# Guide de rédaction mathématique rigoureuse

Pour étudiants du premier cycle universitaire

Yassine Ait Mohamed

**Résumé**

Ce guide présente les principes fondamentaux de la rédaction mathématique rigoureuse à l'intention des étudiants du premier cycle universitaire. Il développe une méthodologie structurée pour communiquer clairement des raisonnements mathématiques, en mettant l'accent sur l'utilisation correcte des symboles logiques, la structure des démonstrations et les conventions de notation établies.

## Introduction

La rédaction mathématique a pour but de faire comprendre clairement au lecteur un raisonnement, une démonstration ou la résolution d'un problème. Bien rédiger peut signifier deux choses : d'une part, exposer sa pensée avec ordre et rigueur, et si possible avec style ; d'autre part, se conformer aux conventions de notation pratiquées par la communauté mathématique.

Un raisonnement faux mais bien rédigé permet généralement de trouver facilement l'erreur commise. Au contraire, un raisonnement correct mais mal rédigé est souvent le signe d'une compréhension fragile, voire d'une arnaque involontaire. Une copie mal rédigée induit parfois chez le lecteur le sentiment troublant de ne pas être lui-même à la hauteur en mathématiques. Par contre, lorsque la rédaction est précise et rigoureuse, le lecteur trouve que la question n'était finalement pas si compliquée. Ne dit-on pas que le génie est la capacité de rendre simple ce qui est compliqué ?

La rédaction est toujours un compromis, car une épreuve de mathématique a une durée limitée et toutes choses n'ont pas nécessité à être détaillées dans les moindres détails. Il s'agit la plupart du temps de mettre en évidence un passage particulier, particulièrement important, de la résolution de la question. Une démonstration est comme une plaidoirie d'avocat : il faut argumenter, apporter les preuves et ménager ses effets pour mettre en évidence la vérité. En général, la résolution d'une question peut être séparée en deux parties : une suite de calculs et l'utilisation d'un théorème dont on vérifiera scrupuleusement que les hypothèses sont bien vérifiées.

Une suite de calculs sans aucune phrase en français sera indigeste et le lecteur se découragera vite, car aucun lien de raisonnement ne permet de comprendre où mènent ces calculs. Cette rédaction, qui en réalité n'en est pas une, n'aide aucunement le lecteur et donne l'impression que vous ne comprenez pas vraiment ce que vous faites. Inversement, une rédaction minimaliste où le lecteur ne voit que le résultat d'un calcul sans aucun détail lui donnera le sentiment qu'on veut lui faire croire quelque chose sans preuve.

Une bonne rédaction ne s'improvise pas. Elle requiert de la pratique et mêle des automatismes qui ne s'acquièrent que par l'exercice régulier, ainsi que des définitions et théorèmes qu'il faut savoir citer au bon moment et précisément. La critique est aisée et l'art est difficile, mais comme dans la rédaction vous devez être votre propre critique, l'art ne sera finalement que du plaisir.

Un premier test pour évaluer la qualité de votre rédaction consiste à faire lire votre travail par une personne de même niveau que vous. Si cette personne trouve que la question n'était pas si compliquée, votre rédaction est certainement précise et rigoureuse. Si au contraire elle doute de sa propre capacité de compréhension, votre rédaction doit être confuse.

# 1. Schéma général de la rédaction mathématique

Avant d'entrer dans les détails, visualisons la structure globale d'une démonstration mathématique bien construite.

**INTRODUCTION**

**Poser le cadre**

- Introduire tous les objets
- Énoncer les hypothèses
- Rappeler ce qui doit être démontré

*Soit $x \in E$…*
*Supposons que…*
*Montrons que…*

↓

**DÉVELOPPEMENT**

**Construire la preuve**

- Raisonner étape par étape
- Justifier chaque transition
- Utiliser les définitions et théorèmes
- Effectuer les calculs nécessaires

*Par définition…*
*Or nous avons…*
*Donc…*
*En appliquant…*

↓

**CONCLUSION**

**Conclure explicitement**

- Rappeler ce qui a été démontré
- Vérifier que la question est répondue
- Marquer la fin (CQFD, $\square$, etc.)

*Ainsi, nous avons démontré que…*
*Ceci achève la démonstration.*

**À retenir**

Cette structure en trois temps n'est pas une contrainte arbitraire, mais reflète la nature même du raisonnement mathématique. L'introduction garantit que tous les objets manipulés sont bien définis, le développement construit la preuve étape par étape, et la conclusion permet au lecteur de vérifier que la question posée a été résolue.

# 2. Principes approfondis de rédaction mathématique rigoureuse

## 2.1 Clarté et lisibilité

Une rédaction mathématique se doit d'être claire et accessible au lecteur. Pour cela, il importe de :

1. Soigner la présentation en n'hésitant pas à aérer le texte (paragraphes, espaces, formules isolées).
2. Écrire des phrases complètes avec un vocabulaire précis et éviter les abréviations non standards.
3. Utiliser la première personne du pluriel (« nous ») ou la troisième personne du singulier (« on ») pour donner un ton formel et inclusif, tout en restant neutre.
4. Relire soigneusement pour corriger fautes d'orthographe ou coquilles.

### 2.2 Organisation structurée du raisonnement

Un texte mathématique doit suivre un ordre logique perceptible dès la première lecture :

1. Présenter clairement *ce que l'on cherche à démontrer.*
2. Annoncer *les hypothèses* et préparer le terrain (notations, définitions).
3. Décomposer les raisonnements en étapes successives, explicitant les transitions.
4. Introduire des connecteurs logiques variés pour guider la progression (par conséquent, en effet, cependant, d'où, etc.).
5. Terminer par une conclusion qui rappelle et reformule le résultat obtenu.

