} \\ s = \dfrac{(1+\sqrt{2})^{2k} - (1-\sqrt{2})^{2k}}{2\sqrt{2}} \end{cases}.$$

Revenant aux entiers n et p, on obtient :

$$\begin{cases} n = \dfrac{(1+\sqrt{2})^{2k} + (1-\sqrt{2})^{2k} - 2}{4} \\ p = \dfrac{(1+\sqrt{2})^{2k} - (1-\sqrt{2})^{2k}}{4\sqrt{2}} \end{cases}.$$

L'ensemble des entiers triangulaires carrés est l'ensemble des entiers de la forme :

$$N = p^2 = \frac{\left((1+\sqrt{2})^{2k} - (1-\sqrt{2})^{2k}\right)^2}{32}, \quad \text{où } k \in \mathbb{N}^*.$$

Table des premières valeurs :

k	n	p	N
1	1	1	1
2	8	6	36
3	49	35	1225
4	288	204	41616
5	1681	1189	1413721
6	9800	6930	48024900
7	57121	40391	1631432881
8	332928	235416	55420693056

EXERCICE E

1) Récurrence : pour $k = 1$, $(1+p)^p = 1 + p^2 + \mu p^3$, qui est congru à 1 modulo p^2 et à $1 + p^2$ modulo p^3. Soit $k \in \mathbb{N}^*$ tel que $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ avec $\lambda \notin p\mathbb{Z}$:

$$(1+p)^{p^{k+1}} = (1+\lambda p^{k+1})^p = 1 + \lambda p^{k+2} + \mu p^{k+3} \equiv 1\,[p^{k+2}].$$

2) $(1+p)^{p^{n-1}} \equiv 1\,[p^n]$ et $(1+p)^{p^{n-2}} \not\equiv 1\,[p^n]$. Donc l'ordre de $1+p$ est p^{n-1}.
3) x a pour ordre $p-1$ dans $\mathbb{Z}/p\mathbb{Z}$. On considère le morphisme de groupes $(\mathbb{Z}/p^n\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ qui, à la classe de x modulo p^n, associe sa classe modulo p. L'ordre de x dans $(\mathbb{Z}/p^n\mathbb{Z})^*$ est un multiple de $p-1$: $q = r(p-1)$. L'élément $y = x^r$ est d'ordre $p-1$. Comme $p-1$ et p^{n-1} sont premiers entre eux, l'ordre de $y(1+p)$ est $(p-1)p^{n-1}$, c'est-à-dire $\varphi(p)$: le groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$ est cyclique.

EXERCICE F

1) Si $\alpha = \dfrac{p}{q}$ avec $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$, il est racine du polynôme $qX - p$, à coefficients entiers. Mais $\sqrt{2}$ est racine du polynôme $X^2 - 2$ et il n'est pas rationnel.
2) L'ensemble des polynômes à coefficients rationnels admettant α pour racine est non vide (il contient le polynôme nul), stable par soustraction et par multiplication par un polynôme quelconque à coefficients rationnels : c'est un idéal de $\mathbb{Q}[X]$. Comme $\mathbb{Q}$ est un corps, l'anneau $\mathbb{Q}[X]$ est principal, donc l'idéal trouvé est engendré par un seul élément $Q_0 \in \mathbb{Q}[X]$. En multipliant par le dénominateur commun des coefficients simplifiés de Q_0, on obtient un polynôme annulateur P_0 à coefficients entiers premiers entre eux dans leur ensemble. Il est unique à l'association près, c'est-à-dire ici au signe près.

3) • $\alpha = \dfrac{\sqrt{5}+1}{2}$. Alors $\alpha^2 = \dfrac{\sqrt{5}+3}{2} = \alpha + 1$, d'où $P_0 = X^2 - X - 1$.
• $\alpha = \sqrt{\sqrt{3}+\sqrt{2}} - \sqrt{\sqrt{3}-\sqrt{2}}$. Alors $\alpha^2 = 2\sqrt{3} - 2$ donc $(a^2+2)^2 = 12$ d'où $a^4 + 4a^2 - 8 = 0$. Le polynôme $P_0 = X^4 + 4X^2 - 8$ est irréductible dans $\mathbb{Z}[X]$: c'est le polynôme minimal de α.
• $\alpha = \cos(\theta)$, avec $\theta = \dfrac{2\pi}{5}$. Alors $\cos(5\theta) = 16\cos^5\theta - 20\cos^3\theta + 5\cos\theta = 1$, d'où $16\alpha^5 - 20\alpha^3 + 5\alpha - 1 = 0$. Mais $16X^5 - 20X^3 + 5X - 1 = (X-1)(4X^2+2X-1)^2$, dont les racines sont $1, \cos\frac{2\pi}{5}$ et $\cos\frac{4\pi}{5}$. Le polynôme minimal de α est $P_0 = 4X^2 + 2X - 1$.

EXERCICE G

1) Comme $p \wedge q = 1$, il vient $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$.
2) D'après le théorème de Fermat, p divise $x^p - x = x(x^{p-1} - 1)$. Comme p est premier, il divise soit x, soit $x^{p-1} - 1$. De même, q divise soit x soit $x^{q-1} - 1$.
3) Récurrence ; $k = 0$: évident. Soit $k \in \mathbb{N}$ tel que $x^{k\varphi(n)+1} \equiv x\ [n]$.
• Si x n'est divisible ni par p, ni par q, alors $x^{\varphi(n)} = x^{(p-1)(q-1)}$ est congru à 1 modulo p et modulo q, donc modulo pq. On a alors : $x^{(k+1)\varphi(n)+1} \equiv x\ [pq]$.
• Si x est divisible par p, alors $x^{\varphi(n)}$ est congru à 0 modulo p et à 1 modulo q, donc $x^{(k+1)\varphi(n)+1}$ est de toutes façons congru à x modulo p et modulo q, donc modulo pq.
4) Comme $c \wedge \varphi(n) = 1$, $\overline{c}$ est inversible dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$: il existe d tel que $cd \equiv 1\ [\varphi(n)]$, c'est-à-dire $cd = k\varphi(n) + 1$. D'après la question précédente, $x^{cd} \equiv x\ [n]$.
5) a) Si le destinataire reçoit le message y, il retrouve le message initial : $x = y^d\ [n]$. Il est seul à connaître la clé de décodage d.
b) Pour calculer d, il faut inverser $\overline{c}$ dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$, opération facile, à condition de connaître $\varphi(n)$ et donc de connaître les nombres premiers p et q. Si n est un très grand nombre (plusieurs centaines de chiffres), sa décomposition en facteurs premiers est impossible en un temps raisonnable, même pour un ordinateur très puissant.
c) Ici, $n = 181\,429$, $\varphi(n) = 180\,576$, $d = 9\,589$. Pour $x = 180\,119$, on obtient $y \equiv x^c\ [n] = 91\,322$, soit « IMV ». On retrouve bien $x \equiv y^d\ [n] = 180\,119$, soit « RAS ».

