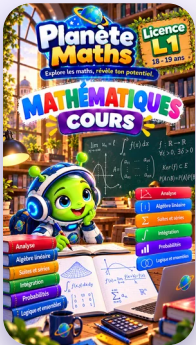


Arithmétique et structures : cours de maths Licence L1 à télécharger en PDF



Le livre de cours de maths Licence L1

Tout le programme en un seul PDF de 99 pages, à imprimer ou à garder sur ta tablette.

[Voir le livre](#)

Ce chapitre réunit deux univers : les entiers, avec leurs diviseurs et leurs congruences, et les structures algébriques (groupes, anneaux, corps) qui en dégagent les règles de calcul. On y voit comment un calcul sur les restes devient un exemple de groupe, puis comment les morphismes comparent deux structures.

1. Divisibilité et PGCD

D

Divisibilité

Pour $a, b \in \mathbb{Z}$, on dit que a divise b , noté $a \mid b$, s'il existe $k \in \mathbb{Z}$ tel que $b = ka$. Le PGCD de deux entiers non tous nuls est le plus grand entier positif qui les divise tous les deux, noté $a \wedge b$.

P**Division euclidienne et algorithme d'Euclide**

Pour $b > 0$, il existe un unique couple (q, r) avec $a = bq + r$ et $0 \leq r < b$. De plus $a \wedge b = b \wedge r$. En itérant, le dernier reste non nul est le PGCD.

E**Exemple 1 : PGCD de 1260 et 468**

$1260 = 2 \times 468 + 324$, puis $468 = 1 \times 324 + 144$, puis $324 = 2 \times 144 + 36$, enfin $144 = 4 \times 36 + 0$. Donc $1260 \wedge 468 = 36$.

2. Théorème de Bézout**P****Bézout et Gauss**

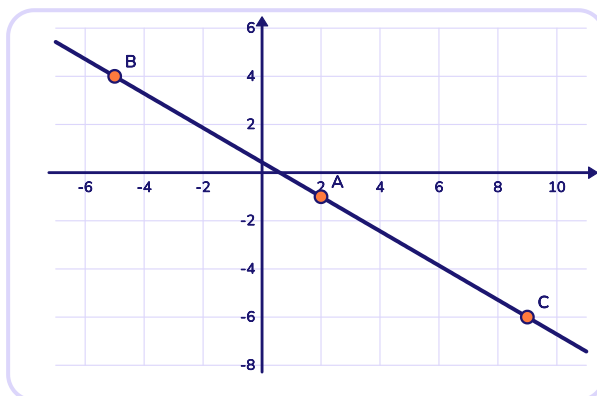
Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b$. En particulier a et b sont premiers entre eux si et seulement si $au + bv = 1$ pour certains entiers u, v . **Lemme de Gauss** : si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

M**Méthode : remonter l'algorithme d'Euclide**

1. Écrire toutes les divisions euclidiennes jusqu'au reste 1 (ou le PGCD).
2. Isoler chaque reste : $r = a - bq$.
3. Remplacer, en remontant, chaque reste par l'expression précédente.

E Exemple 2 : relation de Bézout pour 47 et 18

$47 = 2 \times 18 + 11$, $18 = 11 + 7$, $11 = 7 + 4$, $7 = 4 + 3$, $4 = 3 + 1$. En remontant :
 $1 = 4 - 3 = 2 \times 4 - 7 = 2 \times 11 - 3 \times 7 = 5 \times 11 - 3 \times 18 = 5 \times 47 - 13 \times 18$
. Vérification : $235 - 234 = 1$.



Les solutions entières de $5x + 7y = 3$ sont les points à coordonnées entières de la droite tracée ci-dessus ; elles sont régulièrement espacées.

3. Nombres premiers

D Nombre premier

Un entier $p \geq 2$ est premier si ses seuls diviseurs positifs sont **1** et **p** . Tout entier $n \geq 2$ s'écrit de façon unique, à l'ordre près, comme produit de nombres premiers.

