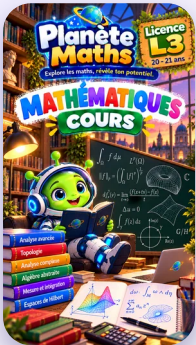


# Groupes, anneaux et corps : cours de maths Licence L3 à télécharger en PDF



## Le livre de cours de maths Licence L3

Tout le programme en un seul PDF de 101 pages, à imprimer ou à garder sur ta tablette.

[Voir le livre](#)

Ce chapitre rassemble trois grandes structures de l'algèbre : les **groupes**, les **anneaux** et les **corps**. Le fil conducteur est la notion de **quotient** : on identifie des éléments « équivalents » pour obtenir un objet plus simple, qui conserve l'essentiel de la structure. Nous l'utiliserons pour compter, classer et construire de nouveaux corps.

## 1. Groupes quotients

D

### Sous-groupe distingué

Un sous-groupe  $H$  d'un groupe  $G$  est **distingué** (on note  $H \triangleleft G$ ) si  $gHg^{-1} = H$  pour tout  $g \in G$ , c'est-à-dire si  $ghg^{-1} \in H$  pour tous  $g \in G, h \in H$ .

Tout sous-groupe d'un groupe abélien est distingué, ainsi que tout sous-groupe d'indice 2. Le noyau d'un morphisme de groupes est toujours distingué.

## P

## Groupe quotient

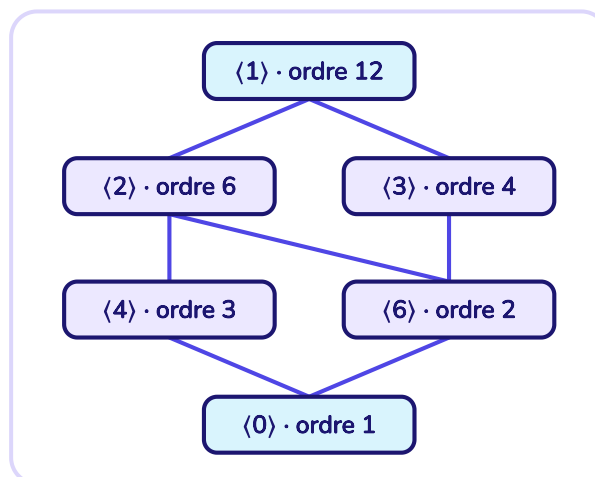
Si  $H \triangleleft G$ , l'ensemble  $G/H$  des classes  $gH$  est un groupe pour la loi  $(gH)(g'H) = gg'H$ . Son ordre est l'indice  $[G : H]$ , égal à  $|G|/|H|$  si  $G$  est fini. La projection  $\pi : G \rightarrow G/H$  est un morphisme surjectif de noyau  $H$ .

## P

## Premier théorème d'isomorphisme

Si  $f : G \rightarrow G'$  est un morphisme de groupes, alors  $G/\ker f \cong \operatorname{Im} f$ , l'isomorphisme envoyant la classe  $g\ker f$  sur  $f(g)$ .

Dans  $\mathbb{Z}/12\mathbb{Z}$ , les sous-groupes sont ceux engendrés par les diviseurs de 12 ; ils sont tous distingués, et leur inclusion se lit sur le treillis ci-dessous.



## E

Exemple 1 : un quotient de  $\mathbb{Z}/12\mathbb{Z}$ 

Prenons  $H = \langle 4 \rangle = \{0, 4, 8\}$ . Alors  $|G/H| = 12/3 = 4$ . La classe de 1 vérifie  $k \cdot 1 \in H$  si et seulement si  $4 \mid k$  : elle est d'ordre 4, donc  $G/H$  est cyclique, isomorphe à  $\mathbb{Z}/4\mathbb{Z}$  (c'est le morphisme « réduction modulo 4 », de noyau  $H$ ).



### Attention

Un sous-groupe n'est pas toujours distingué : dans  $S_3$ , le sous-groupe  $\{\text{id}, (1\ 2)\}$  ne l'est pas, car  $(1\ 3)(1\ 2)(1\ 3) = (2\ 3)$ . En revanche  $A_3$  l'est (indice 2) et  $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ .

