

# Groupes et anneaux I — TDs

Ivan Lejeune

11 décembre 2024

## Table des matières

TD1 — Rappels d'arithmétique des entiers . . . . .	2
Exercices en TD . . . . .	2
Exercices supplémentaires et approfondissement . . . . .	4
TD2 — Etude de $\mathbb{Z}/n\mathbb{Z}$ . . . . .	7
Exercices en TD . . . . .	7
TD3 — Introduction à la théorie des groupes . . . . .	12
Exercices en TD . . . . .	12
TD4 — Introduction à la théorie des anneaux et des corps . . . . .	21
Exercices en TD . . . . .	21

## TD1 — Rappels d'arithmétique des entiers

### Exercices en TD

**Exercice 1.1.** Résoudre les exercices du chapitre 1 du poly.

**Exercice 1.** Pour  $n \in \mathbb{Z}$ , quand a-t-on  $1|n$  ?  $n|1$  ?  $0|n$  ?  $n|0$  ?

**Solution.** Pour prouver que  $a|b$ , on cherche  $k \in \mathbb{Z}$  tel que  $b = ak$ .

- Pour  $k = n$ , on a  $1 \times k = n$  pour tout  $n \in \mathbb{Z}$ . On a donc toujours  $1|n$ .
- Si  $n \notin \{1, -1\}$  alors on n'a pas  $n|1$ . On a donc  $n|1 \iff n \in \{1, -1\}$ .
- L'unique solution à  $0|n$  est  $n = 0$ . On a donc  $0|n \iff n = 0$ .
- Pour  $k = 0$ , on a  $n \times k = 0$  pour tout  $n \in \mathbb{Z}$ . On a donc toujours  $n|0$ .

**Exercice 2.** Calculer la division euclidienne de 1767 par 18.

**Solution.**  $1767 = 98 \times 18 + 3$ .

**Exercice 3.** Pour quels entiers  $k$  a-t-on  $k^2 \equiv 2 \pmod{6}$  ?

**Solution.** Il suffit de traiter les cas pour  $k \equiv i \pmod{6}$  pour  $i \in \llbracket 0, 5 \rrbracket$ .

	$k^2 \equiv \dots \pmod{6}$
$k \equiv 0 \pmod{6}$	0
$k \equiv 1 \pmod{6}$	1
$k \equiv 2 \pmod{6}$	4
$k \equiv 3 \pmod{6}$	$9 \equiv 3$
$k \equiv 4 \pmod{6}$	$16 \equiv 4$
$k \equiv 5 \pmod{6}$	$25 \equiv 1$

Il n'y a aucun entier  $k \in \mathbb{Z}$  tel que  $k^2 \equiv 2 \pmod{6}$ .

**Exercice 4.** Soient deux entiers naturels  $m, n$ . Montrer qu'on a l'équivalence :

$$m\mathbb{Z} \subset n\mathbb{Z} \iff n|m$$

**Solution.** Commençons par réécrire les ensembles comme :

$$m\mathbb{Z} = \{mk, k \in \mathbb{Z}\}, \quad n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}$$

Montrons le sens direct  $m\mathbb{Z} \subset n\mathbb{Z} \implies n|m$  :

Si on a  $m\mathbb{Z} \subset n\mathbb{Z}$  alors tout  $mk \in m\mathbb{Z}$  peut s'écrire comme élément de  $n\mathbb{Z}$ . Cela revient à dire que pour tout  $mk \in m\mathbb{Z}$ , il existe  $k' \in \mathbb{Z}$  tel que  $mk = nk'$ . En particulier, pour  $k = 1$  on a un  $k' \in \mathbb{Z}$  tel que  $m = nk'$ , soit que  $n|m$ .

Montrons le sens indirect  $n|m \implies m\mathbb{Z} \subset n\mathbb{Z}$ .

Si  $n|m$  alors il existe  $k \in \mathbb{Z}$  tel que  $nk = m$ . Alors, pour tout  $k' \in \mathbb{Z}$ , on a  $mk' = nk'k \in n\mathbb{Z}$ . Ainsi, on a  $m\mathbb{Z} \subset n\mathbb{Z}$ .

**Exercice 5.** Pour  $a \in \mathbb{Z}$ , que vaut  $a \wedge 0$  ?  $a \wedge 1$  ?

**Solution.** Le plus grand diviseur à la fois de  $a$  et 0 est  $a$ .

Le plus grand diviseur à la fois de  $a$  et 1 est 1.

**Exercice 6.** Montrer que pour  $a, b \in \mathbb{Z}$  on a :

$$a \wedge b = 1 \iff \text{il n'existe aucun nombre premier } p \text{ qui divise à la fois } a \text{ et } b$$

**Solution.** Commençons par montrer le sens indirect "il n'existe aucun nombre premier  $p$  qui divise à la fois  $a$  et  $b$ "  $\implies a \wedge b = 1$  :  
Réécrivons  $a$  et  $b$  comme suit :

$$a = 1 \times \prod_i p_i^{q_i}, \quad b = 1 \times \prod_j p_j^{q_j}$$

Comme tous les  $p_i$  sont différents de tous les  $p_j$  par hypothèse, on a forcément  $a \wedge b = 1$ .

Montrons maintenant le sens direct :

Supposons qu'il existe  $p$  premier qui divise à la fois  $a$  et  $b$ . Alors, par propriété du PGCD,  $p$  divise aussi le PGCD de  $a$  et  $b$ , soit 1. C'est impossible car  $p > 1$ .

Alors  $a \wedge b = 1 \implies$  il n'existe aucun nombre premier  $p$  qui divise à la fois  $a$  et  $b$ .

**Exercice 7.** Utiliser l'algorithme d'Euclide pour calculer le PGCD de 1071 et 1029

**Solution.**

$$\begin{array}{rcl} 1071 & = & 1 \times 1029 + 42 \\ 1029 & = & 24 \times 42 + 21 \\ 42 & = & 2 \times 21 + 0 \end{array}$$

**Exercice 8.** Pour  $a \in \mathbb{Z}$ , que vaut  $a \vee 0$  ?  $a \vee 1$  ?

**Solution.** Le PPCM de  $a$  et 0 vaut 0 car 0 est l'unique multiple de 0.

Le PPCM de  $a$  et 1 vaut  $a$  car pour tout  $m \in \mathbb{N}$ , si  $a|m$  alors  $1|m$ .

**Exercice 9.** Soient  $u, a, b \in \mathbb{Z}$ . Montrer qu'on a l'équivalence :

$$u \wedge (ab) = 1 \iff (u \wedge a = 1 \text{ et } u \wedge b = 1)$$

**Solution.** Montrons le sens direct d'abord :

Réécrivons  $ab$  comme  $\prod_i p_i^{q_i}$ . Comme  $u \wedge (ab) = 1$ , aucun des facteurs  $p_i$  ne divise  $u$ . Ainsi, comme  $a$  et  $b$  ne possèdent aucun facteur autre que les  $p_i$ ,  $u \wedge a = u \wedge b = 1$ .

De la même manière pour le sens indirect :

Comme  $u \wedge a = u \wedge b = 1$ ,  $u$  ne possède aucun facteur premier en commun ni avec  $a$  ni avec  $b$ . Ainsi  $ab$  qui ne possède que des facteurs de  $a$  et  $b$  ne possède aucun facteur premier en commun avec  $u$ . Donc  $u \wedge (ab) = 1$ .

**Exercice 10.** Calculer les décompositions en produit de nombres premiers de 504 et 1540 et en déduire  $504 \wedge 1540$  et  $504 \vee 1540$ .

**Solution.** On a

$$\begin{array}{ll} 504 & = 2 \times 252 \\ & = 2 \times 2 \times 126 \\ & = 2^2 \times 2 \times 63 \\ & = 2^3 \times 7 \times 9 \\ & = 2^3 \times 3^2 \times 7 \end{array} \quad \begin{array}{ll} 1540 & = 2 \times 770 \\ & = 2 \times 2 \times 385 \\ & = 2^2 \times 5 \times 77 \\ & = 2^2 \times 5 \times 7 \times 11 \end{array}$$

On a alors clairement  $504 \wedge 1540 = 2^2 \times 7 = 28$  et  $504 \vee 1540 = 2^3 \times 3^2 \times 5 \times 7 \times 11 = 27720$ .

On peut vérifier qu'on a bien  $28 \times 27720 = 776160 = 504 \times 1540$ .

**Exercice 11.** Utiliser l'algorithme d'Euclide étendu pour calculer le PGCD de 186 et 309 et trouver une relation de Bézout entre ces deux nombres.

**Exercice 12.** Montrer que 14 est inversible modulo 31 et en calculer un inverse. Pour quels entiers  $x$  a-t-on  $14x \equiv 2 \pmod{31}$  ?