### 2.3 Justification rigoureuse

Chaque affirmation doit être justifiée soit :

1. Par une définition rappelée, clairement citée.
2. Par un théorème ou une propriété dont les hypothèses sont précisées et vérifiées.
3. Par un calcul ou une construction explicite.

Il est conseillé d'indiquer explicitement les références aux résultats utilisés.

**Exemple 1.** *Montrons que la fonction $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2$ est strictement croissante sur $\mathbb{R}_+$.*

Preuve. *Soient $x, y \in \mathbb{R}_+$ tels que $x < y$. Alors,*

$$f(y) - f(x) = y^2 - x^2 = (y - x)(y + x).$$

*Comme $y - x > 0$ et $y + x > 0$, il en résulte que $f(y) > f(x)$. Donc $f$ est strictement croissante sur $\mathbb{R}_+$.* □

## 3. Originalité et précision dans la rédaction mathématique

La qualité d'une démonstration mathématique ne réside pas uniquement dans sa rigueur logique, mais également dans la clarté et la variété de son expression. Cette section présente des recommandations pour enrichir le style rédactionnel et éviter les formulations stéréotypées qui nuisent à la lisibilité.

### 3.1 Éviter les tournures génériques

La locution impersonnelle « *on a* » constitue l'un des écueils les plus fréquents en rédaction mathématique. Son usage systématique uniformise le style et génère une monotonie préjudiciable à l'engagement du lecteur. Il convient de lui substituer des formulations actives employant un vocabulaire précis et nuancé.

#### 3.1.1 Exemples de reformulations

1. **Calculs élémentaires**
   - × *Formulation à proscrire :* « On a $5^2 \equiv 1 \pmod 3$. »
   - ✓ *Formulation recommandée :* « Un calcul direct établit que $5^2 \equiv 1 \pmod 3$. »
2. **Application de théorèmes**
   - × *Formulation à proscrire :* « Soit $x \in \mathbb{F}_p^\times$ un élément inversible. D'après le théorème de Lagrange, on a $x^{p-1} = 1$. »

- ✓ *Formulation recommandée :* « Soit $x \in \mathbb{F}_p^{\times}$. Le théorème de Lagrange implique directement que $x^{p-1} = 1$. »

3. **Propriétés algébriques**
   - × *Formulation à proscrire :* « On a $(a+b)^2 = a^2 + 2ab + b^2$. »
   - ✓ *Formulation recommandée :* « Le développement du binôme fournit $(a+b)^2 = a^2 + 2ab + b^2$. »
4. **Déductions logiques**
   - × *Formulation à proscrire :* « Puisque $f$ est continue et $K$ est compact, on a que $f(K)$ est compact. »
   - ✓ *Formulation recommandée :* « La continuité de $f$ et la compacité de $K$ garantissent que $f(K)$ est compact. »

## 3.2 Bannir les expressions vagues

Les formules d'évidence telles que « *il est clair que* », « *il est évident que* », ou « *trivialement* » constituent des facilités de langage à éviter absolument. Ces expressions masquent souvent un manque de précision dans l'argumentation et peuvent dérouter le lecteur.

### 3.2.1 Alternatives recommandées

| **Expressions à éviter** | **Formulations préférables** |
|---|---|
| Il est clair que | Il en résulte que |
| Il est évident que | Cela découle directement de |
| Trivialement | Cela se déduit immédiatement de |
| Évidemment | La définition implique que |
| Manifestement | L'hypothèse entraîne que |

**Exemple d'application :**

× « Il est clair que $x^2 \geq 0$ pour tout réel $x$. »

✓ « La définition du carré d'un nombre réel implique que $x^2 \geq 0$. »

## 3.3 Éliminer les redondances

Les expressions tautologiques alourdissent inutilement le discours mathématique et révèlent un manque de concision dans l'argumentation.

### 3.3.1 Expressions redondantes courantes

1. *Il existe un unique élément unique* ⟶ *Il existe un unique élément*
2. *Ceci montre donc* ⟶ *Cela établit que*
3. *Comme on l'a déjà vu précédemment* ⟶ *Comme établi plus haut*
4. *Soit $x$ un élément quelconque arbitraire* ⟶ *Soit $x$ un élément quelconque*
5. *Il s'ensuit par conséquent que* ⟶ *Il s'ensuit que*

## 3.4 Privilégier la voix active

Les constructions passives excessivement longues nuisent à la fluidité du discours. La voix active, plus directe, améliore significativement la lisibilité.

**Exemples de reformulations :**

✗ « Il est démontré que la fonction est continue. »

✓ « Le lemme précédent établit la continuité de la fonction. »

✗ « Il peut être vérifié que la matrice est inversible. »

✓ « Un calcul du déterminant confirme l'inversibilité de la matrice. »

## 3.5 Contextualiser les symboles mathématiques

L'insertion d'expressions symboliques sans explication contextuelle nuit à la compréhension. Chaque relation mathématique doit être intégrée dans une phrase complète qui en explicite le sens.

### 3.5.1 Exemples d'intégration contextuelle

1. **Implications logiques**
   - ✗ « $f(x) = 0 \Longrightarrow g(x) = 1$ »
   - ✓ « Si $f(x) = 0$, alors nécessairement $g(x) = 1$. »
2. **Équivalences**
   - ✗ « $\det(A) \neq 0 \Leftrightarrow A$ inversible »
   - ✓ « La matrice $A$ est inversible si et seulement si son déterminant est non nul. »
3. **Relations d'appartenance**
   - ✗ « $\lambda \in \mathrm{Sp}(A)$ »
   - ✓ « Le scalaire $\lambda$ appartient au spectre de l'opérateur $A$. »
4. **Relations d'inclusion**
   - ✗ « $\ker(f) \subset \mathrm{Im}(g)$ »
   - ✓ « Le noyau de $f$ est inclus dans l'image de $g$. »