Corrigés des sujets de concours

SUJET I

Rappelons que $y^n = 1$ équivaut à $y = e^{\frac{2ik\pi}{n}}$ pour $k \in [\![0, n-1]\!]$. En appliquant à $y = x/e^{i\theta}$ et $y = x/e^{-i\theta}$, on en déduit :

$$P = (X^n - \mathrm{e}^{in\theta})(X^n - \mathrm{e}^{-in\theta}) = \prod_{k=0}^{n-1}\left(X - \mathrm{e}^{i(\theta+\frac{2k\pi}{n})}\right)\prod_{k=0}^{n-1}\left(X - \mathrm{e}^{-i(\theta+\frac{2k\pi}{n})}\right).$$

$$P = \prod_{k=0}^{n-1}\left(X^2 - 2X\cos\left(\theta + \frac{2k\pi}{n}\right) + 1\right).$$

SUJET II

On sait que q est impair, donc $q \equiv 1\ [2]$. Il suffit de prouver que $q \equiv 1\ [p]$ pour conclure grâce au théorème chinois, puisque $p \wedge 2 = 1$.
Comme $2^p \equiv 1\ [q]$, l'ordre de $\overline{2}$ dans le groupe $(\mathbb{Z}/q\mathbb{Z})^*$ est un diviseur de p. Comme ce n'est pas 1, c'est p. Or cet ordre divise le cardinal du groupe, qui est $q-1$: p divise $q-1$, c'est-à-dire $q \equiv 1\ [p]$.

SUJET III

$1-X^p$ et $1-X^q$ divisent $1-X^{pq}$; or $(1-X^p)\wedge(1-X^q)=1-X$, d'où A divise B.

$$\frac{B}{A}=\frac{(1-X^{pq})(1-X)}{(1-X^p)(1-X^q)}=\frac{\displaystyle\sum_{k=0}^{q-1}X^{kp}}{\displaystyle\sum_{k=0}^{q-1}X^k}.$$

Le numérateur et le dénominateur ayant des coefficients entiers, et le dénominateur étant unitaire, le quotient est à coefficients entiers.
On obtient facilement $Q(0)=Q(1)=1$.

SUJET IV

1) Pour tout $p\in\mathbb{N}$: $(n+km)^p\equiv n^p\ [m]$. Donc, pour tout polynôme $P\in\mathbb{Z}[X]$: $P(n+km)$ est congru à $P(n)$ modulo m ; en d'autres termes si $m=P(n)$, alors $P(n+km)\equiv 0\,[m]$.
2) Soit P un polynôme de $\mathbb{Z}[X]$ tel que, pour tout $n\in\mathbb{Z}$, $P(n)$ soit un nombre premier. Pour tout $k\in\mathbb{Z}$, $P(n)|P(n+km)$. Pour k assez grand, on a $P(n)\neq P(n+km)$ (cette dernière quantité tendant vers l'infini puisque P n'est pas constant) ; donc la relation $P(n)|P(n+km)$ avec $P(n)$ et $P(n+km)$ premiers implique $P(n)=P(m+km)$ dès que k est grand. Le polynôme $P-m$ admet une infinité de racines : il est nul ; finalement P est constant.

SUJET V

1) Posons : $P=\displaystyle\sum_{k=0}^{n}a_kX^k$ et $Q=\displaystyle\sum_{k=0}^{n-1}b_kX^k$. De l'égalité $P(X)=(X-\alpha)Q(X)$, on tire :

$$\begin{cases} a_n &= b_{n-1}\\ a_{n-1} &= b_{n-2}-\alpha b_{n-1}\\ &\vdots\\ a_{n-k} &= b_{n-k-1}-\alpha b_{n-k} \quad \text{pour tout } k\in[\![1,n-1]\!]\,.\\ &\vdots\\ a_1 &= b_0-\alpha b_1 \end{cases}$$

Montrons par récurrence que pour tout $k\in[\![1,n]\!]$, $b_{n-k}\in\mathbb{Z}$.
- Pour $k=1$, $b_{n-1}=a_n\in\mathbb{Z}$.
- Soit $k\in[\![1,n-1]\!]$ tel que $b_{n-k}\in\mathbb{Z}$. Alors, $b_{n-k-1}=a_{n-k}+\alpha b_{n-k}\in\mathbb{Z}$.

Ainsi, tous les coefficients du polynôme Q sont des entiers relatifs : $Q\in\mathbb{Z}[X]$.

2) Pour tout $x\in\mathbb{Z}$, $Q(x)\in\mathbb{Z}$ et $P(x)=(x-\alpha)Q(x)$, donc si $P(x)\neq 0$, alors $x-\alpha$ divise $P(x)$.

3) En choisissant un entier x non racine de P, l'entier $P(x)$ n'a qu'un nombre fini de diviseurs d_i dans $\mathbb{Z}$. Les racines entières de P sont à chercher parmi les valeurs $x-d_i$. La méthode est d'autant plus rapide que $P(x)$ a peu de diviseurs.

4) Exemple : pour $P=X^4-8X^2+5X+6$, on a $P(-1)=-6$, qui a 8 diviseurs dans $\mathbb{Z}$: $\{1,2,3,6,-1,-2,-3,-6\}$, mais $P(1)=4$, qui n'a que 6 diviseurs : $\{d_i\}=\{1,2,4,-1,-2,-4\}$, d'où les valeurs possibles des racines entières de P : $\{1-d_i\}=\{-3,-1,0,2,3,5\}$, parmi lesquelles seules -3 et 2 sont effectivement racines de P. L'ensemble des racines entières de $P=X^4-8X^2+5X+6$ est $\{-3,2\}$.

SUJET VI

1) D'après le théorème de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $up + vq = 1$, d'où $u\frac{p}{q} + v = \frac{1}{q}$. D'une part, $1 \in A$ donc $|v| = 1 + \cdots + 1 \in A$ (ceci prouve au passage que tout sous-anneau A de $\mathbb{Q}$ contient $\mathbb{Z}$) puis $v \in A$. D'autre part par hypothèse $\frac{1}{q} \in A$ implique $|u|\frac{p}{q} = \frac{p}{q} + \cdots + \frac{p}{q} \in A$ puis $u\frac{p}{q} \in A$. Il s'ensuit que $\frac{1}{q} \in A$.

2) $I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$. Comme $I \neq \{0\}$, il existe $\frac{p}{q} \in I$ non nul.

Alors $q\frac{p}{q} = p \in I$, d'où $p \in n\mathbb{Z}$. D'après la question précédente, $\frac{1}{q} \in A$, donc $\frac{p}{q} \in nA$. On a montré que $I \subset nA$. Réciproquement, $n \in I$, donc $nA \subset I$. En définitive, $I = nA$.