**Exercice 1.2.** Résoudre pour  $x \in \mathbb{Z}$  :

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 7 \pmod{12} \end{cases}$$

**Solution.** On a  $x \equiv 3 \pmod{5}$  qui nous donne “ $x$  finit par 3 ou 8”.  
On calcule alors les valeurs de  $x$  qui vérifient  $x \equiv 7 \pmod{12}$ .

$$\begin{aligned} x &\equiv 7 \pmod{12} \\ &\equiv 7 + 12 = 19 \pmod{12} \\ &\equiv 7 + 24 = 31 \pmod{12} \\ &\equiv 7 + 36 = 43 \pmod{12} \end{aligned}$$

Une solution particulière est donc  $x = 43$ .

Comme  $5 \wedge 12 = 1$ , d’après le théorème chinois, l’ensemble des solutions est :

$$S = \{43 + 60k, k \in \mathbb{Z}\}$$

**Exercice 1.3 Congruences.** Résoudre pour  $x \in \mathbb{Z}$  :

$$12x \equiv 9 \pmod{21} \quad \text{puis} \quad 12x \equiv 11 \pmod{21}$$

**Exercice 1.4 Relations de Bézout.** Soit  $a, b \in \mathbb{Z}$  tels que  $a \wedge b = 1$  et soit  $au + bv = 1$  une relation de Bézout avec  $u, v \in \mathbb{Z}$ .

- 1) Soit  $k \in \mathbb{Z}$  et posons  $u' = u - kb$  et  $v' = v + ka$ . Montrer qu’on a la relation de Bézout :  
 $au' + bv' = 1$ .
- 2) Montrer que toutes les relations de Bézout pour  $a, b$  sont de cette forme.

## Exercices supplémentaires et approfondissement

**Exercice 1.5 Inversibilité modulo un entier.** Est-ce que 18 est inversible modulo 49 ? Si oui, en calculer un inverse. Mêmes questions avec 42 modulo 135.

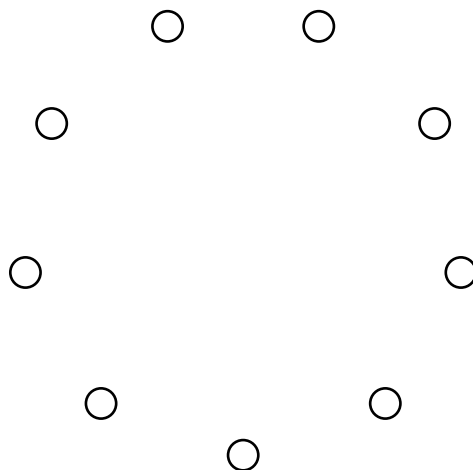
**Exercice 1.6 Cubes.** Soient  $a, b \in \mathbb{N}^*$  premiers entre eux, tels que le produit  $ab$  est un cube (c’est-à-dire s’écrit  $n^3$  pour un  $n \in \mathbb{N}$ ). Montrer que  $a$  et  $b$  sont tous les deux des cubes.

**Exercice 1.7 Racine.** Soit  $n \in \mathbb{N}$  qui n’est pas le carré d’un entier. Montrer que  $\sqrt{n}$  est irrationnel.

**Exercice 1.8 De gros gros nombres.**

- 1) Quels sont les restes des divisions euclidiennes de  $10^{100}$  par 13 et 19 ?
- 2) Quel est le reste de la division euclidienne de  $10^{100}$  par  $247 = 13 \times 19$  ? En déduire que  $10^{99} + 1$  est divisible par 247.

**Exercice 1.9 Le petit théorème de Fermat pour les enfants.** Soit un entier  $n \in \mathbb{N}^*$ . On considère  $n$  petits disques répartis uniformément sur un cercle comme sur la figure suivante (avec  $n = 9$ ). On considère un entier  $a \in \mathbb{N}$  et on imagine qu’on dispose de  $a$  couleurs différentes. Un **coloriage** est une façon d’assigner une des  $a$  couleurs à chaque disque.



- 1) Combien y a-t-il de coloriage différents ?
- 2) Soit  $C$  un coloriage. On obtient d'autres coloriage en faisant tourner  $C$  d'un angle multiple de  $2\pi/n$ . Soit  $k$  le nombre de coloriage *différents* qu'on obtient ainsi. Montrer que  $k$  est un diviseur de  $n$ . Combien y a-t-il de coloriage pour lesquels  $k = 1$  ?
- 3) Supposons maintenant que  $n = p$  est un nombre premier. Dédurre des questions précédentes que  $p$  divise  $a^p - a$ .

**Exercice 1.10 Coefficients binomiaux.** Soit un entier  $n \geq 2$ . Montrer que si  $n$  divise tous les coefficients binomiaux  $\binom{n}{k}$  avec  $0 < k < n$  alors  $n$  est premier.

**Exercice 1.11.** Un **triplet pythagoricien** est un triplet  $(a, b, c)$  d'entiers naturels non nuls qui vérifient l'équation :

$$a^2 + b^2 = c^2$$

Dit autrement, par le théorème de Pythagore,  $a$ ,  $b$ ,  $c$  sont les longueurs des côtés d'un triangle rectangle. Le triplet pythagoricien le plus connu est  $(3, 4, 5)$ .

- 1) Soit  $(a, b, c)$  un triplet pythagoricien et  $k \in \mathbb{N}^*$ . Montrer que  $(ka, kb, kc)$  est aussi un triplet pythagoricien.

Dans tout l'exercice on dira qu'un triplet pythagoricien  $(a, b, c)$  est **primitif** s'il n'existe aucun entier  $k \geq 2$  qui divise à la fois  $a$ ,  $b$  et  $c$  (ou dit autrement, si  $a \wedge b \wedge c = 1$ ).

**Les 3 parties de l'exercice sont indépendantes**

**Partie 1 La formule d'Euclide.** Soient deux entiers  $m, n$  avec  $m > n \geq 1$ . On pose

$$(*) \quad a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

- 2) Montrer que  $(a, b, c)$  est un triplet pythagoricien.
- 3) On suppose que  $m$  et  $n$  sont de parités différentes (c'est-à-dire que l'un est pair et l'autre impair) et premiers entre eux.
  - a) Déterminer la parité de  $a$ , de  $b$ , de  $c$ .
  - b) Montrer qu'il n'existe aucun nombre premier  $p$  qui divise à la fois  $a$  et  $c$ .
  - c) En déduire que  $(a, b, c)$  est un triplet pythagoricien primitif.

**Partie 2 Intermède.**

- 4) Soient deux entiers  $x, y \in \mathbb{N}^*$  tels que  $x \wedge y = 1$  et tels que le produit  $xy$  est le carré d'un entier. Montrer que  $x$  et  $y$  sont des carrés d'entiers.

**Partie 3 Classification des triplets pythagoriciens.** Soit  $(a, b, c)$  un triplet pythagoricien primitif.

- 5) Montrer que  $a \wedge c = 1$ .
- 6) Pour un entier  $k$ , quels sont les restes possibles pour  $k^2$  dans la division euclidienne par 4 ? On justifiera.
- 7) Dédire de la question précédente que  $a$  et  $b$  sont de parités différentes, puis que  $c$  est impair.
- 8) Quitte à échanger les rôles joués par  $a$  et  $b$  on peut supposer que  $a$  est impair et que  $b$  est pair, ce qu'on fait maintenant. Montrer que  $(c - a) \wedge (c + a) = 2$ .
- 9) Montrer que le produit de  $\frac{c+a}{2}$  et  $\frac{c-a}{2}$  est un carré, et déduire de la question 4) qu'il existe des entiers  $m, n$  avec  $m > n \geq 1$  tels que  $(a, b, c)$  est de la forme  $(*)$ .
- 10) Parmi les triangles rectangles dont les 3 côtés sont de longueurs entières, déterminer tous ceux qui ont un côté de longueur 17.

## TD2 — Etude de $\mathbb{Z}/n\mathbb{Z}$

### Exercices en TD

**Exercice 2.1 En cercle.** Soit  $n \in \mathbb{N}^*$ . On note

$$\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

l'ensemble des racines  $n$ -ièmes de l'unité. Montrer que l'application

$$\begin{aligned} f: \mathbb{Z} &\rightarrow \mathbb{U}_n \\ k &\mapsto \exp\left(\frac{2ik\pi}{n}\right) \end{aligned}$$

passse au quotient par la relation de congruence modulo  $n$  et induit l'application

$$\begin{aligned} g: \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{U}_n \\ \bar{k} &\mapsto \exp\left(\frac{2ik\pi}{n}\right). \end{aligned}$$

Montrer que  $g$  est bijective.

**Solution.** On a  $g$  bijective par construction.

**Exercice 2.2 Inversibles.** Faire la liste des éléments inversibles de  $\mathbb{Z}/14\mathbb{Z}$  et calculer leurs inverses. Même chose avec  $\mathbb{Z}/20\mathbb{Z}$ .