## 3.6 Vocabulaire de liaison mathématique

L'emploi d'un vocabulaire varié pour exprimer les relations logiques enrichit considérablement la qualité rédactionnelle. Le tableau suivant propose des alternatives aux connecteurs usuels :

| **Relation logique** | **Expressions variées** |
|---|---|
| Conséquence | implique, entraîne, induit, conduit à, a pour conséquence |
| Justification | découle de, résulte de, provient de, s'appuie sur |
| Équivalence | équivaut à, revient à, est équivalent à, correspond à |
| Conclusion | établit que, démontre que, prouve que, confirme que |
| Généralisation | s'étend à, se généralise en, admet pour extension |

Ces recommandations stylistiques, appliquées de manière cohérente, transforment une démonstration techniquement correcte en un texte mathématique élégant et accessible, facilitant ainsi la transmission du savoir mathématique.

# 4. Conseils pratiques pour améliorer votre rédaction

1. **Relisez-vous systématiquement**, si possible à voix haute. Une phrase difficile à prononcer sera difficile à comprendre.
2. **Faites tester votre rédaction** par un camarade de même niveau. Si cette personne comprend votre démonstration sans vos explications orales, votre rédaction est réussie.
3. **Vérifiez la logique** : assurez-vous que chaque implication est correcte et que toutes les notions utilisées ont été préalablement définies.
4. **Structurez en paragraphes** : un nouveau paragraphe marque une nouvelle étape du raisonnement.
5. **Concluez explicitement** : terminez vos démonstrations en écrivant « Ceci complète la démonstration » ou en utilisant le symbole $\square$.
6. **Consultez des corrigés** : observez comment les mathématiciens expérimentés rédigent leurs démonstrations.

# 5. Exemples de rédaction : démonstrations complètes

Cette section présente plusieurs démonstrations complètes illustrant l'application des principes de rédaction exposés précédemment.

## 5.1 Solutions de l'examen périodique MAT141 - Éléments d'algèbre-Trimestre d'automne 2018

### Question 1

### Partie (a)

**Proposition 1.** Soient $f : E \to F$ et $g : F \to G$ deux fonctions avec $g$ bijective. Alors $f$ est surjective si et seulement si $g \circ f$ est surjective.

*Démonstration.* Supposons que $f$ est surjective et montrons que $g \circ f$ est surjective. Soit $z \in G$. Puisque $g$ est bijective, elle est en particulier surjective. Il existe donc $y \in F$ tel que $g(y) = z$. Or $f$ est surjective par hypothèse, donc il existe $x \in E$ tel que $f(x) = y$. Par conséquent, nous avons

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= g(y) \\ &= z.\end{aligned}$$

Ceci montre que pour tout $z \in G$, il existe $x \in E$ tel que $(g \circ f)(x) = z$. Donc $g \circ f$ est surjective. Inversement, supposons que $g \circ f$ est surjective et montrons que $f$ est surjective. Soit $y \in F$, on a $g(y) \in G$. Comme $g \circ f$ est surjective, il existe $x \in E$ tel que $(g \circ f)(x) = g(y)$, c'est-à-dire $g(f(x)) = g(y)$. Or $g$ est bijective, donc en particulier injective. L'injectivité de $g$ implique que $f(x) = y$. Nous avons ainsi montré que pour tout $y \in F$, il existe $x \in E$ tel que $f(x) = y$. Par conséquent, $f$ est surjective. $\square$

### Partie (b)

La fonction $f : \mathbb{R}^+ \to \mathbb{R}^+$ définie par $f(x) = 1 + x + x^2$ pour tout $x \in \mathbb{R}^+$ est injective mais non surjective.

*Démonstration.* Nous allons d'abord montrer l'injectivité, puis la non-surjectivité.
**Injectivité de $f$.**
Soient $x_1, x_2 \in \mathbb{R}^+$ tels que $f(x_1) = f(x_2)$. Cela signifie que

$$1 + x_1 + x_1^2 = 1 + x_2 + x_2^2.$$

En simplifiant, nous obtenons

$$x_1 + x_1^2 = x_2 + x_2^2,$$

ce qui se réécrit

$$x_1^2 - x_2^2 + x_1 - x_2 = 0.$$

En factorisant, nous avons

$$\begin{aligned}(x_1 - x_2)(x_1 + x_2) + (x_1 - x_2) &= 0\\ (x_1 - x_2)(x_1 + x_2 + 1) &= 0.\end{aligned}$$

Puisque $x_1, x_2 \in \mathbb{R}^+$, nous avons $x_1 + x_2 + 1 \geq 1 > 0$. Donc nécessairement $x_1 - x_2 = 0$, c'est-à-dire $x_1 = x_2$. Ceci établit l'injectivité de $f$.
**Non-surjectivité de $f$.** Considérons $y = \frac{1}{2}$. Supposons par l'absurde qu'il existe $x \in \mathbb{R}^+$ tel que $f(x) = \frac{1}{2}$. Alors

$$1 + x + x^2 = \frac{1}{2}.$$

En réarrangeant, nous obtenons

$$x^2 + x + \frac{1}{2} = 0.$$

Le discriminant de cette équation du second degré est

$$\begin{aligned}\Delta &= 1 - 4 \cdot 1 \cdot \frac{1}{2}\\ &= -1 < 0.\end{aligned}$$

Comme le discriminant est strictement négatif, cette équation n'admet pas de solution réelle. Par conséquent, $\frac{1}{2} \notin \mathrm{Im}(f)$, ce qui montre que $f$ n'est pas surjective. □

# Question 2

## Partie (b)

L'ensemble $G = 2\mathbb{Z}_{36} = \{0, 2, 4, \ldots, 34\}$ est un sous-groupe de $(\mathbb{Z}_{36}, +)$.