3) Z_p est un sous-anneau de $\mathbb{Q}$. Soit $x = \frac{a}{b}$ avec $a \in \mathbb{Z}^*$, $b \in \mathbb{N}^*$ et $a \wedge b = 1$. Si p ne divise pas b, alors il est premier avec b et donc $x \in Z_p$. Si p divise b, il ne divise pas a et, de même, $\frac{1}{x} \in Z_p$.

4) a) • $0 \in I$, donc $I \neq \varnothing$.

• Si $I = \{0\}$, c'est un idéal de A. Supposons maintenant que $I \neq \{0\}$. Soit x et y dans I non nuls, prouvons que $x - y$ est dans I. Remarquons que par hypothèse x et y ne sont pas inversibles *dans* A, néanmoins étant non nuls ils sont inversibles *dans* $\mathbb{Q}$: x^{-1} et y^{-1} existent mais sont des éléments de $\mathbb{Q}^*$, pas de A. Supposons que $x - y$ soit inversible dans A : il existe $z \in A$ tel que $(x - y)z = 1$. On a : $xz - yz = 1$, d'où $z - x^{-1}yz = x^{-1}$ et $y^{-1}xz - z = y^{-1}$. On sait, d'après l'hypothèse, que $x^{-1}y$ ou $y^{-1}x$ appartient à A. Puisque $z \in A$, on en déduit que $x^{-1} = z - x^{-1}yz$ ou $y^{-1} = y^{-1}xz - z$ appartient à A, c'est-à-dire que x ou y est inversible dans A, ce qui est contraire à l'hypothèse. Donc $x - y$ n'est pas inversible dans A : il appartient à I, qui est donc un sous-groupe de $(A, +)$.

• Soit $a \in A$ et $x \in I$. Supposons que ax soit inversible dans A : il existe $z \in A$ tel que $zax = 1$. Comme z et a sont dans A, $za \in A$ et, par conséquent, x est inversible dans A, ce qui est contraire à l'hypothèse. Donc ax n'est pas inversible dans A : il appartient à I, qui est donc un idéal de A.

b) Soit J un idéal de A. Si un élément x de J est inversible dans A, alors $x \times \frac{1}{x} = 1 \in J$, par conséquent $J = A$. Tout idéal strict de A est donc inclus dans I.

c) Si $I = \{0\}$, alors pour tout $x \in \mathbb{Q}^*$, x ou x^{-1} appartient à A et est inversible dans A; donc x et x^{-1} appartiennent tous deux à A, donc $A = \mathbb{Q}$.

Si $I \neq \{0\}$, d'après le résultat de la question 2), il existe $n \in \mathbb{N}^*$ tel que $I = nA$. Si $n = 1$, alors $I = A$, ce qui est absurde, car $1 \notin I$. Donc $n \geqslant 2$. Supposons que $n = n_1 n_2$ avec $(n_1, n_2) \in [\![2, n-1]\!]^2$. Comme n n'est pas inversible dans A, l'un au moins des entiers n_1 ou n_2 n'est pas inversible dans A. Supposons, par exemple, que $n_1 \in I$. Alors $n_1 A$ est un idéal strict de A, donc inclus dans I : $n_1 A \subset I$. De plus, $I = nA \subset n_1 A$ puisque n_1 divise n. En définitive, $I = n_1 A$. On peut réitérer ce procédé jusqu'à trouver un entier p, diviseur premier de n, tel que $I = pA$. Il reste à montrer que $A = Z_p$.

• Soit $x = \frac{a}{b} \in A$ avec $a \wedge b = 1$. D'après le résultat de la question 1), $\frac{1}{b} \in A$. Si p divise b, alors $b \in I$, c'est-à-dire que b n'est pas inversible dans A, ce qui contredit la phrase précédente. Donc p ne divise pas b ; comme il est premier, il est premier avec b. Par définition, $x \in Z_p$. On a montré que $A \subset Z_p$.

• Réciproquement, soit $x \in Z_p$. Il vient $x = \frac{a}{b}$ avec $p \wedge b = 1$. Supposons que $x \notin A$. Alors $x \neq 0$ et $\frac{1}{x} = \frac{b}{a} \in A$. Comme $\frac{1}{x}$ n'est pas inversible dans A, $\frac{1}{x} \in I = pA$. Il existe $\frac{c}{d} \in A$ avec $c \wedge d = 1$ tel que $\frac{b}{a} = p\frac{c}{d}$. On a $bd = pac$, donc p divise bd ; étant premier avec b, il divise d. Cela signifie que d n'est pas inversible dans A : $\frac{1}{d} \notin A$. Or $\frac{c}{d} \in A$, en contradiction avec le résultat de la question 1). Donc $x \in A$. On a montré que $Z_p \subset A$ et finalement $A = Z_p$.

SUJET VII

1) A est un anneau intègre, donc commutatif. Soit x un élément non nul de A. L'application f de A dans A : $y \mapsto xy$ est linéaire. Comme A est intègre, $\operatorname{Ker} f = \{0\}$: f est injective et comme A est de dimension finie, elle est surjective. Il existe donc un élément y de A tel que $xy = 1_A$, c'est-à-dire que x est inversible. A est un corps.

2) Soit $x \in A$ et $I_x = \{P \in \mathbb{R}[X],\ P(x) = 0\}$. I_x est un idéal de $\mathbb{R}[X]$. Si $n = \dim(A)$, la famille $(1_A, x, x^2, \dots, x^n)$ est liée, il existe donc un $(n+1)$-uplet non nul de réels $(\alpha_0, \dots, \alpha_n)$ tel que $\sum_{k=0}^{n} \alpha_k x^k = 0$, autrement dit un polynôme P non nul tel que $P(x) = 0$. Donc $I_x \neq \{0\}$. L'anneau $\mathbb{R}[X]$ étant principal, I_x est engendré par un polynôme unitaire P_0. Supposons qu'il existe des polynômes non constants Q_0 et R_0 tels que $P_0 = Q_0 R_0$. On a alors $P_0(x) = Q_0(x)R_0(x) = 0$ donc, comme A est intègre, $Q_0(x) = 0$ ou $R_0(x) = 0$, ce qui contredit la définition de P_0. Ainsi, le polynôme P_0 est irréductible dans $\mathbb{R}[X]$: il est de degré inférieur ou égal à 2. S'il est de degré 1, x est réel; on peut choisir $\alpha = 0$ et $\beta = x^2$. S'il est de degré 2, il existe $(\alpha, \beta) \in \mathbb{R}^2$ tel que $P_0 = X^2 - \alpha X - \beta$, d'où $x^2 - \alpha x - \beta = 0$.