**Solution.** Pour  $\mathbb{Z}/14\mathbb{Z}$ , les inversibles sont les éléments qui ne divisent pas 14, soit :

$$\{\bar{1}, \bar{3}, \bar{5}, \bar{9}, \bar{11}, \bar{13}\} \text{ ou } \{\bar{1}, \bar{3}, \bar{5}, \bar{-5}, \bar{-3}, \bar{-1}\}$$

On a donc :

$$\begin{aligned} 1^{-1} &\equiv 1 \pmod{14} \\ 3^{-1} &\equiv 5 \pmod{14} \\ 5^{-1} &\equiv 3 \pmod{14} \\ -5^{-1} &\equiv -3 \pmod{14} \\ -3^{-1} &\equiv -5 \pmod{14} \\ -1^{-1} &\equiv -1 \pmod{14} \end{aligned}$$

Pour  $\mathbb{Z}/20\mathbb{Z}$ , les inversibles sont les éléments qui ne divisent pas 20, soit :

$$\{\bar{1}, \bar{3}, \bar{7}, \bar{9}, \bar{11}, \bar{13}, \bar{17}, \bar{19}\} \text{ ou } \{\bar{1}, \bar{3}, \bar{7}, \bar{9}, \bar{-9}, \bar{-7}, \bar{-3}, \bar{-1}\}$$

On a donc :

$$\begin{aligned} 1^{-1} &\equiv 1 \pmod{20} \\ 3^{-1} &\equiv 7 \pmod{20} \\ 7^{-1} &\equiv 3 \pmod{20} \\ 9^{-1} &\equiv 9 \pmod{20} \\ -9^{-1} &\equiv 9 \pmod{20} \\ -7^{-1} &\equiv -3 \pmod{20} \\ -3^{-1} &\equiv -7 \pmod{20} \\ -1^{-1} &\equiv -1 \pmod{20} \end{aligned}$$

**Exercice 2.3 Puissance.** On se place dans  $\mathbb{Z}/41\mathbb{Z}$ . Calculer  $\bar{2}^{2023}$

**Solution.** Comme 41 est premier, 2 est inversible dans  $\mathbb{Z}/41\mathbb{Z}$ . Par le petit théorème de Fermat, on a

$$2^{40} \equiv 1 \pmod{41}$$

On a donc

$$2^{2023} = 2^{50 \times 40 + 23} = (2^{40})^{50} \times 2^{23} \equiv 2^{23} \pmod{41}$$

Pour calculer  $2^{23}$ , on utilise la méthode piétonne :

$$\bar{2}^1 = \bar{2}$$

$$\bar{2}^2 = \bar{4}$$

$$\bar{2}^3 = \bar{8}$$

$$\bar{2}^4 = \overline{16}$$

$$\bar{2}^5 = \overline{32}$$

$$\bar{2}^6 = \overline{23}$$

$$\bar{2}^7 = \bar{5}$$

$$\bar{2}^8 = \overline{10}$$

$$\bar{2}^9 = \overline{20}$$

$$\bar{2}^{10} = \overline{40}$$

On en conclut alors que  $\bar{2}^{20} = \bar{1}$  et alors

$$\bar{2}^{2023} = \bar{2}^{23} = \bar{2}^3 = \bar{8}$$

**Exercice 2.4 Sous-groupes.** Quels sous-groupes de  $\mathbb{Z}/1000\mathbb{Z}$  contiennent  $\overline{120}$  ?

**Solution.** Les sous-groupes de  $\mathbb{Z}/1000\mathbb{Z}$  sont les  $\langle \bar{d} \rangle$  avec  $d \in \mathbb{N}^*$  un diviseur de 1000.

On sait que  $1000 = 2^3 5^3$ . Alors, les diviseurs positifs de 1000 sont les  $2^a 5^b$  avec  $a, b \in \{0, 1, 2, 3\}$ .

Or

$$\langle \bar{d} \rangle = \{ \bar{0}, \bar{d}, \bar{2d}, \dots, \overline{(e-1)d} \}$$

avec  $e = \frac{1000}{d}$ . Donc

$$\begin{aligned} \overline{120} \in \langle \bar{d} \rangle &\iff 120 \in \{0, d, 2d, \dots, (e-1)d\} \\ &\iff d \mid 120 \end{aligned}$$

On sait que  $d$  divise 1000 et 120 donc il divise  $1000 \wedge 120 = 40$ .

On a donc les sous-groupes de  $\mathbb{Z}/1000\mathbb{Z}$  contenant  $\overline{120}$  sont

$$\langle \bar{1} \rangle, \langle \bar{2} \rangle, \langle \bar{4} \rangle, \langle \bar{5} \rangle, \langle \bar{8} \rangle, \langle \bar{10} \rangle, \langle \bar{20} \rangle, \langle \bar{40} \rangle$$

**Exercice 2.5 Théorème de Wilson.** Le but de cet exercice est de démontrer le théorème de Wilson : pour un entier  $n \geq 2$ , on a :

$$n \text{ est premier} \iff (n-1)! \equiv -1 \pmod{n}$$

1. Soit  $p$  un nombre premier.

(a) Quels éléments  $x \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{\bar{0}\}$  sont égaux à leur inverse ?



(b) En calculant le produit de tous les éléments de  $(\mathbb{Z}/p\mathbb{Z}) \setminus \{\bar{0}\}$ , montrer qu'on a :

$$(p-1)! \equiv -1 \pmod{p}$$

2. Soit  $n$  un nombre composé. Montrer que :

$$(n-1)! \not\equiv -1 \pmod{n}$$

En déduire le théorème de Wilson.

### Solution.

1. Soit  $p$  un nombre premier.

(a) Soit  $x \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{\bar{0}\}$ . On a :

$$\begin{aligned} x = x^{-1} &\iff x^2 = \bar{1} \\ &\iff x^2 - \bar{1} = \bar{0} \\ &\iff (x - \bar{1})(x + \bar{1}) = \bar{0} \\ &\iff x - \bar{1} = \bar{0} \text{ ou } x + \bar{1} = \bar{0} \text{ (car } p \text{ est premier)} \\ &\iff x = \bar{1} \text{ ou } x = \overline{-1} \end{aligned}$$

Conclusion : les  $x \in \mathbb{Z}/p\mathbb{Z}$  égaux à leur inverse sont  $\bar{1}$  et  $\overline{-1}$ .

(b) Dans le produit :

$$\bar{1} \times \bar{2} \times \dots \times \overline{p-1}$$

tous les éléments se simplifient avec leur inverse par paires *sauf* les éléments égaux à leur propre inverse.

Par la question précédente, on a donc :

$$\bar{1} \times \bar{2} \times \dots \times \overline{p-1} = \bar{1} \times \overline{-1} = \overline{-1}$$

On en déduit :

$$(p-1)! \equiv -1 \pmod{p}$$

2. Soit  $n$  un nombre composé.

On procède par l'absurde. Supposons que  $(n-1)! \equiv -1 \pmod{n}$ .

Il existe donc  $k \in \mathbb{Z}$  tel que :

$$(n-1)! = kn - 1$$

On en déduit que :

$$kn - (n-1)! = 1 \tag{1}$$

Comme  $n$  est composé, on peut écrire  $n = ab$  avec  $1 < a, b < n$ .

Comme  $a|(n-1)!$ , on peut voir (1) comme une relation de Bézout entre  $n$  et  $a$  qui montre que  $n \wedge a = 1$ , ce qui est absurde car  $n \wedge a = a \neq 1$ .

Autre raisonnement :

On écrit  $n = ab$  avec  $1 < a, b < n$ .

▷ Cas 1 :  $a \neq b$

Dans ce cas, on voit apparaître  $a$  et  $b$  à des places différentes dans le produit  $(n-1)!$  et donc  $ab$  divise  $(n-1)!$ . Alors  $(n-1)! \equiv 0 \pmod{n}$ .

▷ Cas 2 :  $a = b$ , soit  $n = a^2$ .

Dans ce cas, on voit apparaître  $a$  et  $2a$  à des places différentes dans le produit  $(n-1)!$  (à condition que  $a > 2$ ) et donc  $a^2$  divise  $(n-1)!$ . Alors  $(n-1)! \equiv 0 \pmod{n}$ .

Si  $a = 2$ , on a  $n = 4$  et alors  $(3)! = 6 \not\equiv -1 \pmod{4}$ .

**Exercice 2.6 Une formule de Gauss.** Soit un entier  $n \in \mathbb{N}^*$ . On veut montrer qu'on a :

$$\sum_{d|n} \varphi(d) = n$$

1. Vérifier que la formule est vraie pour  $n = 12$ .
2. Soit  $d$  un diviseur de  $n$ . On note  $e = \frac{n}{d}$ . Montrer qu'il y a  $\varphi(e)$  entiers  $a \in \{1, \dots, n\}$  tels que  $a \wedge n = d$ .
3. Conclure.

**Solution.** 1. Pour  $n = 12$ , on a :

$$\begin{aligned} \sum_{d|12} \varphi(d) &= \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) \\ &= 1 + 1 + 2 + 2 + 2 + 4 \\ &= 12 \end{aligned}$$

Donc la formule est vraie pour  $n = 12$ .