## 2. Actions de groupes



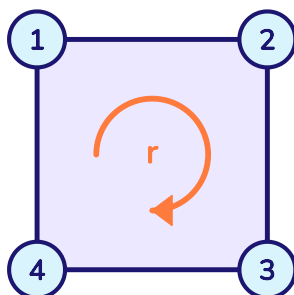
### Action, orbite, stabilisateur

Une **action** de  $G$  sur un ensemble  $X$  est un morphisme  $G \rightarrow \mathfrak{S}(X)$ , noté  $(g, x) \mapsto g \cdot x$ . L'**orbite** de  $x$  est  $G \cdot x = \{g \cdot x : g \in G\}$  et son **stabilisateur** est  $G_x = \{g \in G : g \cdot x = x\}$ , sous-groupe de  $G$ .



### Formule orbite-stabilisateur

L'application  $gG_x \mapsto g \cdot x$  est une bijection de  $G/G_x$  (ensemble des classes) sur  $G \cdot x$ . Si  $G$  est fini :  $|G| = |G \cdot x| \times |G_x|$ . Les orbites partitionnent  $X$ , d'où l'**équation aux classes**  $|X| = \sum |G \cdot x_i|$  (une somme sur un représentant par orbite).



$r$  : rotation de  $90^\circ$  ; orbite de  $1 = \{1, 2, 3, 4\}$

**E****Exemple 2 : rotations d'un carré**

Le groupe  $C_4 = \langle r \rangle$  des rotations d'un carré agit sur les 4 sommets. L'orbite du sommet 1 est  $\{1, 2, 3, 4\}$  (taille 4) et le stabilisateur est réduit à l'identité :  $4 = 4 \times 1$ . Pour compter les coloriage des sommets avec 2 couleurs à rotation près, la formule de Burnside donne le nombre d'orbites :  $\frac{1}{4} \sum_g |\text{Fix}(g)| = \frac{16+2+4+2}{4} = 6$ .

**3. Théorèmes de Sylow**

Soit  $G$  fini avec  $|G| = p^a m$ ,  $p$  premier ne divisant pas  $m$ . Un  **$p$ -sous-groupe de Sylow** est un sous-groupe d'ordre  $p^a$ .

**P****Théorèmes de Sylow**

- Il existe au moins un  $p$ -sous-groupe de Sylow.
- Deux  $p$ -sous-groupes de Sylow sont conjugués.
- Le nombre  $n_p$  de  $p$ -sous-groupes de Sylow vérifie  $n_p \equiv 1 \pmod{p}$  et  $n_p \mid m$ .

**M****Méthode : étudier un groupe d'ordre donné**

- Décomposer  $|G| = p^a m$  pour chaque premier  $p$ .
- Lister les diviseurs de  $m$  congrus à 1 modulo  $p$  : ce sont les valeurs possibles de  $n_p$ .
- Si  $n_p = 1$ , le sous-groupe de Sylow est unique donc distingué (conjugaison).  
Sinon, compter les éléments d'ordre  $p$  pour obtenir une contradiction.

**E****Exemple 3 : un groupe d'ordre 15**

Ici  $15 = 3 \times 5$ . On a  $n_5 \mid 3$  et  $n_5 \equiv 1 \pmod{5}$ , donc  $n_5 = 1$ . De même  $n_3 \mid 5$  et  $n_3 \equiv 1 \pmod{3}$  donne  $n_3 = 1$ . Les deux sous-groupes sont distingués, d'intersection triviale :  $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$ . Tout groupe d'ordre 15 est cyclique.

**4. Anneaux, idéaux et quotients****D****Idéal**

Un **idéal**  $I$  d'un anneau commutatif  $A$  est un sous-groupe additif tel que  $aI \subset I$  pour tout  $a \in A$ . L'anneau quotient  $A/I$  est formé des classes  $a + I$ , avec  $(a + I)(b + I) = ab + I$ . Le noyau d'un morphisme d'anneaux est un idéal, et  $A/\ker f \cong \text{Im } f$ .

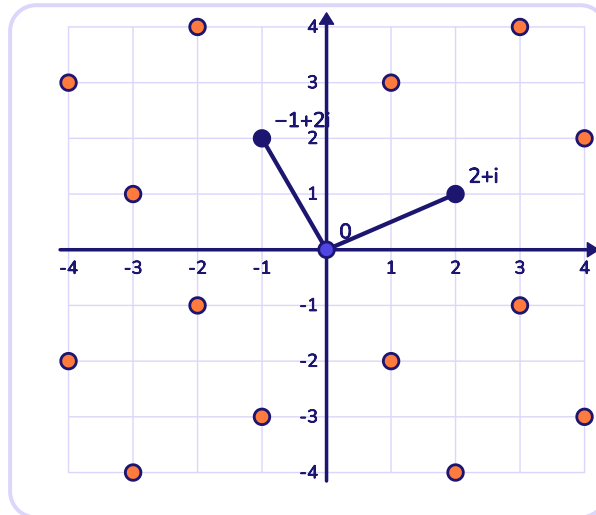
**D****Anneau principal**

Un anneau intègre est **principal** si tous ses idéaux sont de la forme  $(a) = aA$ . L'anneau  $\mathbb{Z}$ , les anneaux  $K[X]$  (où  $K$  est un corps) et  $\mathbb{Z}[i]$  sont principaux (ils sont euclidiens). En revanche  $\mathbb{Z}[X]$  ne l'est pas : l'idéal  $(2, X)$  n'est engendré par aucun élément.