3) Démontrons la contraposée de l'implication demandée, c'est-à-dire : $(x \notin \mathbb{R}) \Rightarrow (x^2 \notin \mathbb{R}_+)$.
Soit $x \in A$ tel que $x \notin \mathbb{R}$. Le polynôme $X^2 - \alpha X - \beta$ étant irréductible sur $\mathbb{R}$, son discriminant $\Delta = \alpha^2 + 4\beta$ est strictement négatif, d'où $\beta < 0$. Si $x^2 \in \mathbb{R}_+$, $\alpha x = x^2 - \beta \in \mathbb{R}_+^*$, donc $\alpha \neq 0$ et $x = \frac{1}{\alpha}(x^2 - \beta)$ est réel, en contradiction avec l'hypothèse. On a montré que $(x \notin \mathbb{R})$ implique $(x^2 \notin \mathbb{R}_+)$, soit, en contraposant, que $(x^2 \in \mathbb{R}_+)$ implique $(x \in \mathbb{R})$.

4) Pour tout $x \in A$ et $\xi \in \mathbb{R}$:

$$(x - \xi)^2 = x^2 - 2\xi x + \xi^2 = \alpha x + \beta - 2\xi x + \xi^2 = (\alpha - 2\xi)x + \beta + \xi^2.$$

Supposons que $x - \xi \in V$, c'est-à-dire $(x - \xi)^2 = \gamma \in \mathbb{R}_-$, d'où $(\alpha - 2\xi)x = \gamma - \beta - \xi^2 \in \mathbb{R}$.
Si $\alpha - 2\xi \neq 0$, alors $x = \dfrac{\gamma - \beta - \xi^2}{\alpha - 2\xi}$, qui est réel. Alors $(x - \xi)^2 \in \mathbb{R}_-$ n'est possible que si $x = \xi$.
Dans tous les cas, il n'existe donc qu'une seule valeur possible de ξ pour laquelle $x - \xi \in V$: $\xi = x$ si x est réel; $\xi = \frac{\alpha}{2}$ sinon.
Réciproquement, ces valeurs conviennent : si $x \in \mathbb{R}$, $(x - x)^2 = 0 \in \mathbb{R}_-$ et si $x \notin \mathbb{R}$:

$$(x - \frac{\alpha}{2})^2 = x^2 - \alpha x + \frac{\alpha^2}{4} = \beta + \frac{\alpha^2}{4} = \frac{\Delta}{4} \in \mathbb{R}_-.$$

5) Soit $(x, y) \in V^2$ et $(\alpha, \beta) \in \mathbb{R}^2$. Supposons que $\alpha x + \beta y = \gamma \in \mathbb{R}$. Alors :

$$\begin{cases} \alpha x^2 + \beta x y = \gamma x \\ \alpha x y + \beta y^2 = \gamma y \end{cases} \quad \text{d'où :} \quad \begin{cases} \alpha^2 x^2 + \alpha\beta x y = \alpha\gamma x \\ \alpha\beta x y + \beta^2 y^2 = \beta\gamma y \end{cases}.$$

En retranchant membre à membre : $\alpha^2 x^2 - \beta^2 y^2 = \gamma(\alpha x - \beta y)$.

Supposons $\gamma \neq 0$.
Comme $\alpha^2 x^2 - \beta^2 y^2$ est réel, $\alpha x - \beta y = \dfrac{\alpha^2 x^2 - \beta^2 y^2}{\gamma} = \delta \in \mathbb{R}$.
N'oublions pas que $\alpha x + \beta y = \gamma$. Par addition, il en résulte $2\alpha x = \gamma + \delta \in \mathbb{R}$. Puis si $\alpha \neq 0$, on obtient $x \in \mathbb{R}$.
Mais $x \in V$ donc $x^2 \in \mathbb{R}_-$, d'où $x = 0$.
De même, par soustraction, il vient $2\beta y = \gamma - \delta \in \mathbb{R}$. Puis si $\beta \neq 0$, on obtient $y \in \mathbb{R}$, d'où comme auparavant $y = 0$.
Mais $x = y = 0$ implique $\gamma = 0$, en contradiction avec l'hypothèse.
En définitive, $\gamma = \alpha x + \beta y = 0$.

6) Tout d'abord $0 \in V$, donc $V \neq \varnothing$. Montrons maintenant que V est stable par combinaison linéaire. Soit $(x, y) \in V^2$, $(\alpha, \beta) \in \mathbb{R}^2$.

$$(\alpha x + \beta y)^2 = \alpha^2 x^2 + 2\alpha\beta x y + \beta^2 y^2.$$

On sait que $\alpha^2 x^2$ et $\beta^2 y^2$ sont réels. De plus : $(2\alpha\beta x y)^2 = 4\alpha^2\beta^2 x^2 y^2$, qui est réel positif. On en déduit d'après le résultat de la question 2) que $2\alpha\beta x y$ est réel. Ainsi $(\alpha x + \beta y)^2$ est réel. Deux cas se présentent :
- $(\alpha x + \beta y)^2 \in \mathbb{R}_+$: d'après le résultat de la question 2), $\alpha x + \beta y \in \mathbb{R}$ et d'après celui de la question 4), $\alpha x + \beta y = 0$, qui est bien élément de V ;
- $(\alpha x + \beta y)^2 \in \mathbb{R}_-$, ce qui signifie précisément que $\alpha x + \beta y$ est élément de V.

Dans les deux cas, $\alpha x + \beta y \in V$. Ainsi V est stable par combinaison linéaire.
On a bien montré que V est un sous-espace vectoriel de A.

CORRIGÉS

Le résultat de la question 3) prouve que pour tout $x \in A$, il existe un unique réel ξ tel que $x - \xi = v \in V$, c'est-à-dire $x = \xi + v$, donc $A = \mathbb{R} \oplus V$. D'ailleurs, il est évident que $\mathbb{R} \cap V = \{0\}$.

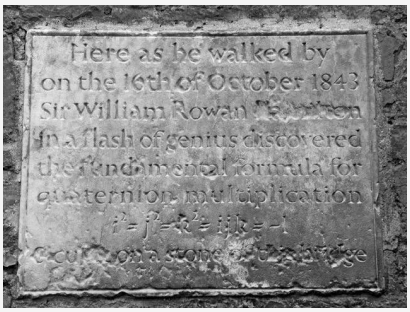
7) Soit $x \in V \backslash \{0\}$. On a $x^2 = \beta$, avec $\beta \in \mathbb{R}_-^*$. Alors $\left(\frac{x}{\sqrt{-\beta}}\right)^2 = -1$. Il existe bien dans V des éléments de carré (-1).
Pour tout $x \in V$, $x^2 = \beta = -\beta v^2$, avec $\beta \in \mathbb{R}_-$. D'où $(x - \sqrt{-\beta}\, v)(x + \sqrt{-\beta}\, v) = 0$ (grâce à la commutativité de A, voir remarque *in fine*) et, comme A est intègre, $x = \sqrt{-\beta}\, v$ ou $x = -\sqrt{-\beta}\, v$. Dans les deux cas, $x \in \mathrm{Vect}(v)$. Donc l'espace vectoriel V est de dimension 1, engendré par v. Comme $A = \mathbb{R} \oplus V$, $\dim(A) = 2$.