2. Pour  $a \in \{1, \dots, n\}$  tel que  $a \wedge n = d$ , on a  $d | a$  et donc il existe un entier  $k$  tel que  $a = kd$ . Alors, on a

$$(kd) \wedge (ed) = d$$

d'où  $k \wedge e = 1$ .

De plus, comme  $a \in \{1, \dots, n\}$ , on a nécessairement  $k \in \{1, \dots, e\}$ .

On a montré que :

$$(a \in \{1, \dots, n\} \mid a \wedge n = d) \implies (\exists k \in \{1, \dots, e\} \mid k \wedge e = 1, a = kd)$$

La réciproque ( $\Leftarrow$ ) est aussi vraie, il suffit de faire le même raisonnement.

Il y a donc autant d'entiers  $a \in \{1, \dots, n\}$  tels que  $a \wedge n = d$  que d'entiers  $k \in \{1, \dots, e\}$ .

Or, il y a  $\varphi(e)$  entiers  $k \in \{1, \dots, e\}$  tels que  $k \wedge e = 1$ .

Alors, il y a  $\varphi(e)$  entiers  $a \in \{1, \dots, n\}$  tels que  $a \wedge n = d$ .

3. On partitionne l'ensemble  $\{1, \dots, n\}$  suivant le pgcd avec  $n$ , ce pgcd est alors un diviseur  $d$  de  $n$ .

On a donc :

$$\{1, \dots, n\} = \bigsqcup_{d|n} \{a \in \{1, \dots, n\} \mid a \wedge n = d\}$$

Par le point précédent, on sait que les ensembles  $\{a \in \{1, \dots, n\} \mid a \wedge n = d\}$  sont disjoints et leur réunion est  $\{1, \dots, n\}$ .

On peut réécrire cette somme dans un autre ordre en utilisant l'involution  $d \mapsto \frac{n}{d}$  de l'ensemble des diviseurs de  $n$ . On obtient :


$$\sum_{d|n} \varphi(d) = n$$

## Exercices supplémentaires, et approfondissement

**Exercice 2.7 Equations.**

1. Résoudre dans  $\mathbb{Z}/37\mathbb{Z}$  l'équation  $\overline{7}x + \overline{5} = \overline{1}$ .
2. Résoudre dans  $\mathbb{Z}/37\mathbb{Z}$  l'équation  $x^2 - \overline{6}x + \overline{10} = \overline{0}$ .

**Exercice 2.8 Un exercice de baccalauréat (filière C, académie de Paris, juin 1978).** Dans l'anneau  $\mathbb{Z}/91\mathbb{Z}$  (dont les éléments sont notés  $\overline{0}, \overline{1}, \dots, \overline{90}$ ),

- 
1. discuter, suivant la valeur du paramètre  $a \in \mathbb{Z}/91\mathbb{Z}$ , l'équation

$$ax = \bar{0}$$

2. résoudre l'équation

$$x^2 + \bar{2}x - \bar{3} = \bar{0}$$

## TD3 — Introduction à la théorie des groupes

### Exercices en TD

**Exercice 3.1 Groupes.** Ces choses-ci sont-elles des groupes ?

- $(2\mathbb{Z}, +)$
- $(2\mathbb{Z}, \times)$
- L'ensemble des fonctions de  $[0, 1]$  dans  $\mathbb{R}$ , muni de l'addition des fonctions.
- L'ensemble des fonctions continues de  $[0, 1]$  dans  $\mathbb{R}$ , muni de l'addition des fonctions.
- L'ensemble des matrices  $n \times n$  inversibles et à coefficients entiers, muni du produit matriciel.
- L'ensemble des parties d'un ensemble  $E$ , muni de l'union.
- L'ensemble des permutations  $\sigma \in \mathfrak{S}_6$  telles que  $\sigma^2 = \text{Id}$ , muni de la composition.

**Solution.**

- $(2\mathbb{Z}, +)$  est un groupe car :
  - Il est non vide :  $0 \in 2\mathbb{Z}$ .
  - Il est stable par l'addition : si  $a, b \in 2\mathbb{Z}$ , alors  $a + b \in 2\mathbb{Z}$ .
  - Il est stable par l'opposé : si  $a \in 2\mathbb{Z}$ , alors  $-a \in 2\mathbb{Z}$ .
- $(2\mathbb{Z}, \times)$  n'est pas un groupe car  $0 \notin 2\mathbb{Z}$ .
- L'ensemble des fonctions de  $[0, 1]$  dans  $\mathbb{R}$ , muni de l'addition des fonctions, est un groupe.
- L'ensemble des fonctions continues de  $[0, 1]$  dans  $\mathbb{R}$ , muni de l'addition des fonctions, est un groupe.
- L'ensemble des matrices  $n \times n$  inversibles et à coefficients entiers, muni du produit matriciel, n'est pas un groupe car l'inverse d'une matrice à coefficients entiers n'est pas forcément à coefficients entiers.
- L'ensemble des parties d'un ensemble  $E$ , muni de l'union, n'est pas un groupe car il n'est pas stable par l'opposé.
- L'ensemble des permutations  $\sigma \in \mathfrak{S}_6$  telles que  $\sigma^2 = \text{Id}$ , muni de la composition, n'est un groupe car il n'est pas commutatif.

**Exercice 3.2 Tarte à la crème.** Soit  $G$  un groupe tel que tout  $x \in G$  vérifie  $x^2 = e$ . Démontrer que  $G$  est abélien.

**Solution.** On veut montrer que pour tout  $x, y \in G$ ,  $xy = yx$ . Soient  $x, y \in G$ . Alors :

$$\begin{aligned}(xy)^2 = e &\implies xyxy = e \\ &\implies xyxyy = y \\ &\implies xyx = y \\ &\implies xyxx = yx \\ &\implies xy = yx\end{aligned}$$

Comme  $(xy)^2 = e$ , on a bien  $xy = yx$ .

**Exercice 3.3 Petits groupes.** Déterminer toutes les tables de multiplication possibles pour des groupes d'ordre  $\leq 5$ . (On se gardera d'utiliser le théorème de Lagrange.)

- Vous devez trouver (au nom des éléments près) un seul groupe d'ordre 1, un seul d'ordre 2, un seul d'ordre 3, deux de l'ordre 4 et un seul d'ordre 5.
- Remarquez que tous ces groupes sont abéliens.

**Solution.** On va dresser les tables de multiplication pour les groupes d'ordre 1, 2, 3, 4 et 5. On peut retrouver ces tables à partir des "règles de sudoku".

- Pour l'ordre 1, il n'y a qu'un groupe :  $\{e\}$ , de table :

×	e
e	e

- Pour l'ordre 2, il n'y a qu'un groupe :  $\{e, a\}$ , de table :

×	e	a
e	e	a
a	a	e

- Pour l'ordre 3, il n'y a qu'un groupe :  $\{e, a, b\}$ , de table :

×	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

- Pour l'ordre 4, il y a deux groupes :

×	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

et

×	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

- Pour l'ordre 5, il y a un seul groupe :

×	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

**Exercice 3.4 Sous-groupes.** Lister tous les sous-groupes du groupe symétrique  $\mathfrak{S}_3$ .

**Solution.** Commençons par expliciter tous les éléments de  $\mathfrak{S}_3$  :

$$\mathfrak{S}_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

Les sous-groupes de  $\mathfrak{S}_3$  sont :

- Les groupes triviaux :
  - $\{e\}$ , le groupe trivial.
  - $\mathfrak{S}_3$ , le groupe symétrique.
- Les sous-groupes engendrés par un élément :
  - $\langle (1\ 2) \rangle = \{e, (1\ 2)\}$ ,
  - $\langle (1\ 3) \rangle = \{e, (1\ 3)\}$ ,
  - $\langle (2\ 3) \rangle = \{e, (2\ 3)\}$ ,
  - $\langle (1\ 2\ 3) \rangle = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ ,
  - $\langle (1\ 3\ 2) \rangle = \langle (1\ 2\ 3) \rangle$ .
- Les sous-groupes engendrés par plus d'un élément engendrent tout le groupe.

**Exercice 3.5 24 heures chrono (contrôle continu 2023–2024).**

1. Montrer que le groupe  $\mathbb{Z}/24\mathbb{Z}$  a autant de générateurs que de sous-groupes. Faire la liste des générateurs. Faire la liste des sous-groupes, en décrivant chaque sous-groupe de la manière la plus explicite possible.
2. Montrer que le groupe  $(\mathbb{Z}/24\mathbb{Z})^\times$  peut être engendré par 3 de ses éléments.
3. Lister les sous-groupes d'ordre 2 du groupe  $(\mathbb{Z}/24\mathbb{Z})^\times$ .
4. Donner un exemple de sous-groupe d'ordre 4 du groupe  $(\mathbb{Z}/24\mathbb{Z})^\times$ . (Bonus : lister tous les sous-groupes d'ordre 4 de  $(\mathbb{Z}/24\mathbb{Z})^\times$ .)