P Infinité des nombres premiers

Il y a une infinité de nombres premiers. Démonstration : si $p_1, \dots, p_n$ étaient tous les premiers, l'entier $N = p_1 \cdots p_n + 1$ aurait un diviseur premier p_i , qui diviserait aussi $N - p_1 \cdots p_n = 1$, absurde.

E Exemple 3 : diviseurs de 360

$360 = 2^3 \times 3^2 \times 5$. Le nombre de diviseurs positifs vaut $(3 + 1)(2 + 1)(1 + 1) = 24$.

4. Congruences

D Congruence modulo n

On écrit $a \equiv b \pmod{n}$ si $n \mid a - b$. C'est une relation d'équivalence, compatible avec la somme et le produit : on peut additionner et multiplier des congruences.



P Inverse modulaire et petit théorème de Fermat

La classe de a est inversible modulo n si et seulement si $a \wedge n = 1$ (c'est Bézout). Si p est premier et $p \nmid a$, alors $a^{p-1} \equiv 1 \pmod{p}$.

E Exemple 4 : résoudre $5x \equiv 3 \pmod{17}$

Comme $5 \times 7 = 35 = 2 \times 17 + 1$, l'inverse de 5 est 7. Donc $x \equiv 7 \times 3 = 21 \equiv 4 \pmod{17}$. Contrôle : $5 \times 4 = 20 \equiv 3$.



Attention

On ne simplifie pas une congruence n'importe comment : $6 \equiv 2 \pmod{4}$ mais $3 \not\equiv 1 \pmod{4}$. Simplifier par c exige $c \wedge n = 1$.

5. Groupes



Groupe

Un groupe $(G, *)$ est un ensemble muni d'une loi interne associative, ayant un élément neutre e , et dans lequel tout élément x a un inverse x^{-1} . Il est abélien si la loi est commutative. Le nombre d'éléments est l'ordre de G .

Exemples : $(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $(\mathbb{R}_+^*, \times)$, le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des classes inversibles pour le produit. Voici la table du groupe $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$:

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

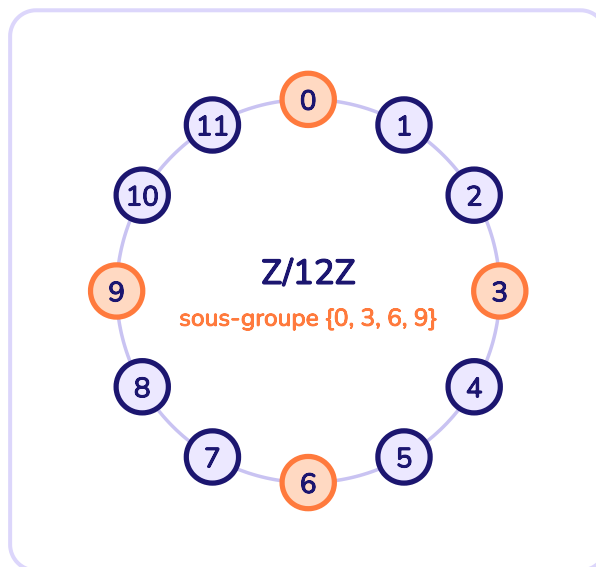
Chaque ligne et chaque colonne contiennent tous les éléments exactement une fois : c'est une propriété de toute table de groupe fini.

6. Sous-groupes

P Caractérisation d'un sous-groupe

Une partie H de G est un sous-groupe si et seulement si $e \in H$ et, pour tous $x, y \in H$, $xy^{-1} \in H$. Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$.

Théorème de Lagrange : dans un groupe fini, l'ordre d'un sous-groupe divise l'ordre du groupe.