*Démonstration.* **(i)** L'élément neutre de $\mathbb{Z}_{36}$ est 0, et nous avons $0 = 2 \cdot 0 \in G$. Donc $G \neq \emptyset$.
**(ii)** Soient $x, y \in G$. Alors il existent $a, b \in \mathbb{Z}$ tels que $x = 2a \pmod{36}$ et $y = 2b \pmod{36}$. Nous avons

$$\begin{aligned}x + y &= 2a + 2b\\ &= 2(a + b) \pmod{36}.\end{aligned}$$

Donc $x + y \in G$. Ceci montre que $G$ est stable par addition.
**(iii)** Soit $x \in G$. Alors $x = 2a \pmod{36}$ pour un certain $a \in \mathbb{Z}$. L'inverse de $x$ dans $\mathbb{Z}_{36}$ est $-x$, et nous avons

$$\begin{aligned}-x &= -2a\\ &= 2(-a) \pmod{36}.\end{aligned}$$

Donc $-x \in G$.
Nous concluons que $G$ est un sous-groupe de $\mathbb{Z}_{36}$. □

# Question 3

## Partie (a)

Soit $G$ un groupe. On définit une relation $\sim$ sur $G$ par : pour $x, y \in G$, on a $x \sim y$ si et seulement s'il existe $a \in G$ tel que $y = a^{-1}xa$.

### Question (i)

La relation $\sim$ est une relation d'équivalence sur $G$.

*Démonstration.* Pour montrer que $\sim$ est une relation d'équivalence, nous devons vérifier trois propriétés : réflexivité, symétrie et transitivité.
**Réflexivité.** Soit $x \in G$. Notons $e$ l'élément neutre de $G$. Nous avons

$$\begin{aligned} e^{-1}xe &= exe \\ &= x. \end{aligned}$$

Donc il existe $a = e \in G$ tel que $x = a^{-1}xa$, ce qui montre que $x \sim x$.
**Symétrie.** Soient $x, y \in G$ tels que $x \sim y$. Par définition, il existe $a \in G$ tel que $y = a^{-1}xa$. Montrons que $y \sim x$.
En multipliant l'égalité $y = a^{-1}xa$ à gauche par $a$ et à droite par $a^{-1}$, nous obtenons

$$\begin{aligned} aya^{-1} &= aa^{-1}xaa^{-1} \\ &= x. \end{aligned}$$

En posant $b = a^{-1}$, nous avons $b \in G$ (car $G$ est un groupe) et

$$x = b^{-1}yb.$$

Ceci montre que $y \sim x$.
**Transitivité.** Soient $x, y, z \in G$ tels que $x \sim y$ et $y \sim z$. Par définition, il existent $a, b \in G$ tels que

$$y = a^{-1}xa \quad \text{et} \quad z = b^{-1}yb.$$

En substituant la première égalité dans la seconde, nous obtenons

$$\begin{aligned} z &= b^{-1}(a^{-1}xa)b \\ &= b^{-1}a^{-1}xab \\ &= (ab)^{-1}x(ab). \end{aligned}$$

En posant $c = ab \in G$, nous avons $z = c^{-1}xc$, ce qui montre que $x \sim z$. □

### Question (ii)

Soient $x, y \in G$ et $a \in G$ tels que $y = a^{-1}xa$. Alors pour tout entier $n \geq 1$, on a $y^n = a^{-1}x^n a$.

*Démonstration.* Nous procédons par récurrence sur $n$.
**Initialisation.** Pour $n = 1$, nous avons $y^1 = y = a^{-1}xa = a^{-1}x^1a$ par hypothèse. La proposition $\mathcal{P}_1$ est donc vraie.
**Hérédité.** Soit $n \geq 1$. Supposons que $y^n = a^{-1}x^n a$ (hypothèse de récurrence). Montrons que

$y^{n+1} = a^{-1}x^{n+1}a$.
Par définition de la puissance, nous avons

$$y^{n+1} = y^n \cdot y.$$

En utilisant l'hypothèse de récurrence et l'hypothèse $y = a^{-1}xa$, nous obtenons

$$\begin{aligned} y^{n+1} &= (a^{-1}x^n a)(a^{-1}xa) \\ &= a^{-1}x^n(aa^{-1})xa \\ &= a^{-1}x^n exa \\ &= a^{-1}x^n xa \\ &= a^{-1}x^{n+1}a. \end{aligned}$$

La propriété est donc héréditaire.
**Conclusion.** Par le principe de récurrence, la proposition est vraie pour tout entier $n \geq 1$. □

### Partie (b)

Soit $G$ un groupe d'élément neutre $e$ et soient $a, b, x \in G$ tels que $ba^2 = a^{-1}b$, $a^5 = e$ et $axab = ba$. Alors $x = e$ et $ba = a^2b$.

## Question 4

### Partie (a)

**Proposition 2.** L'ensemble $G = \mathbb{Z} \times \mathbb{Z} = \{(a, b) : a, b \in \mathbb{Z}\}$ muni de l'addition

$$(a, b) + (a', b') = (a + a', b + b')$$

est un groupe abélien.