**Solution.**

1. Les générateurs de  $\mathbb{Z}/24\mathbb{Z}$  sont exactement :

$$\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{17}, \bar{19}, \bar{23}$$

Les sous-groupes de  $\mathbb{Z}/24\mathbb{Z}$  sont :

$$\begin{aligned} \langle \bar{1} \rangle &= \mathbb{Z}/24\mathbb{Z}, \\ \langle \bar{2} \rangle &= \{\bar{0}, \bar{2}, \bar{4}, \dots, \bar{22}\}, \\ \langle \bar{3} \rangle &= \{\bar{0}, \bar{3}, \bar{6}, \dots, \bar{21}\}, \\ \langle \bar{4} \rangle &= \{\bar{0}, \bar{4}, \bar{8}, \bar{12}, \bar{16}, \bar{20}\}, \\ \langle \bar{6} \rangle &= \{\bar{0}, \bar{6}, \bar{12}, \bar{18}\}, \\ \langle \bar{8} \rangle &= \{\bar{0}, \bar{8}, \bar{16}\} \langle \bar{12} \rangle = \{\bar{0}, \bar{12}\}, \\ \langle \bar{24} \rangle &= \{\bar{0}\}. \end{aligned}$$

Il y en a autant.

2. On a

$$(\mathbb{Z}/24\mathbb{Z})^\times = \langle \bar{5}, \bar{7}, \bar{11} \rangle$$

car

$$\begin{aligned} \bar{5} \times \bar{7} &= \bar{11} \\ \bar{5} \times \bar{11} &= \bar{5} \\ \bar{7} \times \bar{11} &= \bar{7} \\ \bar{5} \times \bar{7} \times \bar{11} &= \bar{1} \end{aligned}$$

3. Un sous-groupe d'ordre 2 est de la forme

$$\langle a \rangle = \{\bar{1}, a\}$$

avec  $a \neq \bar{1}, a^2 = \bar{1}$ . Or,  $\forall a \in (\mathbb{Z}/24\mathbb{Z})^\times$ , on a  $a^2 = 1$ . Alors, les sous-groupes d'ordre 2 de  $(\mathbb{Z}/24\mathbb{Z})^\times$  sont :

$$\begin{aligned} \langle \bar{5} \rangle &= \{\bar{1}, \bar{5}\}, \\ \langle \bar{7} \rangle &= \{\bar{1}, \bar{7}\}, \\ \langle \bar{11} \rangle &= \{\bar{1}, \bar{11}\}, \\ \langle \bar{17} \rangle &= \{\bar{1}, \bar{17}\}, \\ \langle \bar{19} \rangle &= \{\bar{1}, \bar{19}\}, \\ \langle \bar{23} \rangle &= \{\bar{1}, \bar{23}\}. \end{aligned}$$

4. Un exemple de sous-groupe d'ordre 4 est

$$\langle \bar{5}, \bar{7} \rangle = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$$

**Exercice 3.6 Union de sous-groupes (contrôle continu 2023–2024).**

1. Soit  $G$  un groupe et  $H, K$  deux sous-groupes de  $G$ . Montrer que  $H \cup K$  est un sous-groupe de  $G$  si et seulement si  $H \subseteq K$  ou  $K \subseteq H$ .
2. Donner un exemple de groupe  $G$  et de trois sous-groupes  $H, K, L$  de  $G$  qui sont tous les trois différents de  $G$  et tels que  $G = H \cup K \cup L$ .

**Exercice 3.7 Morphismes de groupes ?.** Ces choses-là sont-elles des morphismes de groupes ?

1.  $f: \mathbb{Z} \rightarrow \mathbb{Z}^*, n \mapsto 2^n$ .
2.  $g: \mathbb{C}^* \rightarrow \mathbb{C}^*, z \mapsto z^3$ .
3.  $h: \mathbb{Z}/10\mathbb{Z} \rightarrow \mathbb{Z}, \bar{k} \mapsto k$ .
4.  $i: \text{GL}_2(\mathbb{R}) \rightarrow \mathbb{R}, A \mapsto \text{tr}(A)$ .
5.  $j: \mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}, \bar{k} \mapsto \tilde{k}$ .
6.  $k: \mathfrak{S}_4 \rightarrow \mathfrak{S}_4, \sigma \mapsto \sigma(1 \ 2)$ .
7.  $l: \mathfrak{S}_4 \rightarrow \mathfrak{S}_4, \sigma \mapsto (1 \ 2)\sigma(1 \ 2)$ .

**Solution.**

1.  $f$  n'est pas définie.
2.  $g$  est un morphisme de groupes car

$$g(z_1 z_2) = (z_1 z_2)^3 = z_1^3 z_2^3 = g(z_1)g(z_2).$$

3.  $h$  n'est pas définie
4.  $i$  n'est pas un morphisme de groupes car  $\text{tr}(I_2) = 2 \neq 0$ .
5.  $j$  n'est pas un morphisme de groupes car  $j(\bar{1} + \bar{2}) = \tilde{0} \neq \tilde{1} + \tilde{2} = j(\bar{1}) + j(\bar{2})$ .
6.  $k$  n'est pas un morphisme de groupes car  $k(\text{Id}) = (1 \ 2) \neq \text{Id}$ .
7.  $l$  est un morphisme de groupes car

$$\begin{aligned} l(\sigma_1 \sigma_2) &= (1 \ 2)(\sigma_1 \sigma_2)(1 \ 2) \\ &= (1 \ 2)\sigma_1(1 \ 2)(1 \ 2)\sigma_2(1 \ 2) \\ &= l(\sigma_1)l(\sigma_2). \end{aligned}$$

**Exercice 3.8 Exo 15.****Solution.**

1. Le sous groupe engendré par  $\bar{3}$  est

$$H = \{\bar{3}, \bar{9}, \bar{5}, \bar{4}, \bar{1}\}$$

et le sous-groupe engendré par  $\bar{10}$  est

$$K = \{\bar{10}, \bar{1}\}$$

On vérifie alors les trois propriétés :

(i) Si  $x \in H$ , alors le couple  $(x, \bar{1})$  convient. Sinon,  $x \in \{\bar{2}, \bar{6}, \bar{7}, \bar{8}, \bar{10}\}$ . On a alors

$$\begin{aligned} x = \bar{2} \equiv x = \bar{9}0 &\implies (\bar{9}, \bar{10}) \\ x = \bar{6} \equiv x = \bar{5}0 &\implies (\bar{5}, \bar{10}) \\ x = \bar{7} \equiv x = \bar{4}0 &\implies (\bar{4}, \bar{10}) \\ x = \bar{8} \equiv x = \bar{3}0 &\implies (\bar{3}, \bar{10}) \\ x = \bar{10} &\implies (\bar{1}, \bar{10}) \end{aligned}$$

La première propriété est donc vérifiée pour tout  $x \in G$ .

(i) On a bien  $H \cap K = \{1\}$ .

(i) Le groupe  $\mathbb{Z}/p\mathbb{Z}$  est toujours abélien donc on a bien que tous les éléments de  $H$  et  $K$  commutent entre eux.

2. Commençons par montrer que les ensembles

$$H = G_1 \times \{e_2\}, \quad K = \{e_1\} \times G_2$$

sont bien des sous-groupes de  $G$ , soit qu'ils vérifient les trois propriétés :

- $e_G \in H$ ,
- Si  $x, y \in H$ , alors  $xy \in H$ ,
- Si  $x \in H$ , alors  $x^{-1} \in H$ .

Montrons-les :

- $e_G = (e_{G_1}, e_{G_2}) \in H$  car  $e_{G_1} \in G_1$ .
- Soient  $x = (x_1, e_{G_2})$  et  $y = (y_1, e_{G_2})$  alors

$$xy = (x_1 y_1, e_{G_2}) \in H$$

car  $x_1 y_1 \in G_1$ .

- Soit  $x = (x_1, e_{G_2})$ , alors

$$x^{-1} = (x_1^{-1}, e_{G_2}) \in H$$

car  $x_1^{-1} \in G_1$ .

De même pour  $K$ .

On a montré que ces deux ensembles sont bien des sous-groupes de  $G$ , montrons maintenant qu'ils vérifient les trois propriétés demandées :

- (i) Soit  $x = (x_1, x_2) \in G$ , alors le couple  $(x_1, e_{G_2}), (e_{G_1}, x_2)$  convient.
- (i) Il est clair que  $H \cap K = \{(e_{G_1}, e_{G_2})\} = e_G$ .
- (i) Comme le produit se fait terme à terme et que tout élément de  $G_i$  commute avec  $\{e_i\}$ , on a bien que tous les éléments de  $H$  et  $K$  commutent entre eux.