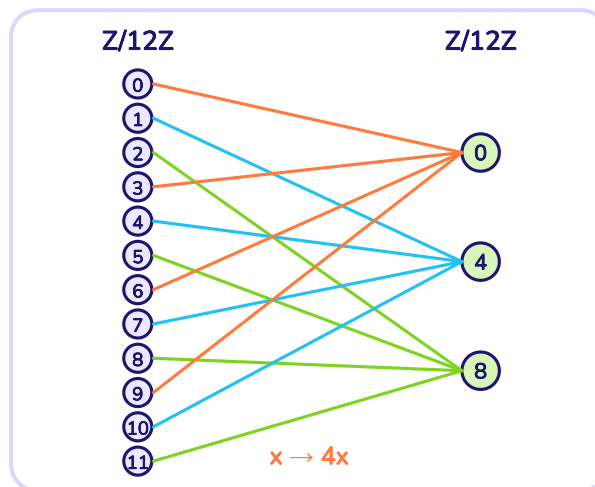
E Exemple 5 : sous-groupe engendré

Dans $(\mathbb{Z}/12\mathbb{Z}, +)$, le sous-groupe engendré par 3 est $\{0, 3, 6, 9\}$, d'ordre 4 ; et $4 \mid 12$, conformément à Lagrange.

7. Morphismes

D Morphisme de groupes

Une application $f : G \rightarrow H$ est un morphisme si $f(xy) = f(x)f(y)$ pour tous x, y . Son **noyau** est $\ker f = \{x \in G : f(x) = e_H\}$ et son **image** est $\text{Im } f = f(G)$; ce sont des sous-groupes. Alors f est injectif si et seulement si $\ker f = \{e_G\}$.



E Exemple 6 : un morphisme de $\mathbb{Z}/12\mathbb{Z}$

L'application $f(x) = 4x$ est un morphisme additif de $\mathbb{Z}/12\mathbb{Z}$ dans lui-même. Son noyau est $\{0, 3, 6, 9\}$ (car $4x \equiv 0 \pmod{12}$ équivaut à $3 \mid x$) et son image est $\{0, 4, 8\}$. On vérifie $4 \times 3 = 12$: l'ordre du noyau multiplié par celui de l'image vaut l'ordre du groupe.

8. Anneaux et corps

D

Anneau, corps

Un anneau $(A, +, \times)$ est un groupe abélien pour $+$, muni d'un produit associatif, distributif sur $+$, avec un élément neutre **1**. Un **corps** est un anneau commutatif où $1 \neq 0$ et où tout élément non nul est inversible.

P

Quand $\mathbb{Z}/n\mathbb{Z}$ est-il un corps ?

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier. Dans le cas contraire, il possède des diviseurs de zéro : par exemple dans $\mathbb{Z}/12\mathbb{Z}$, $3 \times 4 = 12 \equiv 0$ alors que $3 \neq 0$ et $4 \neq 0$.

!

Le conseil de Zyro

Pour savoir si une classe est inversible modulo n , calcule d'abord son PGCD avec n : si c'est 1, l'algorithme d'Euclide remonté te donne directement l'inverse.

À retenir

- $a \wedge b$ s'obtient par l'algorithme d'Euclide ; Bézout donne $au + bv = a \wedge b$.
- Gauss : $a \mid bc$ et $a \wedge b = 1$ entraînent $a \mid c$.
- Tout entier ≥ 2 se décompose de façon unique en nombres premiers.
- a est inversible modulo n si et seulement si $a \wedge n = 1$; Fermat : $a^{p-1} \equiv 1 \pmod{p}$.
- Sous-groupe : $e \in H$ et $xy^{-1} \in H$; Lagrange : l'ordre de H divise celui de G .
- Un morphisme est injectif si et seulement si son noyau est trivial.
- $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Le livre de cours de maths Licence L1

Tout le programme en un seul PDF de 99 pages, à imprimer ou à garder sur ta tablette.

Voir le livre

Zyro te conseille la suite

 Exercices de maths

 Contrôles de maths

Arithmétique et structures : exercices de maths Licence L1

Arithmétique et structures : contrôle de maths Licence L1

 **QCM de maths**

Arithmétique et structures : QCM de maths Licence L1

 **Exercices de maths**

Espaces vectoriels : exercices de maths Licence L1

 **Exercices de maths**

Applications linéaires et matrices : exercices de maths Licence L1

 **Contrôles de maths**

Espaces vectoriels : contrôle de maths Licence L1

Zyro vous emmène sur nos sites partenaires

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

Décollage