*Démonstration.* Pour montrer que $(G, +)$ est un groupe abélien, nous devons vérifier les quatre axiomes de groupe ainsi que la commutativité.
**(i) Associativité.** Soient $(a, b), (c, d), (e, f) \in G$. Nous avons

$$\begin{aligned} [(a, b) + (c, d)] + (e, f) &= (a + c, b + d) + (e, f) \\ &= ((a + c) + e, (b + d) + f) \\ &= (a + (c + e), b + (d + f)) \quad \text{(par associativité dans } \mathbb{Z}) \\ &= (a, b) + (c + e, d + f) \\ &= (a, b) + [(c, d) + (e, f)]. \end{aligned}$$

**(ii) Élément neutre.** Considérons l'élément $e_G = (0, 0) \in G$. Pour tout $(a, b) \in G$, nous avons

$$\begin{aligned} (a, b) + (0, 0) &= (a + 0, b + 0) \\ &= (a, b) \end{aligned}$$

et

$$\begin{aligned} (0, 0) + (a, b) &= (0 + a, 0 + b) \\ &= (a, b). \end{aligned}$$

Donc $(0, 0)$ est l'élément neutre de $G$.
**(iii) Inverse.** Soit $(a, b) \in G$. Considérons l'élément $(-a, -b) \in G$. Nous avons

$$\begin{aligned}(a, b) + (-a, -b) &= (a + (-a), b + (-b)) \\ &= (0, 0)\end{aligned}$$

et

$$\begin{aligned}(-a, -b) + (a, b) &= ((-a) + a, (-b) + b) \\ &= (0, 0).\end{aligned}$$

Donc $(-a, -b)$ est l'inverse de $(a, b)$ dans $G$.
**(iv) Commutativité.** Soient $(a, b), (c, d) \in G$. Nous avons

$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d) \\ &= (c + a, d + b) \quad \text{(par commutativité dans } \mathbb{Z}) \\ &= (c, d) + (a, b).\end{aligned}$$

L'opération est donc commutative.
Nous concluons que $(G, +)$ est un groupe abélien. □

## Partie (b)

L'ensemble $H = \{5^a 7^b : a, b \in \mathbb{Z}\}$ est un sous-groupe du groupe multiplicatif $(\mathbb{R}^*, \cdot)$ des réels non nuls.

*Démonstration.* **(i)** L'élément $1 = 5^0 \cdot 7^0 \in H$. Donc $H \neq \emptyset$.
**(ii)** Soient $x, y \in H$. Alors il existent $a, b, c, d \in \mathbb{Z}$ tels que $x = 5^a 7^b$ et $y = 5^c 7^d$. Nous avons

$$\begin{aligned}xy &= (5^a 7^b)(5^c 7^d) \\ &= 5^a \cdot 5^c \cdot 7^b \cdot 7^d \\ &= 5^{a+c} 7^{b+d}.\end{aligned}$$

Puisque $a + c \in \mathbb{Z}$ et $b + d \in \mathbb{Z}$, nous avons $xy \in H$. Donc $H$ est stable par multiplication.
**(iii)** Soit $x \in H$. Alors $x = 5^a 7^b$ pour certains $a, b \in \mathbb{Z}$. L'inverse de $x$ dans $\mathbb{R}^*$ est

$$\begin{aligned}x^{-1} &= (5^a 7^b)^{-1} \\ &= 5^{-a} 7^{-b}.\end{aligned}$$

Puisque $-a \in \mathbb{Z}$ et $-b \in \mathbb{Z}$, nous avons $x^{-1} \in H$. Par conséquent, $H$ est un sous-groupe de $(\mathbb{R}^*, \cdot)$. □

## Partie (c)

Il existe un isomorphisme $f : G \to H$ entre les groupes $G = (\mathbb{Z} \times \mathbb{Z}, +)$ et $H = (\{5^a 7^b : a, b \in \mathbb{Z}\}, \cdot)$.

*Démonstration.* Définissons l'application $f : G \to H$ par

$$f((a, b)) = 5^a 7^b$$

pour tout $(a,b) \in G$. Nous allons montrer que $f$ est un isomorphisme en vérifiant qu'elle est un morphisme, qu'elle est injective et qu'elle est surjective.
$f$ est un morphisme. En effet, soient $(a,b),(c,d) \in G$. Nous avons

$$\begin{aligned} f((a,b)+(c,d)) &= f((a+c,b+d)) \\ &= 5^{a+c}7^{b+d} \\ &= 5^a \cdot 5^c \cdot 7^b \cdot 7^d \\ &= (5^a 7^b)(5^c 7^d) \\ &= f((a,b)) \cdot f((c,d)). \end{aligned}$$

$f$ est injective. Soient $(a,b),(c,d) \in G$ tels que $f((a,b)) = f((c,d))$. Cela signifie que

$$5^a 7^b = 5^c 7^d.$$

En divisant les deux côtés par $5^c 7^b$, on obtient

$$5^{a-c} = 7^{d-b}.$$

Si $a \neq c$, le membre de gauche est divisible par 5, tandis que le membre de droite ne l'est pas, car aucune puissance de 7 n'est divisible par 5. C'est une contradiction. Donc $a = c$. En remplaçant dans l'égalité initiale, on obtient $7^b = 7^d$, d'où $b = d$. Ainsi $(a,b) = (c,d)$, ce qui montre que $f$ est injective.
$f$ est surjective. Soit $y \in H$. Par définition de $H$, il existent $a,b \in \mathbb{Z}$ tels que $y = 5^a 7^b$. En posant $x = (a,b) \in G$, nous avons

$$\begin{aligned} f(x) &= f((a,b)) \\ &= 5^a 7^b \\ &= y. \end{aligned}$$

Donc $f$ est surjective. $\square$

**Proposition 3.** Soit $(G, \cdot)$ un groupe et $a \in G$. Pour tout entier naturel $n \geq 1$, on a $(a^n)^{-1} = (a^{-1})^n$.

*Démonstration.* **Initialisation.** Pour $n = 1$, nous avons $(a^1)^{-1} = a^{-1} = (a^{-1})^1$. La proposition $\mathcal{P}_1$ est donc vraie.