8) Si $V = \{0\}$, alors $A = \mathbb{R}$. Si $V \neq \{0\}$, considérons l'application φ de $\mathbb{C}$ dans A définie par $\varphi(z) = \mathfrak{Re}(z) + \mathfrak{Im}(z)v$. Il est clair que φ est un morphisme de $\mathbb{C}$ dans A. Soit $z = a + ib \in \mathrm{Ker}\,\varphi$, avec $(a, b) \in \mathbb{R}^2$. $\varphi(z) = a + bv = 0$. Comme $A = \mathbb{R} \oplus V$, $a = b = 0$, donc $z = 0$. $\mathrm{Ker}\,\varphi = \{0\}$, donc φ est injective. Comme $\dim_{\mathbb{R}}(\mathbb{C}) = \dim(A) = 2$, φ est surjective. C'est un isomorphisme de $\mathbb{C}$ dans A.
Conclusion : toute $\mathbb{R}$-algèbre de dimension finie unitaire et intègre (donc commutative) est isomorphe à $\mathbb{R}$ ou $\mathbb{C}$.

Remarque : si l'on n'impose plus à A d'être commutative, tout en excluant les diviseurs de zéro, le résultat ne s'applique plus. Par exemple, le corps gauche des quaternions est une $\mathbb{R}$-algèbre de dimension 4, unitaire et sans diviseurs de zéro, qui n'est bien sûr isomorphe ni à $\mathbb{R}$ ni à $\mathbb{C}$. Le fait de devoir abandonner la commutativité pour créer une telle algèbre de dimension strictement supérieure à 2 est la grande découverte du mathématicien irlandais Sir William Rowan Hamilton en 1843. Il imagina 3 éléments linéairement indépendants de V vérifiant :

$$i^2 = j^2 = k^2 = ijk = -1;$$
$$ij = -ji = k;\ jk = -kj = i;\ ki = -ik = j.$$

Excité par l'émergence brutale de cette idée alors qu'il longeait le Royal Canal à Dublin, il grava ces formules sur une pierre du pont de Brougham. Cette gravure, disparue depuis, a été remplacée par une plaque commémorative.



SUJET VIII

1) D'après la relation coefficients-racines, on sait que $|a_k|$ est égal à la somme des produits $\lambda_{i_1} \cdots \lambda_{i_p}$, où $p = n - k$. Il y a $\binom{n}{k}$ tels termes, chacun inférieur à $M(P)$. D'où le résultat.

2) $L(P)^2 = \sum_{k=0}^{n} |a_k|^2 \leqslant M(P)^2 \sum_{k=0}^{n} \binom{n}{k}^2 \leqslant M(P)^2 \left(\sum_{k=0}^{n} \binom{n}{k}\right)^2 = M(P)^2 2^{2n}$, d'où la formule.

3)
$$\int_0^{2\pi} |P(\mathrm{e}^{i\theta})|^2 \mathrm{d}\theta = \int_0^{2\pi} \sum_{k=0}^{n} a_k \mathrm{e}^{ik\theta} \sum_{\ell=0}^{n} \overline{a_\ell} \mathrm{e}^{-i\ell\theta}\, \mathrm{d}\theta$$
$$= \int_0^{2\pi} \sum_{k,\ell=0}^{n} a_k \overline{a_\ell} \mathrm{e}^{i(k-\ell)\theta} \mathrm{d}\theta = \sum_{k=0}^{n} |a_k|^2 \int_0^{2\pi} \mathrm{d}\theta = 2\pi L(P)^2.$$

4) $L(P)^2 = L\big((X - \lambda)Q\big)^2 = \frac{1}{2\pi} \int_0^{2\pi} \left|\mathrm{e}^{i\theta} - \lambda\right|^2 \left|Q(\mathrm{e}^{i\theta})\right|^2 \mathrm{d}\theta$. Or :
$$\left|\mathrm{e}^{i\theta} - \lambda\right| = \left|1 - \lambda \mathrm{e}^{-i\theta}\right| = \left|\overline{\lambda} \mathrm{e}^{i\theta} - 1\right|.$$
Désignons par $(\lambda_1, \ldots, \lambda_p)$ les racines de P de module strictement supérieur à 1 et $(\lambda_{p+1}, \ldots, \lambda_n)$ celles dont le module est inférieur ou égal à 1. En itérant le calcul précédent, on obtient :
$$L(P) = L\big((\overline{\lambda_1} X - 1) \cdots (\overline{\lambda_p} X - 1)(X - \lambda_{p+1}) \cdots (X - \lambda_n)\big).$$

5) Le coefficient dominant de ce nouveau polynôme a pour module $M(p)$. Donc $L(P) \geqslant M(P)$.

SUJET IX

Partie A : Anneaux $\mathbb{Z}[\sqrt{n}]$

1) L'application de $\mathbb{Z}^2$ dans $\mathbb{Z}[\sqrt{n}]$: $(a,b) \mapsto a + b\sqrt{n}$ est surjective par définition. Elle est injective parce que $\sqrt{n} \notin \mathbb{Q}$.
2) $\mathbb{Z}[\sqrt{n}]$ contient le réel 1 ; il est stable par soustraction et multiplication : c'est un sous-anneau de $\mathbb{R}$. Tout sous-anneau d'un corps commutatif est intègre.
3) $\varphi(1) = 1$; si $(x,y) \in \mathbb{Z}[i]$ alors $\varphi(x-y) = \varphi(x) - \varphi(y)$ et $\varphi(xy) = \varphi(x)\varphi(y)$: c'est un morphisme d'anneaux. Il est clairement bijectif et égal à sa bijection réciproque : c'est un automorphisme involutif de $\mathbb{Z}[\sqrt{n}]$.
4) a) Pour tout $x \in \mathbb{Z}[i]$, $x\varphi(x) = 0 \Rightarrow x = 0$ ou $\varphi(x) = 0$, ce qui revient à $x = 0$.
b) $N(xy) = xy\varphi(xy) = x\varphi(x)y\varphi(y) = N(x)N(y)$.
5) A-5. Soit x un élément inversible de $\mathbb{Z}[\sqrt{n}]$: $xx^{-1} = 1$, d'où $N(x)N(x^{-1}) = 1$; $N(x)$ est un élément inversible de l'anneau $\mathbb{Z}$: $N(x) = \pm 1$. Réciproquement, si $N(x) = 1$ alors $x\varphi(x) = 1$, donc x est inversible et $x^{-1} = \varphi(x)$; de même, si $N(x) = -1$, alors $x^{-1} = -\varphi(x)$.