3. On note  $H$  et  $K$  les sous-groupes de  $G$ .

- (a) On procède par l'absurde. Supposons qu'il existe deux écritures de  $x = yz = y'z'$ . Alors on a

$$\begin{aligned} yz &= y'z' \\ \equiv y^{-1}yz &= y^{-1}y'z' \\ \equiv z &= y^{-1}y'z' \end{aligned}$$

Or  $z \in K$  donc  $y^{-1}y'z' \in K$ . Comme  $z' \in K$ , on a  $y^{-1}y' \in K$ . Or  $y, y' \in H$  donc  $y^{-1}y' \in H$ . On a donc  $y^{-1}y' \in H \cap K = \{e\}$  donc  $y = y'$ . Il en est de même pour  $z$ .

L'écriture est donc unique.



- (b) On a déjà montré au point précédent que l'écriture est unique et donc tout élément de  $G$  peut s'écrire de manière unique comme  $yz$  avec  $y \in H$  et  $z \in K$  donc on peut considérer l'application

$$\begin{aligned} f: H \times K &\rightarrow G \\ (x, y) &\mapsto xy \end{aligned}$$

qui est bijective d'après (i) et le point précédent.

Montrons maintenant que c'est un morphisme de groupes : Soient  $(x, y), (x', y') \in H \times K$ , on a :

$$\begin{aligned} f((x, y)(x', y')) &= f((xx', yy')) \\ &= xx'yy' \\ &= xyx'y' \\ &= f(x, y)f(x', y') \end{aligned}$$

donc  $f$  est un morphisme de groupes.

En conclusion,  $G$  est isomorphe à  $H \times K$ .

**Remarque.** Via l'isomorphisme  $G = H \times K$ , on a correspondance entre les sous-groupes

$$H \leftrightarrow H \times \{e\}, \quad K \leftrightarrow \{e\} \times K$$

On retrouve donc le cas de la question 2.

**Remarque.** En appliquant à la question 1, on obtient un isomorphisme de groupes :

$$\begin{aligned} (\mathbb{Z}/11\mathbb{Z})^\times &\simeq \langle \bar{3} \rangle \times \langle \bar{10} \rangle \\ &\simeq (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \end{aligned}$$

On verra plus tard que pour  $p$  premier, le groupe  $(\mathbb{Z}/p\mathbb{Z})^\times$  est cyclique (d'ordre  $p-1$ ), donc  $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ . Notamment,

$$\begin{aligned} (\mathbb{Z}/11\mathbb{Z})^\times &\simeq \mathbb{Z}/10\mathbb{Z} \\ &\simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{aligned}$$

d'après le théorème des restes chinois (car 5 et 2 sont premiers entre eux).

**Remarque.** Il existe des groupes finis qui ne sont pas isomorphes à un produit direct de groupes cycliques, par exemple  $\mathfrak{S}_3$ , car un produit de groupes cycliques est abélien.

En revanche, c'est un fait (pas trivial) que tout groupe fini abélien est isomorphe à un produit de groupes cycliques.

4. On se place dans le groupe  $\mathfrak{S}_3$ . On considère alors

$$\begin{aligned} H &= \langle (1\ 2) \rangle = \{(1\ 2), \text{Id}\}, \\ K &= \langle (1\ 2\ 3) \rangle = \{(1\ 2\ 3), (1\ 3\ 2), \text{Id}\} \end{aligned}$$

On a tout de suite (ii) qui est vérifié.

Il manque  $(1\ 3), (2\ 3)$  à "former". Or

$$\begin{aligned} (1\ 3) &= (1\ 2)(1\ 2\ 3), \\ (2\ 3) &= (1\ 2)(1\ 3\ 2) \end{aligned}$$

Donc (i) est vérifié.

En revanche, on a  $(1\ 2)(1\ 2\ 3) \neq (1\ 2\ 3)(1\ 2)$  donc (iii) n'est pas vérifié.

**Exercice 3.9 Exo 12.** Enoncé à remplir.

**Solution.**

1. On veut montrer l'égalité

$$\overbrace{\sigma(i_1 \ i_2 \ \dots \ i_k)}^{\alpha} \sigma^{-1} = \overbrace{(\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_k))}^{\beta}$$

Soit  $j \in \{1, \dots, n\}$ . Procédons par cas :

▷ Cas 1 :  $j \notin \{\sigma(i_1), \dots, \sigma(i_k)\}$ .

Alors  $\beta(j) = j$ . On calcule

$$\begin{aligned} \alpha(j) &= \sigma(i_1 \ i_2 \ \dots \ i_k) \sigma^{-1}(j) \\ &= \sigma(\sigma^{-1}(j)) \end{aligned}$$

Donc  $\alpha(j) = \beta(j)$ .

▷ Cas 2 :  $j = \sigma(i_r)$  pour un  $r \in \{1, \dots, k\}$ .

Alors

$$\begin{aligned} \alpha(j) &= \sigma(i_1 \ i_2 \ \dots \ i_k) \underbrace{\sigma^{-1}(\sigma(i_r))}_{i_r} \\ &= \sigma(i_{r+1}) \end{aligned}$$

D'autre part,

$$\begin{aligned} \beta(j) &= (\sigma(i_1) \ \sigma(i_2) \ \dots \ \sigma(i_k))(\sigma(i_r)) \\ &= \sigma(i_{r+1}) \end{aligned}$$

Donc  $\alpha(j) = \beta(j)$ .

Conclusion : on a  $\forall j \in \{1, \dots, n\}, \alpha(j) = \beta(j)$  donc  $\alpha = \beta$ .

**Remarque.** Soient deux ensembles  $E$  et  $F$  de cardinal fini  $n$ . Soit  $\sigma: E \rightarrow F$  une bijection.

Soit  $f \in \text{Bij}(E)$ . Alors,  $\sigma f \sigma^{-1}$  est une bijection de  $F$ .

Slogan : “ $\sigma f \sigma^{-1}$ , c'est comme  $f$ , après avoir renommé les éléments”.

En effet, notons  $E = \{x_1, \dots, x_n\}$  et  $F = \{y_1, \dots, y_n\}$  avec  $\sigma(x_i) = y_i$ .

Si  $f(x_i) = x_j$  alors

$$(\sigma f \sigma^{-1})(y_i) = (\sigma f)(x_i) = \sigma(f(x_i)) = \sigma(x_j) = y_j$$

et

$$(\sigma f \sigma^{-1})(y_i) = y_j$$

2. Il suffit de montrer que toutes les transpositions adjacentes  $(1 \ 2), (2 \ 3), \dots, (n-1 \ n)$  sont dans

$$\langle (1 \ 2), (1 \ 2 \ \dots \ n) \rangle$$

(car par le cours, les transpositions adjacentes engendrent  $\mathfrak{S}_n$ ).

On a

$$(1 \ 2 \ \dots \ n)(1 \ 2)(1 \ 2 \ \dots \ n)^{-1} = (2 \ 3)$$

$$(1 \ 2 \ \dots \ n)(2 \ 3)(1 \ 2 \ \dots \ n)^{-1} = (3 \ 4)$$

etc.

donc toutes les transpositions adjacentes sont dans  $\langle (1 \ 2), (1 \ 2 \ \dots \ n) \rangle$ .

Conclusion :  $\mathfrak{S}_n = \langle (1 \ 2), (1 \ 2 \ \dots \ n) \rangle$ .

**Remarque.** Le sous-groupe engendré par  $(i\ j), (1\ 2\ \dots\ n)$  est déterminé dans un autre pdf. Pour le cas

$$S = \langle (1\ 3), (1\ 2\ 3\ 4) \rangle$$

On a  $S \simeq D_4$ , le groupe diédral d'ordre 8.

Plus précisément, on a un morphisme de groupes

$$\begin{aligned} F: D_4 &\rightarrow S_4 \\ f &\mapsto \sigma_f \end{aligned}$$

où  $\sigma_f$  est la restriction de  $f$  à  $\{1, 2, 3, 4\}$ . Alors  $S = \text{Im}(F)$ .

**Exercice 3.10 Exo 13.** Enoncé à remplir.

**Solution.** Soient  $s_1, s_2$  deux réflexions de  $\mathbb{R}^2$ .

Sens indirect : Si  $s_1 = s_2$  alors  $s_1 s_2 = s_2 s_1$ .

Si  $s_1 = -s_2$  alors  $s_1 s_2 = s_1(-s_1) = s_1 \circ (-s_1) = -s_1 \circ s_1 = -\text{Id}$ . et  $s_2 s_1 = (-s_1) \circ s_1 = -s_1 \circ s_1 = -\text{Id}$ .

Sens direct : On suppose que  $s_1 s_2 = s_2 s_1$ .

Ecrivons  $s_1 = s_{\Delta_1}$  et  $s_2 = s_{\Delta_2}$  avec  $\Delta_1$  et  $\Delta_2$  deux droites linéaires de  $\mathbb{R}^2$ .

On sait par le cours que

$$s_1 s_2 = r_{-2\theta}$$

où  $\theta$  est l'angle orienté de  $\Delta_1$  vers  $\Delta_2$ .