**Hérédité.** Soit $n \geq 1$. Supposons que $(a^n)^{-1} = (a^{-1})^n$ (hypothèse de récurrence). Montrons que $(a^{n+1})^{-1} = (a^{-1})^{n+1}$.
Par définition de la puissance, nous avons $a^{n+1} = a^n \cdot a$. En utilisant la propriété $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$ valable dans tout groupe, nous obtenons

$$\begin{aligned}(a^{n+1})^{-1} &= (a^n \cdot a)^{-1} \\ &= a^{-1} \cdot (a^n)^{-1}.\end{aligned}$$

Or, par hypothèse de récurrence, $(a^n)^{-1} = (a^{-1})^n$. Donc

$$\begin{aligned}(a^{n+1})^{-1} &= a^{-1} \cdot (a^{-1})^n \\ &= (a^{-1})^{n+1}.\end{aligned}$$

La propriété est donc héréditaire.

**Conclusion.** Par le principe de récurrence, la proposition est vraie pour tout entier naturel $n \geq 1$.

$\square$

**Proposition 4.** Soit $(G, \cdot)$ un groupe. Si $H$ et $K$ sont deux sous-groupes de $G$, si $H \cup K$ est un sous-groupe de $G$ alors $H \subseteq K$ ou $K \subseteq H$.

*Démonstration.* Supposons que $H \cup K$ soit un sous-groupe de $G$, mais que $H \nsubseteq K$ et $K \nsubseteq H$. Puisque $H \nsubseteq K$, il existe un élément $h \in H$ tel que $h \notin K$. De même, puisque $K \nsubseteq H$, il existe un élément $k \in K$ tel que $k \notin H$. Or $h \in H \subseteq H \cup K$ et $k \in K \subseteq H \cup K$. Comme $H \cup K$ est supposé être un sous-groupe, il doit être stable par l'opération du groupe. Donc le produit $h \cdot k$ appartient à $H \cup K$. Nous avons alors deux cas possibles : soit $h \cdot k \in H$, soit $h \cdot k \in K$.
*Premier cas :* Si $h \cdot k \in H$, alors puisque $h \in H$ et que $H$ est un sous-groupe, nous avons $h^{-1} \in H$. Par stabilité de $H$, on obtient $k = h^{-1} \cdot (h \cdot k) \in H$, ce qui contredit le fait que $k \notin H$.
*Second cas :* Si $h \cdot k \in K$, alors puisque $k \in K$ et que $K$ est un sous-groupe, nous avons $k^{-1} \in K$. Par stabilité de $K$, on obtient $h = (h \cdot k) \cdot k^{-1} \in K$, ce qui contredit le fait que $h \notin K$.
Dans les deux cas, nous aboutissons à une contradiction. Par conséquent, si $H \cup K$ est un sous-groupe, alors nécessairement $H \subseteq K$ ou $K \subseteq H$. $\square$

## 5.2 Extensions entières d'anneaux

**Proposition 5.** Soient $R$ et $S$ deux anneaux intègres, avec $S$ entier sur $R$. Alors $S$ est un corps si et seulement si $R$ est un corps.

*Démonstration.* Supposons que $R$ est un corps et montrons que $S$ est un corps. Soit $x \in S \setminus \{0\}$. Puisque $S$ est entier sur $R$, alors nous pouvons écrire

$$x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0, \quad (\star)$$

avec $m \in \mathbb{N}^*$, $a_i \in R$ $(0 \leq i \leq m)$. De plus, comme $R$ est intègre, nous pouvons supposer que $a_0 \neq 0$ [1]. Alors $a_0$ a un inverse dans $R$. Par $(\star)$, nous avons

1. Si $a_0 = 0$, on peut factoriser $x$ dans l'équation $(\star)$. Comme $R$ est intègre et que $x$ est non nul, on obtient une équation de degré strictement inférieur. On peut donc supposer, quitte à réduire le degré, que $a_0 \neq 0$.

$$\begin{aligned} a_0 &= -(x^m + a_{m-1}x^{m-1} + \cdots + a_1 x) \\ &= -(x^{m-1} + a_{m-1}x^{m-2} + \cdots + a_1)x \quad (\star\star) \end{aligned}$$

En multipliant $(\star\star)$ par $a_0^{-1}$, nous obtenons

$$1 = -a_0^{-1}(x^{m-1} + a_{m-1}x^{m-2} + \cdots + a_1)x,$$

ce qui montre que $x$ est inversible dans $S$.

Inversement, supposons que $S$ est un corps et soit $r \in R \setminus \{0\}$. Alors $r^{-1} \in S$ et nous pouvons écrire

$$r^{-n} + b_{n-1}r^{-(n-1)} + \cdots + b_0 = 0, \quad (\star\star\star)$$

pour un certain $n \in \mathbb{N}^*$ et certains éléments $b_i \in R$. En multipliant $(\star\star\star)$ par $r^{n-1}$ nous obtenons

$$r^{-1} + b_{n-1} + \cdots + b_0 r^{n-1} = 0.$$

Donc, $r^{-1} = -(b_{n-1} + \cdots + b_0 r^{n-1}) \in R$. Par conséquent, $R$ est un corps. □

**Théorème 1.** *Soient $R$ et $S$ deux anneaux avec $S$ entier sur $R$. Soit $P$ un idéal premier de $S$. Alors :*

*(1) $P \cap R$ est un idéal premier de $R$.*

*(2) $P$ est un idéal maximal de $S$ si et seulement si $P \cap R$ est un idéal maximal dans $R$.*

Pour la démonstration, nous avons besoin du lemme suivant :

**Lemme 1.** *Soient $R$ et $S$ deux anneaux avec $S$ entier sur $R$. Soit $P$ un idéal de $S$. Alors :*

*(1) $P \cap R$ est un idéal de $R$.*

*(2) $S/P$ est entier sur $R/P \cap R$.*

*Démonstration.* (1) Soit $\iota : R \longrightarrow S$ l'homomorphisme inclusion. Alors $\iota^{-1}(P)$ est un idéal de $R$. De plus, on a

$$\begin{aligned} \iota^{-1}(P) &= \{r \in R \mid \iota(r) \in P\} \\ &= \{r \in R \mid r \in P\} \\ &= P \cap R. \end{aligned}$$