Partie B : Étude de l'anneau $\mathbb{Z}[\sqrt{5}]$

1) D'après la question précédente, $x = a + b\sqrt{5}$ est inversible dans $\mathbb{Z}[\sqrt{5}]$ si et seulement si $N(x) = a^2 - 5b^2 = \pm 1$. Par exemple : 1, -1, $2+\sqrt{5}$, $2-\sqrt{5}$, $9+4\sqrt{5}$, $9-4\sqrt{5}$ sont inversibles.
On remarque que, pour tout $n \in \mathbb{N}$, $N((2+\sqrt{5})^n) = N(2+\sqrt{5})^n = (-1)^n$; ainsi $(2+\sqrt{5})^n$ est inversible. Or $2+\sqrt{5} > 1$, donc la suite de ses puissances est strictement croissante : elle prend une infinité de valeurs. Par exemple :

$$(2+\sqrt{5})^2 = 9+4\sqrt{5}\,; \quad (2+\sqrt{5})^3 = 38+17\sqrt{5}\,; \quad (2+\sqrt{5})^4 = 161+72\sqrt{5} \quad \cdots$$

2) a) Un carré d'entier est toujours congru à 0 ou 1 modulo 4. Par conséquent $c^2 - 5d^2$ est congru à 0, 1 ou 3 modulo 4 ; jamais à 2. Donc $c^2 - 5d^2 \neq \pm 2$.
b) Si $xy = 2$, $N(x)N(y) = 4$. Comme il est impossible d'avoir $N(x) = \pm 2$, on a nécessairement $N(x) = \pm 1$ ou $N(y) = \pm 1$, c'est-à-dire x ou y inversible. Donc 2 est irréductible dans $\mathbb{Z}[\sqrt{5}]$.
3) I contient 0 et il est stable par soustraction : c'est un sous-groupe de $(\mathbb{Z}[\sqrt{5}], +)$.
Soit $x = a + b\sqrt{5}$ un élément de I (les entiers a et b sont de même parité, c'est-à-dire $a - b \equiv 0\,[2]$) et $y = c + d\sqrt{5}$ un élément quelconque de $\mathbb{Z}[\sqrt{5}]$.

$$xy = (a+b\sqrt{5})(c+d\sqrt{5}) = ac + 5bd + (ad+bc)\sqrt{5},$$

$$(ac+5bd) - (ad+bc) \equiv ac + bd - ad - bc \equiv (a-b)(c-d) \equiv 0\,[2],$$

donc $ac + 5bd$ et $ad + bc$ sont de même parité : $xy \in I$. I est bien un idéal de $\mathbb{Z}[\sqrt{5}]$.
4) Les éléments 2 et $1+\sqrt{5}$ appartiennent à l'idéal I. Supposons que I soit engendré par un élément x : il existe des éléments y et z de $\mathbb{Z}[\sqrt{5}]$ tels que $2 = xy$ et $1+\sqrt{5} = xz$. Comme 2 est irréductible :
- Ou bien x est inversible, ce qui implique $I = \mathbb{Z}[\sqrt{5}]$; c'est absurde.
- Ou bien y est inversible ; alors, $x = 2y^{-1}$ et $2y^{-1}z = 1+\sqrt{5}$. En posant $y^{-1}z = a + ib$, on arrive également à une absurdité.

Donc l'idéal I n'est pas engendré par un seul élément ; l'anneau $\mathbb{Z}[\sqrt{5}]$ n'est pas principal.

Partie C : Anneau des entiers de Gauss

1) On vérifie facilement que :
a) Le nombre complexe 1 est élément de $\mathbb{Z}[i]$.
b) $\mathbb{Z}[i]$ est stable par soustraction : $\forall (u,v) \in \mathbb{Z}[i]^2, \quad u - v \in \mathbb{Z}[i]$.
c) $\mathbb{Z}[i]$ est stable par multiplication : $\forall (u,v) \in \mathbb{Z}[i]^2, \quad uv \in \mathbb{Z}[i]$.
$\mathbb{Z}[i]$ est donc un sous-anneau de $\mathbb{C}$.
Comme $\mathbb{Z}[i]$ est un sous-anneau d'un corps commutatif, il est intègre.
L'élément 2, non nul, n'est pas inversible dans $\mathbb{Z}[i]$: $\mathbb{Z}[i]$ n'est pas un corps.

2) a) Si $u = a + ib$, avec $(a, b) \in \mathbb{Z}^2$, alors $|u|^2 = a^2 + b^2 \in \mathbb{N}$.
b) Si u est inversible dans $\mathbb{Z}[i]$, alors il existe $u' \in \mathbb{Z}[i]$ tel que $uu' = 1$; on en déduit $|u|^2|u'|^2 = 1$: $|u|^2$ est inversible dans $\mathbb{N}$ et donc égal à 1.
Réciproquement, si $|u| = 1$, alors $u\overline{u} = 1$. Or $\overline{u} \in \mathbb{Z}[i]$, donc u est inversible dans $\mathbb{Z}[i]$ et son inverse est $\overline{u}$.
c) L'ensemble des éléments inversibles de $\mathbb{Z}[i]$ est l'ensemble des éléments de $\mathbb{Z}[i]$ de module 1, c'est-à-dire $\{1, i, -1, -i\}$. On reconnaît le groupe $\mathscr{U}_4$ des racines quatrièmes de l'unité.
3) a) Si $v = uw$, alors $|v|^2 = |u|^2|w|^2$: $|u|^2$ divise $|v|^2$ dans $\mathbb{N}$.
b) On remarque que $4 + 7i = (2 + i)(3 + 2i)$, donc $2 + i$ divise $4 + 7i$. Mais l'équation $4 + 7i = (2 - i)(a + ib)$ n'a pas de solutions entières, donc $2 - i$ ne divise pas $4 + 7i$; pourtant, $|2 - i|^2 = 5$ divise $|4 + 7i|^2 = 65$: la réciproque de la question a) est fausse.
c) Pour tout $u \in \mathbb{Z}[i]$, u divise u ; la relation est réflexive.
Si u divise v et v divise u, alors v divise u et u divise v ; la relation est symétrique.
Si u divise v, v divise u, v divise w et w divise v, alors u divise w et w divise u ; la relation est transitive.
C'est une relation d'équivalence. La classe d'équivalence de u est l'ensemble des éléments v de $\mathbb{Z}[i]$ tels qu'il existe w et w' de $\mathbb{Z}[i]$ vérifiant : $v = uw$ et $u = vw'$. On en déduit $u = uww'$, d'où $u = 0$, ou $ww' = 1$, c'est-à-dire w inversible.
La classe d'équivalence de 0 est $\{0\}$. Si $u \neq 0$, la classe d'équivalence de u est $\{u, iu, -u, -iu\}$, c'est-à-dire $\{a + ib, -b + ia, -a - ib, b - ia\}$.
4) a) Soit $z = x + iy$ un complexe, avec x et y réels. Soit a l'entier le plus proche de x (suivant les cas, c'est $E(x)$ ou $E(x) + 1$) ; on a $|x - a| \leqslant \frac{1}{2}$.
De même, si b est l'entier le plus proche de y : $|y - b| \leqslant \frac{1}{2}$.
D'où, en posant $u = a + ib$: $|z - u|^2 = (x - a)^2 + (y - b)^2 \leqslant \frac{1}{2}$ et donc $|z - u| < 1$.
b) Appliquons ce résultat au nombre complexe $z = \frac{u}{v}$: il existe $q \in \mathbb{Z}[i]$ tel que : $\left|\frac{u}{v} - q\right| < 1$, c'est-à-dire $|u - vq| < |v|$. En posant $r = u - vq$, on a bien :