De même, on a

$$s_2 s_1 = r_{+2\theta}$$

On obtient donc que  $r_{-2\theta} = r_{+2\theta}$  donc il existe  $k \in \mathbb{Z}$  tel que  $-2\theta = 2\theta + 2k\pi$  donc  $\theta = -k\frac{\pi}{2}$ .

On a donc soit  $\Delta_1 = \Delta_2$ , soit  $\Delta_1 = \Delta_2^\perp$  (orthogonalité).

Le premier donne  $s_1 = s_2$ , le second donne  $s_1 = -s_{\Delta_2^\perp}$  donc  $s_1 = -s_{\Delta_2} = s_2$ .

En effet, c'est un fait générale que

$$s_{\Delta^\perp} = -s_\Delta$$

Pour se convaincre, choisissons une base  $e, f$  avec  $e$  dans  $\Delta$  et  $f$  dans  $\Delta^\perp$ . Alors la matrice de  $s_\Delta$  est

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

et la matrice de  $-s_\Delta$  est

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

c'est la matrice de  $s_{\Delta^\perp}$ .

**Exercice 3.11 Centre du groupe diédral.** Déterminer le centre du groupe diédral  $D_n$ , pour  $n \in \mathbb{N}^*$ .

**Solution.**

▷ Pour  $n \leq 2$ , le groupe  $D_n$  est abélien donc

$$Z(D_n) = D_n$$

▷ Pour  $n \geq 3$ , on a

$$r^k s = s r^{-k}$$

pour tout  $k \in \{0, \dots, n-1\}$ .

▷ Soit  $r$  une rotation. Alors, pour tout  $k \in \{0, \dots, n-1\}$ , on a

$$r^k s = s r^{-k}$$

Donc pour que  $r \in Z(D_n)$ , il faut que  $r$  soit une rotation telle que  $r^k = r^{-k}$  pour tout  $k \in \{0, \dots, n-1\}$ . Alors,  $r$  est une rotation d'angle 0 ou  $\pi$ .

▷ Avec les notations du cours, on peut montrer qu'aucune réflexion n'est dans le centre de  $D_n$ . Par exemple, on montre que pour  $k \in \{0, \dots, n-1\}$ , on a  $r^k s$  qui ne commute pas avec  $r$ .

$$\cdot r(r^k s) = r^{k+1} s$$

$$\cdot (r^k s)r = r^{k-1} s$$

Ces éléments sont différents car  $r \neq r^{-1}$  pour  $n \geq 3$ .

Ainsi les seuls éléments dans le centre de  $D_n$

$$Z(D_n) = \{\text{Id}, r^{\frac{n}{2}}\}, \quad n \text{ pair},$$

$$Z(D_n) = \{\text{Id}\}, \quad n \text{ impair}.$$

## TD4 — Introduction à la théorie des anneaux et des corps

### Exercices en TD

**Exercice 4.1 Un corps exotique.** On définit sur l'ensemble  $\mathbb{R}^2$  une addition

$$(x, y) + (x', y') = (x + x', y + y')$$

et une multiplication

$$(x, y) \cdot (x', y') = (xx' - yy', xy' + x'y.)$$

Montrer que  $\mathbb{R}^2$  muni de ces deux lois est un corps.

**Solution.** Il faut montrer que  $\mathbb{R}^2$  muni de ces deux lois est un corps, soit que c'est un anneau commutatif dans lequel tout élément non nul est inversible.

▷ Commençons par montrer que c'est un anneau.

Il faut vérifier les 4 axiomes :

1. On sait que  $\mathbb{R}^2$  muni de l'addition par composantes est un groupe abélien.
2. On vérifie que la multiplication est associative :

$$\begin{aligned} ((x, y) \cdot (x', y')) \cdot (x'', y'') &= (xx' - yy', xy' + x'y) \cdot (x'', y'') \\ &= ((xx' - yy')x'' - (xy' + x'y)y'', (xx' - yy')y'' + (xy' + x'y)x'') \\ &= (x(x'x'' - y'y'') - y(y'x'' + x'y''), x(x'y'' + x'y'') + y(x'x'' - y'y'')) \\ &= (x(x'x'' - y'y'') - y(y'x'' + x'y''), x(x'y'' + x'y'') + y(x'x'' - y'y'')) \\ &= (x, y) \cdot (x', y') \cdot (x'', y''). \end{aligned}$$

3. On vérifie qu'il existe un élément neutre pour la multiplication :

$$\begin{aligned} (x, y) \cdot (1, 0) &= (x \cdot 1 - y \cdot 0, x \cdot 0 + y \cdot 1) \\ &= (x, y). \end{aligned}$$

4. On vérifie la distributivité de la multiplication par rapport à l'addition :

$$\begin{aligned} (x, y) \cdot ((x', y') + (x'', y'')) &= (x, y) \cdot (x' + x'', y' + y'') \\ &= (x(x' + x'') - y(y' + y''), x(y' + y'') + y(x' + x'')) \\ &= (xx' - yy' + xx'' - yy'', xy' + xy'' + yx' + yx'') \\ &= (xx' - yy', xy' + x'y) + (xx'' - yy'', xy'' + x'y'') \\ &= (x, y) \cdot (x', y') + (x, y) \cdot (x'', y''). \end{aligned}$$

▷ Montrons maintenant que cet anneau est commutatif.

Il faut vérifier que la multiplication est commutative :

$$\begin{aligned} (x, y) \cdot (x', y') &= (xx' - yy', xy' + x'y) \\ &= (x'x - y'y, x'y + xy') \\ &= (x', y') \cdot (x, y). \end{aligned}$$

▷ Montrons enfin que tout élément non nul est inversible.

Soit  $(x, y) \in \mathbb{R}^2 \setminus \{(0, 0)\}$ . On cherche  $(x', y') \in \mathbb{R}^2$  tel que  $(x, y) \cdot (x', y') = (1, 0)$ . On a donc

$$\begin{aligned} & \begin{cases} xx' - yy' = 1 \\ xy' + x'y = 0 \end{cases} \\ \iff & \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \iff & \frac{1}{x^2 + y^2} \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \iff & \begin{pmatrix} x' \\ y' \end{pmatrix} = \frac{1}{x^2 + y^2} \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{x}{x^2 + y^2} \\ \frac{-y}{x^2 + y^2} \end{pmatrix} \end{aligned}$$

On pose alors

$$(x', y') = \left( \frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right).$$

et on vérifie que  $(x, y) \cdot (x', y') = (1, 0)$ .

Ce corps est  $\mathbb{C}$  :

$$\begin{array}{ccc} \mathbb{R}^2 & & \mathbb{C} \\ (x, y) & \longleftrightarrow & x + iy \end{array}$$

**Exercice 4.2 Entiers de Gauss.** On définit l'ensemble des entiers de Gauss :

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}.$$

1. Montrer que  $\mathbb{Z}[i]$  est un sous-anneau de  $\mathbb{C}$ . Est-il commutatif? Est-il un intègre? Est-il un corps?
2. Pour  $z = a + ib \in \mathbb{Z}[i]$ , on pose

$$N(z) = |z|^2 = a^2 + b^2$$

qu'on appelle la norme. Montrer qu'on a

$$\forall z, z' \in \mathbb{Z}[i], \quad N(zz') = N(z)N(z').$$

3. Montrer que si  $z \in \mathbb{Z}[i]$  est inversible si et seulement si  $N(z) = 1$ . Identifier le groupe des inversibles de  $\mathbb{Z}[i]$ .
4. Soient  $m, n \in \mathbb{N}$ . Montrer que si  $m$  et  $n$  peuvent être écrits comme somme de deux carrés, alors leur produit  $mn$  aussi.
5. Soit maintenant l'ensemble des rationnels de Gauss :

$$\mathbb{Q}(i) = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Q}\}.$$

Montrer qu'il s'agit d'un sous-corps de  $\mathbb{C}$ .

**Solution.** On se place dans

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}.$$

1. On montre facilement que c'est un sous-anneau de  $\mathbb{C}$  en vérifiant les axiomes.
  - ▷ On a bien  $0 \in \mathbb{Z}[i]$
  - ▷ On a bien  $\mathbb{Z}[i]$  stable par addition.
  - ▷ On a bien  $\mathbb{Z}[i]$  stable par passage à l'opposé.
  - ▷ On a bien  $1 \in \mathbb{Z}[i]$
  - ▷ On a bien  $\mathbb{Z}[i]$  stable par multiplication.

Donc  $\mathbb{Z}[i]$  est un sous-anneau de  $\mathbb{C}$ .

Cet anneau est bien commutatif car  $\mathbb{C}$  l'est. De même pour l'intégrité.  
Par contre,  $\mathbb{Z}[i]$  n'est pas un corps car  $2 \in \mathbb{Z}[i]$  n'est pas inversible.