(2) Soit $\varphi : R/(P \cap R) \longrightarrow S/P$ l'application définie par $\varphi(x + P \cap R) = x + P$, pour tout $x \in R$. On vérifie aisément que $\varphi$ est un homomorphisme d'anneaux. Montrons que $\varphi$ est injective. Soient $x_1 + P \cap R$ et $x_2 + P \cap R$ dans $R/(P \cap R)$ tels que $\varphi(x_1 + P \cap R) = \varphi(x_2 + P \cap R)$. Cela implique que $x_1 - x_2 \in P$. Puisque $x_1 - x_2 \in R$, on en déduit que $x_1 - x_2 \in P \cap R$, d'où $x_1 + P \cap R = x_2 + P \cap R$. Par conséquent, $R/(P \cap R)$ peut être identifié à un sous-anneau de $S/P$.
Soit $x \in S$. Comme $x$ est entier sur $R$, nous pouvons écrire

$$x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0,$$

avec $m \in \mathbb{N}^*$, $a_i \in R$ $(0 \leq i \leq m)$. Soit $\overline{x}$ l'image de $x$ dans $S/P$. Alors

$$\overline{x}^m + \overline{a_{m-1}}\overline{x^{m-1}} + \cdots + \overline{a_0} = \overline{0}.$$

Donc $\overline{x}$ est entier sur $\varphi(R/P \cap R)$. D'où $x$ est entier sur $R/P \cap R$.

□

**Démonstration du Théorème 1 :**

(1) $P \cap R$ est un idéal premier. En effet :

  (i) $P \cap R \neq R$ car sinon, $P \cap R = R$, ce qui implique que $R \subset P$. Donc $1 \in P$, une contradiction.

  (ii) Soient $r_1, r_2 \in R$ tels que $r_1 r_2 \in P \cap R$. Alors $r_1 r_2 \in P$. Comme $P$ est premier, alors $r_1 \in P \cap R$ ou $r_2 \in P \cap R$.

(2) Puisque $P$ est premier, l'anneau quotient $S/P$ est intègre. D'après le point (1), $R/P \cap R$ est également intègre, et le lemme 1 assure que $S/P$ est entier sur $R/P \cap R$. La proposition 5 implique alors que $S/P$ est un corps si et seulement si $R/P \cap R$ est un corps. Par conséquent, $P$ est un idéal maximal si et seulement si $P \cap R$ est maximal.

## 5.3 Espaces topologiques noethériens et irréductibles

**Proposition 6.** Soit $X$ un espace topologique. Les conditions suivantes sont équivalentes :

(1) $X$ est noethérien.

(2) Chaque suite décroissante de fermés est constante.

(3) Chaque collection non vide de fermés contient un élément minimal.

*Démonstration.* Montrons que (1) entraîne (2). Soit $X$ noethérien et considérons une suite décroissante de fermés $(F_n)_{n\geq 0}$. En posant $U_n = X \setminus F_n$ pour tout $n \geq 0$, on obtient une suite croissante d'ouverts $(U_n)_{n\geq 0}$. Puisque $X$ est noethérien, cette suite se stabilise, c'est-à-dire qu'il existe un entier $m$ tel que $U_n = U_m$ pour tout $n \geq m$. Par passage au complémentaire, on en déduit que $F_n = F_m$ pour tout $n \geq m$, ce qui établit la stationnarité de la suite $(F_n)_{n\geq 0}$.

Montrons que (2) entraîne (3). Soit $\mathcal{F}$ une collection non vide de fermés. Supposons par l'absurde que $\mathcal{F}$ n'admette pas d'élément minimal. Choisissons $F_0 \in \mathcal{F}$ arbitrairement. Par hypothèse, $F_0$ n'est pas minimal dans $\mathcal{F}$, ce qui garantit l'existence d'un fermé $F_1 \in \mathcal{F}$ vérifiant $F_1 \subsetneq F_0$. En itérant ce raisonnement, on construit par récurrence une suite strictement décroissante $(F_n)_{n\geq 0}$ d'éléments de $\mathcal{F}$, contredisant l'hypothèse que toute suite décroissante de fermés est stationnaire.

Montrons enfin que (3) entraîne (1). Soit $(U_n)_{n\geq 0}$ une suite croissante d'ouverts[2] de $X$. La famille $\mathcal{F} = \{F_n : n \geq 0\}$, où $F_n = X \setminus U_n$, constitue une collection non vide de fermés décroissants. D'après l'hypothèse, $\mathcal{F}$ possède un élément minimal $F_m$. Pour tout $n \geq m$, on a $F_n \subseteq F_m$, et la minimalité de $F_m$ dans $\mathcal{F}$ implique nécessairement $F_n = F_m$. Par conséquent, $U_n = U_m$ pour tout $n \geq m$, ce qui démontre que $X$ est noethérien. □

**Proposition 7.** Soit $X$ un espace topologique non vide. Les conditions suivantes sont équivalentes :

(1) $X$ est irréductible.

(2) Si $U_1, U_2 \subseteq X$ sont des ouverts non vides, alors $U_1 \cap U_2 \neq \emptyset$.

(3) Tout ouvert non vide $U \subseteq X$ est dense dans $X$.

*Démonstration.* Montrons d'abord que (1) entraîne (2). Soit $X$ irréductible et soient $U_1$, $U_2$ deux ouverts non vides de X. Supposons par l'absurde que $U_1 \cap U_2 = \varnothing$. En passant aux compléments, on obtient $X = U_1^c \cup U_2^c$, où $U_1^c$ et $U_2^c$ sont des fermés propres. Puisque $X$ est irréductible, on a nécessairement $U_i^c = X$ pour $i = 1$ ou $i = 2$, ce qui implique $U_i = \varnothing$, contredisant l'hypothèse.