$$\begin{cases} u = vq + r \\ |r| < |v| \end{cases}.$$

c) Contrairement à la division euclidienne dans $\mathbb{Z}$, ici le couple (q, r) n'est pas nécessairement unique.
Pour $u = 1 - i$ et $v = 2i$: $\frac{u}{v} = -\frac{1}{2} - \frac{i}{2}$; il y a quatre éléments de $\mathbb{Z}[i]$ dont la distance à ce nombre complexe est strictement inférieure à 1 :

$$q_1 = 0 \quad ; \quad q_2 = -1 \quad ; \quad q_3 = -1 - i \quad ; \quad q_4 = -i,$$

d'où quatre couples (q, r) répondant à la question :

$$(0, 1 - i) \quad ; \quad (-1, 1 + i) \quad ; \quad (-1 - i, -1 + i) \quad ; \quad (-i, -1 - i).$$

5) Soit I un idéal de $\mathbb{Z}[i]$. Si $I = \{0\}$, il est engendré par 0, donc principal.
Si $I \neq \{0\}$, l'ensemble des carrés des modules des éléments non nuls de I est une partie non vide de $\mathbb{N}$, qui admet donc un plus petit élément n_0. Soit u_0 un élément de I tel que $|u_0|^2 = n_0$. Comme $u_0 \in I$, l'idéal $u_0\mathbb{Z}[i]$ engendré par u_0 est inclus dans I. Réciproquement, soit u un élément quelconque de I. D'après la question précédente il existe $(q, r) \in \mathbb{Z}[i]^2$ tel que $u = u_0q + r$ avec $|r| < |u_0|$, c'est-à-dire $|r|^2 < n_0$. Comme I est un idéal de $\mathbb{Z}[i]$, $u_0q \in I$, et $r = u - u_0q \in I$.
On en déduit que r est un élément de I dont le carré du module est strictement inférieur au plus petit carré des modules des éléments *non nuls* de I ; il est donc nul : $r = 0$, d'où $u = u_0q$ et, par conséquent, $I \subset u_0\mathbb{Z}[i]$. En définitive, $I = u_0\mathbb{Z}[i]$: tout idéal de $\mathbb{Z}[i]$ est principal ; $\mathbb{Z}[i]$ est un anneau principal.
N.B. C'est l'existence d'une division euclidienne dans $\mathbb{Z}$, $\mathbb{K}[X]$ ou $\mathbb{Z}[i]$ qui permet de démontrer que ces anneaux sont principaux. Un anneau intègre dans lequel existe une division euclidienne est dit euclidien. Tout anneau euclidien est principal.

6) a) Soit u un élément de $\mathbb{Z}[i]$ tel que $|u|^2$ soit premier dans $\mathbb{N}$. Supposons que u ne soit pas premier dans $\mathbb{Z}[i]$, c'est-à-dire qu'il existe deux éléments v et w de $\mathbb{Z}[i]$, non inversibles, tels que $u = v\,w$. On a alors : $|u|^2 = |v|^2\,|w|^2$ avec $|v|^2 \neq 1$ et $|w|^2 \neq 1$, ce qui contredit le fait que $|u|^2$ est premier. Donc u est premier dans $\mathbb{Z}[i]$.
b) $2 = (1+i)(1-i)$: 2 n'est pas premier dans $\mathbb{Z}[i]$.
Supposons qu'il existe deux éléments v et w de $\mathbb{Z}[i]$, non inversibles, tels que $v\,w = 3$. On en déduit $|v|^2\,|w|^2 = 9$, avec $|v|^2 \neq 1$ et $|w|^2 \neq 1$. La seule solution est $|v|^2 = |w|^2 = 3$. Si $v = a + i\,b$, $a^2 + b^2 = 3$. Cette égalité est impossible avec a et b entiers. Donc 3 est premier dans $\mathbb{Z}[i]$. Pourtant, $|3|^2 = 9$ n'est pas premier dans $\mathbb{N}$: la réciproque de la question a) est fausse.
c) Soit $u = a + i\,b$ un élément premier de $\mathbb{Z}[i]$, où a et b sont des entiers non nuls. Supposons que $|u|^2 = a^2 + b^2$ ne soit pas premier dans $\mathbb{N}$, c'est-à-dire qu'il existe des entiers c et d strictement supérieurs à 1 tels que $a^2 + b^2 = c\,d$. On a alors $(a+i\,b)(a-i\,b) = c\,d$. Comme $a+i\,b$ est premier, et que c n'en est pas un multiple, c est premier avec $a+i\,b$; de même, c est premier avec $a-i\,b$, donc avec le produit $(a+i\,b)(a-i\,b)$; comme il divise ce produit, c est inversible, ce qui contredit l'hypothèse $c > 1$. Donc $|u|^2$ est premier dans $\mathbb{N}$.
d) Soit a^2+b^2 la somme de deux carrés d'entiers naturels. Si a et b sont de même parité, a^2+b^2 est pair, donc non congru à 3 modulo 4. Supposons donc a pair et b impair. Ainsi $a^2 \equiv 0\ [4]$ et $b^2 \equiv 1\ [4]$, donc $a^2 + b^2 \equiv 1\ [4]$. En définitive, $a^2 + b^2$ n'est jamais congru à 3 modulo 4.
Soit p un entier premier congru à 3 modulo 4. Supposons p non premier dans $\mathbb{Z}[i]$, c'est-à-dire qu'il existe deux éléments v et w de $\mathbb{Z}[i]$, non inversibles, tels que $v\,w = p$. On a alors $|v|^2\,|w|^2 = p^2$, avec $|v|^2 \neq 1$ et $|w|^2 \neq 1$. Comme p est premier, la seule solution est $|v|^2 = |w|^2 = p$; soit, en posant $v = a+i\,b$: $a^2+b^2 = p$, ce qui est impossible d'après la question précédente. Donc p est premier dans $\mathbb{Z}[i]$.
e) Soit p un entier premier congru à 1 modulo 4. En admettant qu'il est somme de deux carrés : $p = a^2 + b^2 = (a+i\,b)(a-i\,b)$. Si l'on suppose p premier dans $\mathbb{Z}[i]$, cette égalité implique que $a + i\,b$ est inversible ou associé à p, donc $a = 0$ ou $b = 0$; ceci est impossible, car p n'est pas un carré d'entier. Par conséquent, p n'est pas premier dans $\mathbb{Z}[i]$.
f) Un élément de $\mathbb{Z}[i]$ réel ou imaginaire pur est associé à un entier naturel. Un entier naturel non premier dans $\mathbb{N}$ ne peut pas être premier dans $\mathbb{Z}[i]$. Restent les nombres premiers de $\mathbb{N}$: le seul qui soit pair est 2 et il n'est pas premier dans $\mathbb{Z}[i]$; les nombres premiers impairs sont congrus à 1 (non premiers dans $\mathbb{Z}[i]$) ou à 3 (premiers dans $\mathbb{Z}[i]$) modulo 4.
Pour résumer, les éléments premiers de $\mathbb{Z}[i]$ sont :
- les éléments de la forme $a + i\,b$ avec a et b entiers non nuls et $a^2 + b^2$ premier dans $\mathbb{N}$;
- les entiers premiers congrus à 3 modulo 4 et leurs associés : $p, i\,p, -p, -i\,p$.