## P

## Quotients et corps

Dans un anneau principal  $A$  et pour  $a \neq 0$  non inversible :  $A/(a)$  est un corps  $\iff a$  est irréductible  $\iff (a)$  est un idéal maximal. Ainsi  $\mathbb{Z}/p\mathbb{Z}$  est un corps pour  $p$  premier, et  $K[X]/(P)$  est un corps si et seulement si  $P$  est irréductible.



## E

Exemple 4 : un quotient de  $\mathbb{Z}[i]$ 

L'application  $a + bi \mapsto a - 2b \bmod 5$  est un morphisme d'anneaux vers  $\mathbb{Z}/5\mathbb{Z}$  (car  $(-2)^2 = 4 \equiv -1$ ). Elle est surjective, de noyau l'idéal  $(2 + i)$ , dont les éléments forment le réseau tracé ci-dessus. Donc  $\mathbb{Z}[i]/(2 + i) \cong \mathbb{Z}/5\mathbb{Z}$  : c'est un corps à 5 éléments.

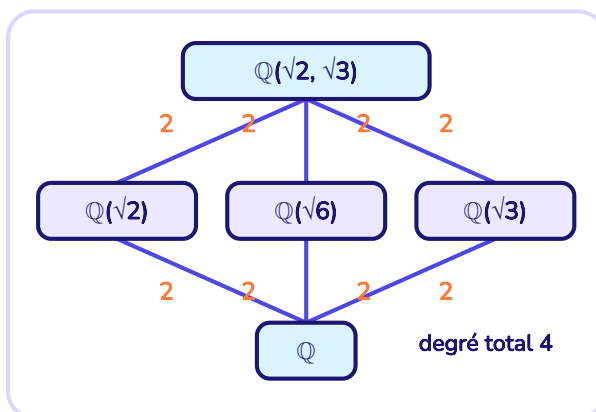
## 5. Extensions de corps

### D Degré d'une extension

Si  $K \subset L$  sont deux corps,  $L$  est un  $K$ -espace vectoriel ; sa dimension est le **degré**  $[L : K]$ . Un élément  $\alpha \in L$  est **algébrique** sur  $K$  s'il est racine d'un polynôme non nul de  $K[X]$  ; son **polynôme minimal** est le polynôme unitaire irréductible  $\mu$  de plus petit degré qui l'annule. Alors  $K(\alpha) \cong K[X]/(\mu)$  et  $[K(\alpha) : K] = \deg \mu$ , avec pour base  $1, \alpha, \dots, \alpha^{\deg \mu - 1}$ .

### P Multiplicativité des degrés

Pour une tour  $K \subset L \subset M$  d'extensions finies :  $[M : K] = [M : L][L : K]$ .



Le polynôme minimal de  $\sqrt{2}$  sur  $\mathbb{Q}$  est  $X^2 - 2$ , celui de  $\sqrt{3}$  sur  $\mathbb{Q}(\sqrt{2})$  est  $X^2 - 3$  : la tour donne  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \times 2 = 4$ , comme sur la figure.



### Astuce de Zyro

Zyro, l'explorateur extraterrestre, retient ceci : pour inverser un élément de  $\mathbb{Q}(\sqrt{d})$ , on multiplie par le conjugué. Ainsi  $(3 + \sqrt{2})^{-1} = \frac{3 - \sqrt{2}}{7}$  puisque  $(3 + \sqrt{2})(3 - \sqrt{2}) = 7$ .

## 6. Corps finis

Un corps fini  $K$  a pour caractéristique un nombre premier  $p$  ; il contient  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  et en est un espace vectoriel de dimension  $n$  :  $|K| = p^n$ .



### Structure des corps finis

- Pour tout premier  $p$  et tout  $n \geq 1$ , il existe un corps à  $p^n$  éléments, unique à isomorphisme près, noté  $\mathbb{F}_{p^n}$ .
- Le groupe multiplicatif  $\mathbb{F}_q^\times$  est cyclique, d'ordre  $q - 1$ .
- $\mathbb{F}_{p^m}$  est un sous-corps de  $\mathbb{F}_{p^n}$  si et seulement si  $m \mid n$ .
- L'application de Frobenius  $x \mapsto x^p$  est un morphisme de corps.