Montrons ensuite que (2) entraîne (3). Soit $U$ un ouvert non vide de $X$. Pour établir que $U$ est dense, considérons un ouvert non vide $V$ arbitraire. D'après l'hypothèse, $U \cap V \neq \varnothing$, ce qui montre que $U$ rencontre tout ouvert non vide de $X$. Par conséquent, $\overline{U} = X$.

2. On peut supposer que $U_0$ est un ouvert non vide tel que $U_0 \neq X$.

Montrons enfin que (3) entraîne (1). Supposons que tout ouvert non vide de $X$ soit dense et considérons une décomposition $X = X_1 \cup X_2$ où $X_1$ et $X_2$ sont des fermés propres. Les ouverts $U_1 = X \setminus X_2$ et $U_2 = X \setminus X_1$ sont alors non vides. Par hypothèse, $U_1$ est dense dans $X$, donc rencontre tout ouvert non vide, notamment $U_2$. Cependant,

$$\begin{aligned} U_1 \cap U_2 &= (X \setminus X_2) \cap (X \setminus X_1) \\ &= X \setminus (X_1 \cup X_2) \\ &= \varnothing, \end{aligned}$$

ce qui constitue une contradiction. Ainsi, $X$ est irréductible. □

**Théorème 2.** *Soit $X$ un espace irréductible et $U \subseteq X$ un ouvert non vide. Alors $U$ est irréductible pour la topologie induite.*

*Démonstration.* Soient $U_1 = W_1 \cap U$ et $U_2 = W_2 \cap U$ deux ouverts non vides de $U$, où $W_1$ et $W_2$ sont des ouverts non vides de $X$. Puisque $X$ est irréductible, la Proposition 2 assure que $W_1 \cap W_2 \neq \emptyset$. On en déduit que

$$\begin{aligned} U_1 \cap U_2 &= (U \cap W_1) \cap (U \cap W_2) \\ &= U \cap (W_1 \cap W_2) \\ &\neq \emptyset. \end{aligned}$$

Ceci prouve que $U$ est irréductible. □

## 5.4 Anneaux noethériens et anneaux de polynômes

**Théorème 3.** *Soit $A$ un anneau tel que $A[X]$ soit noethérien, alors $A$ est noethérien.*

Pour la démonstration, nous avons besoin du lemme suivant :

**Lemme 2.** *Soient $A$, $B$ deux anneaux et $\varphi : A \longrightarrow B$ un homomorphisme d'anneaux. Si $A$ est noethérien, alors $\operatorname{Im}\varphi$ est aussi noethérien.*

*Démonstration.* $\operatorname{Im}\varphi$ est un sous-anneau de $B$. En effet, $\operatorname{Im}\varphi$ est non vide puisque $0_B = \varphi(0_A) \in \operatorname{Im}\varphi$, et pour tous $b_1 = \varphi(a_1)$ et $b_2 = \varphi(a_2)$ avec $a_1, a_2 \in A$, on a $b_1 + b_2 = \varphi(a_1 + a_2) \in \operatorname{Im}\varphi$ et $b_1 b_2 = \varphi(a_1 a_2) \in \operatorname{Im}\varphi$.

Soit $J$ un idéal de $\operatorname{Im}\varphi$. Montrons que $J$ est de type fini. Posons $I := \varphi^{-1}(J)$. Il est clair que $I$ est un idéal de $A$. Comme $A$ est noethérien, alors $I$ est de type fini. Notons $a_1, \ldots, a_n$ les générateurs de $I$, c'est-à-dire $I = \langle a_1, \ldots, a_n \rangle$.

D'autre part, pour tout $y \in J$, il existe $x \in A$ tel que $y = \varphi(x)$. Par définition de l'image réciproque de $J$, on a $x \in I$. Donc il existe $c_1, \ldots, c_n \in A$ tels que $x = \sum_{i=1}^{n} c_i a_i$. En appliquant $\varphi$, nous obtenons

$$y = \varphi(x) = \sum_{i=1}^{n} \varphi(c_i)\varphi(a_i).$$

Or $\varphi(c_i) \in \operatorname{Im}\varphi$, donc $\varphi(c_i)\varphi(a_i) \in J$ (car $\varphi(a_i) \in J$). On en déduit que les $\varphi(a_i)$ sont les générateurs de $J$ dans $\operatorname{Im}\varphi$. Donc $J = \langle \varphi(a_1), \ldots, \varphi(a_n) \rangle$. Par suite, $J$ est de type fini. D'où $\operatorname{Im}\varphi$ est un anneau noethérien. □

Nous sommes maintenant prêts à démontrer notre résultat principal.

*Démonstration du Théorème 1.* Soit $\varphi : A[X] \longrightarrow A$ l'homomorphisme d'anneaux définie par

$$\varphi(P(X)) = P(0), \text{ pour tout } P(X) \in A[X].$$

$\varphi$ est surjective. En effet, pour tout $a \in A$, on a $a = \varphi(P(X))$, avec $P(X) = a \in A[X]$. Puisque $A[X]$ est noethérien par hypothèse, le lemme 1 implique que $\varphi(A[X]) = A$ est noethérien. □

**Corollaire 1.** *Soit* $A$ *un anneau et soit* $n \in \mathbb{N}^*$. *Si l'anneau de polynômes* $A[x_1, \ldots, x_n]$ *est noethérien, alors* $A$ *est noethérien.*

*Démonstration.* Procédons par récurrence sur $n$. Le cas $n = 1$ est le Théorème 1. Pour l'étape de récurrence, on utilise l'identification $A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n]$ et on applique successivement le Théorème 1 puis l'hypothèse de récurrence. □