CHAPITRE 3

Compléments d'algèbre linéaire

Plan du chapitre

Cours, p. 80 ☐
- **1** ▶ Somme, somme directe d'une famille finie de sous-espaces vectoriels, p. 80 ☐
- **2** ▶ Calcul matriciel par blocs, p. 84 ☐
- **3** ▶ Stabilité par un endomorphisme, p. 86 ☐
- **4** ▶ Éléments propres d'un endomorphisme ou d'une matrice carrée, p. 88 ☐
- **5** ▶ Éléments propres en dimension finie, p. 90 ☐

Fiche synthèse, p. 96 ☐
Méthodes pas à pas, p. 98 ☐
Exercices, p. 99 ☐
Corrigés, p. 104 ☐

Objectifs et compétences du programme

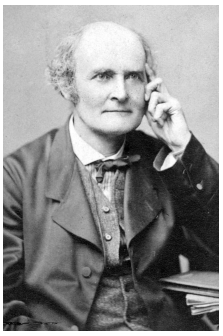
Capacités principales à maîtriser	Méthodes associées	Exercices associés
Montrer qu'un sous-espace est stable par un endomorphisme.	Méthode 1	Exercices 1, 2, 6, B
Déterminer les valeurs propres d'un endomorphisme ou d'une matrice carrée.	Méthode 2	Exercices 3, 5, D, F
Déterminer les vecteurs propres d'un endomorphisme ou d'une matrice carrée.	Méthode 3	Exercices 4, A, E

RETROUVEZ ICI LES FLASHCARDS INTERACTIVES POUR SE TESTER

www.lienmini.fr/212891-FLASH-03

COURS

Histoire des mathématiques



Arthur Cayley, mathématicien anglais (1821-1895)
Brillant étudiant en sciences au Trinity Collège de Cambridge, Arthur Cayley est contraint par son père d'abandonner les mathématiques pour devenir avocat. Il exerce ce métier pendant quatorze ans, tout en consacrant ses temps libres à sa passion : il publie dans cette période plus de 200 articles dans le *Cambridge mathematical Journal*. En 1863, il obtient enfin une chaire de mathématiques à l'Université de Cambridge, poste qu'il occupera jusqu'à sa mort.
Il énonce en 1850 la définition générale d'un groupe, qu'il représente à l'aide d'un graphe désormais appelé « graphe de Cayley ». On lui doit, avec son ami James Sylvester (1814-1897), les notions de matrice et de déterminant. Il énonce en 1857 le théorème dont il partage la paternité avec William Hamilton, qui l'avait démontré en dimension 4 et utilisé pour sa théorie des quaternions, mais c'est Georg Frobenius qui en apporte en 1872 la preuve en dimension quelconque.

Dans tout ce chapitre, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, le plus souvent $\mathbb{R}$ ou $\mathbb{C}$.

1 Somme, somme directe d'une famille finie de sous-espaces vectoriels

1.1. Somme de p sous-espaces vectoriels

Étendons au cas de p sous-espaces vectoriels ($p \in \mathbb{N}^*$) la définition de la somme, vue en première année, de deux sous-espaces vectoriels.

Définition 3.1. Somme de sous-espaces vectoriels

Soit E un $\mathbb{K}$-espace vectoriel et $(F_1, \dots, F_p)$ une famille de p sous-espaces vectoriels de E. On appelle somme de cette famille l'ensemble des combinaisons linéaires d'éléments des sous-espaces F_i, pour $i \in [\![1, p]\!]$. Chacun de ces sous-espaces étant stable par combinaisons linéaires, on peut écrire un élément de cette somme comme une somme d'éléments appartenant à chacun des F_i :

$$\sum_{i=1}^{p} F_i = \left\{x \in E\,, \quad \exists (x_1, \dots, x_p) \in F_1 \times \cdots \times F_p\,, \quad x = x_1 + \cdots + x_p\right\}.$$

Remarques

- La somme de la famille $(F_1, \dots, F_p)$ est le plus petit sous-espace vectoriel de E contenant tous les sous-espaces de cette famille (ou, de façon équivalente, la réunion de cette famille).
- Pour $p = 1$, la somme de la famille (F_1) est évidemment le sous-espace F_1.

PRÉPAS SCIENTIFIQUES

MP/MP*
MPI/MPI*

CONFORME AU NOUVEAU PROGRAMME

Maths

L'ouvrage indispensable pour réussir et faire la différence aux concours

➜ TOUT LE COURS

Pour maîtriser **l'intégralité du programme** :

- toutes les définitions, propositions et démonstrations à retenir
- plus de 1 000 démonstrations et exemples concrets à connaître

➜ LA SYNTHÈSE DES NOTIONS

Pour retenir **l'essentiel du cours** avant les DS, les colles et dans la perspective des concours

➜ LES MÉTHODES PAS À PAS

Pour acquérir **les techniques et astuces** de résolution des exercices

➜ ENTRAÎNEMENT PROGRESSIF

Pour **vous préparer efficacement** et **vous tester** avec plus de 500 exercices de difficulté progressive : application, approfondissement et sujets de concours

➜ TOUS LES CORRIGÉS DÉTAILLÉS

Pour **comprendre** les étapes de résolution et **acquérir** les bons reflexes

OFFERT EN LIGNE

+ Plus de **160 flashcards interactives** pour mémoriser autrement
+ **16 synthèses à télécharger** pour des révisions nomades
+ Tous les **scripts Python interactifs** pour s'entraîner à coder

Des auteurs au cœur de l'enseignement et des attentes des élèves en CPGE

Dans la même collection :

Retrouvez notre collection complète ici :

ISBN : 978-2-311-21289-1