### Exemple 5 : le corps à 4 éléments

Le polynôme  $X^2 + X + 1$  n'a aucune racine dans  $\mathbb{F}_2$  (il vaut 1 en 0 et en 1) et il est de degré 2 : il est irréductible. Donc  $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1) = \{0, 1, \alpha, \alpha + 1\}$  avec  $\alpha^2 = \alpha + 1$ , et la table de multiplication est la suivante.

| $\times$   | 0 | 1          | $\alpha$   | $\alpha+1$ |
|------------|---|------------|------------|------------|
| 0          | 0 | 0          | 0          | 0          |
| 1          | 0 | 1          | $\alpha$   | $\alpha+1$ |
| $\alpha$   | 0 | $\alpha$   | $\alpha+1$ | 1          |
| $\alpha+1$ | 0 | $\alpha+1$ | 1          | $\alpha$   |

On lit que  $\alpha$  et  $\alpha + 1$  sont inverses l'un de l'autre, et que  $\alpha^3 = 1$  : le groupe  $\mathbb{F}_4^\times$  est cyclique d'ordre 3.

## 7. Irréductibilité des polynômes

### P

#### Critères d'irréductibilité

- **Degré 2 ou 3** :  $P \in K[X]$  est irréductible si et seulement s'il n'a pas de racine dans  $K$ .
- **Réduction** : si  $P \in \mathbb{Z}[X]$  est unitaire et que sa réduction modulo un premier  $p$  est irréductible sur  $\mathbb{F}_p$ , alors  $P$  est irréductible sur  $\mathbb{Q}$ .
- **Critère d'Eisenstein** : si  $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$  et si un premier  $p$  divise  $a_0, \dots, a_{n-1}$ , ne divise pas  $a_n$ , et si  $p^2 \nmid a_0$ , alors  $P$  est irréductible sur  $\mathbb{Q}$ .

**E****Exemple 6 : Eisenstein après translation**

Pour  $P = X^4 + 1$ , on développe  $P(X + 1) = X^4 + 4X^3 + 6X^2 + 4X + 2$  : le critère d'Eisenstein avec  $p = 2$  s'applique, donc  $P(X + 1)$  est irréductible, et  $P$  aussi (une factorisation de  $P$  se transporterait par translation). Remarque :  $X^4 + 1$  est pourtant réductible modulo tout nombre premier, ce qui montre qu'une réduction ne suffit pas toujours.

**Attention**

Le test « pas de racine » ne vaut que pour les degrés 2 et 3 :  $(X^2 + 1)^2$  n'a pas de racine réelle et pourtant il est réductible.

**À retenir**

- $H \triangleleft G$  permet de former  $G/H$  ;  $G/\ker f \cong \text{Im } f$ .
- Pour une action :  $|G| = |G \cdot x| |G_x|$  ; les orbites partitionnent  $X$ .
- Sylow : existence, conjugaison,  $n_p \equiv 1 \pmod{p}$  et  $n_p \mid m$  ;  $n_p = 1$  équivaut à un Sylow distingué.
- Dans un anneau principal,  $A/(a)$  est un corps si et seulement si  $a$  est irréductible.
- $[K(\alpha) : K] = \deg \mu_\alpha$  et les degrés se multiplient dans une tour.
- Un corps fini a  $p^n$  éléments et  $\mathbb{F}_q^\times$  est cyclique d'ordre  $q - 1$ .
- Eisenstein, réduction modulo  $p$  et absence de racine (degrés 2 et 3) servent à prouver l'irréductibilité.

## Le livre de cours de maths Licence L3

Tout le programme en un seul PDF de 101 pages, à imprimer ou à garder sur ta tablette.

[Voir le livre](#)

### Zyro te conseille la suite

#### Exercices de maths

Groupes, anneaux et corps : exercices de maths Licence L3

#### Contrôles de maths

Groupes, anneaux et corps : contrôle de maths Licence L3

#### QCM de maths

Groupes, anneaux et corps : QCM de maths Licence L3

#### Exercices de maths

Topologie des espaces métriques : exercices de maths Licence L3

 **Exercices de maths**

Espaces complets et point fixe : exercices  
de maths Licence L3

 **Contrôles de maths**

Topologie des espaces métriques :  
contrôle de maths Licence L3

**Zyro vous emmène sur nos sites partenaires**

Embarquez pour d'autres planètes du savoir et leurs applis.

Décollage