2. On sait que

$$\forall z, z' \in \mathbb{C}, \quad |zz'| = |z||z'|.$$

et donc

$$N(zz') = N(z)N(z').$$

3.  $\triangleright$  Montrons d'abord le sens direct.

On suppose que  $z \in \mathbb{Z}[i]$  est inversible.

Alors, il existe  $z' \in \mathbb{Z}[i]$  tel que  $zz' = 1$ .

En utilisant la question précédente, on a

$$N(zz') = N(z)N(z') = 1.$$

Comme  $N(z) \in \mathbb{N}$  et  $N(z') \in \mathbb{N}$ , on a

$$N(z) = N(z') = 1.$$

$\triangleright$  Montrons maintenant le sens réciproque.

On suppose que  $N(z) = 1$ .

Alors  $z = a + ib$  avec  $a, b \in \mathbb{Z}$  et  $a^2 + b^2 = 1$ . Alors

$$(a + ib)(a - ib) = 1.$$

Donc  $a + ib$  est inversible dans  $\mathbb{Z}[i]$ , d'inverse  $a - ib$ .

Pour  $a, b \in \mathbb{Z}$ , on a

$$a^2 + b^2 = 1 \iff (a, b) \in \{(1, 0), (0, 1), (-1, 0), (0, -1)\}.$$

Donc les inversibles de  $\mathbb{Z}[i]$  sont

$$\mathbb{Z}[\square]^\times = \{1, -1, i, -i\} = \mathbb{U}_4.$$

(groupe cyclique d'ordre 4, engendré par  $i$  ou  $-i$ )

4. Formule magique vue à la question 2 :

$$(a^2 + b^2)(a'^2 + b'^2) = (aa' - bb')^2 + (ab' + ba')^2.$$

5. C'est clair que  $\mathbb{Q}(i)$  est un sous-corps de  $\mathbb{C}$ , montrons simplement l'axiome de stabilité par passage à l'inverse.

Pour  $a, b \in \mathbb{Q}$ , si  $a + ib \neq 0$ , alors

$$\frac{1}{a + ib} = \frac{a}{a^2 + b^2} - i \frac{b}{a^2 + b^2} \in \mathbb{Q}(i).$$

**Exercice 4.3 Nilpotents.** Soit  $A$  un anneau commutatif. On dit qu'un élément  $x \in A$  est nilpotent s'il existe  $n \in \mathbb{N}$  tel que  $x^n = 0$ .

1. Donner un exemple d'un anneau commutatif  $A$  et d'un élément nilpotent  $x \in A$  non nul.
2. Montrer que si  $x$  est nilpotent et que  $y$  est n'importe quel élément de  $A$ , alors  $xy$  est nilpotent.
3. Montrer que l'ensemble des éléments nilpotents de  $A$  est un sous-groupe de  $A$ . Est-ce un sous-anneau ?
4. Montrer que si  $x$  est nilpotent alors  $1 - x$  est inversible.
5. Soient  $u, x \in A$  tel que  $u$  est inversible et  $x$  est nilpotent. Montrer que  $u + x$  est inversible.

**Solution.**

1. On considère

$$A = \mathbb{Z}/4\mathbb{Z}$$

alors  $x = \bar{2} \neq \bar{0}$  est nilpotent car  $x^2 = \bar{4} = \bar{0}$ .

2. Soit  $x \in A$  nilpotent (d'ordre  $n$ ) et  $y \in A$ . Alors

$$(xy)^n = x^n y^n = 0.$$

3. Soit  $N$  l'ensemble des éléments nilpotents de  $A$ . Vérifions les axiomes :

- ▷ On a bien  $0 \in N$  car  $0^1 = 0$ .
- ▷ Soit  $x \in N$ . Alors il existe  $n \in \mathbb{N}$  tel que  $x^n = 0$ . Alors  $(-x)^n = (-1)^n x^n = 0$ , donc  $-x \in N$ .
- ▷ Soit  $x, y \in N$ . Alors il existe  $n, m \in \mathbb{N}$  tels que  $x^n = 0$  et  $y^m = 0$ . Alors

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

Comme 1 n'est pas nilpotent,  $N$  n'est pas un sous-anneau.

**Remarque.** C'est un idéal de  $A$  par la question 2.

- ▷ Soit  $x \in A$  nilpotent. Alors il existe  $n \in \mathbb{N}$  tel que  $x^n = 0$ . Alors

$$(1-x)(1+x+x^2+\dots+x^{n-1}) = 1-x^n = 1.$$

Donc  $1-x$  est inversible, d'inverse  $1+x+x^2+\dots+x^{n-1}$ .

- ▷ Soit  $u, x \in A$  tel que  $u$  est inversible et  $x$  est nilpotent. Alors

$$u+x = u(1+u^{-1}x) = u(1-(-u^{-1}x)).$$

Comme  $-u^{-1}x$  est nilpotent par la question 4,  $1-(-u^{-1}x)$  est inversible, donc  $u+x$  est inversible (produit de deux éléments inversibles).

**Exercice 4.4 Anneaux intègres finis.** Soit  $A$  un anneau intègre fini. Montrer que  $A$  est un corps.

**Solution.** Commençons par montrer que tout élément non nul est inversible.

▷ Montrons maintenant que tout élément non nul est inversible.

Soit  $a \in A \setminus \{0\}$ . Considérons la multiplication à gauche par  $a$  :

$\times a$	$a$
$a_1$	$a_1 a$
$a_2$	$a_2 a$
$\vdots$	$\vdots$
$a_n$	$a_n a$

avec  $a_1, \dots, a_n$  les éléments de  $A$  (distincts).

Alors la multiplication à gauche par  $a$  est une bijection de  $A$  sur  $A$ . Donc il existe  $b \in A$  tel que  $ba = 1$ . Donc  $a$  est inversible.

Comme  $a$  est quelconque, tout élément non nul de  $A$  est inversible.

Donc  $A$  est un corps.



Autre rédaction possible : Soit  $a \in A \setminus \{0\}$ . Considérons les puissances de  $a$  :

$$1, a, a^2, \dots$$

Comme  $A$  est fini, il existe  $n, m \in \mathbb{N}$  tels que  $a^n = a^{n+m}$ .

Alors  $a^n(1 - a^m) = 0$ . Comme  $A$  est intègre, on a  $1 - a^m = 0$ , donc  $a^m = 1$ .

**Exercice 4.5 L'anneau  $\mathbb{Z}[\sqrt{2}]$ .** On définit :

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

1. Montrer que  $\mathbb{Z}[\sqrt{2}]$  est un sous-anneau de  $\mathbb{R}$ .
2. Montrer que  $\mathbb{Z}[\sqrt{2}]$  n'est pas isomorphe à l'anneau des entiers de Gauss  $\mathbb{Z}[i]$ .
3. Montrer que le groupe  $\mathbb{Z}[\sqrt{2}]^\times$  est infini.

**Solution.**

1. Vérifions les axiomes :

- ▷ On a bien  $\mathbb{Z}[\sqrt{2}]$  un groupe abélien pour l'addition.
- ▷ On a bien  $0 \in \mathbb{Z}[\sqrt{2}]$ .
- ▷ Soit  $z = a + b\sqrt{2}, z' = a' + b'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ . Alors

$$zz'(a + b\sqrt{2})(a' + b'\sqrt{2}) = aa' + 2bb' + (ab' + ba')\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

Donc  $\mathbb{Z}[\sqrt{2}]$  est un sous-anneau de  $\mathbb{R}$ .

2. Montrons que  $\mathbb{Z}[\sqrt{2}]$  n'est pas isomorphe à  $\mathbb{Z}[i]$ .

Regardons l'ensemble des solutions de l'équation  $x^2 = -1$ .

Pour  $\mathbb{Z}[\sqrt{2}]$ , on a aucune solution.

Pour  $\mathbb{Z}[i]$ , on a  $x = i$ .

Donc  $\mathbb{Z}[\sqrt{2}]$  n'est pas isomorphe à  $\mathbb{Z}[i]$ .

Autre rédaction, il y a bien une bijection

$$\begin{aligned} \varphi : \mathbb{Z}[i] &\longrightarrow \mathbb{Z}[\sqrt{2}] \\ a + ib &\longmapsto a + b\sqrt{2} \end{aligned}$$

Cette bijection est un isomorphisme de groupes :

$$\begin{aligned} \varphi((a + ib) + (a' + ib)) &= \varphi((a + a') + i(b + b')) \\ &= (a + a') + (b + b')\sqrt{2} \\ &= (a + b\sqrt{2}) + (a' + b'\sqrt{2}) \\ &= \varphi(a + ib) + \varphi(a' + ib). \end{aligned}$$

Mais  $\varphi$  n'est pas un morphisme d'anneaux car

$$\begin{aligned} \varphi(i \times i) &= \varphi(-1) = -1 \\ \varphi(i) \times \varphi(i) &= \sqrt{2} \times \sqrt{2} = 2. \end{aligned}$$

Cela ne montre pas que  $\mathbb{Z}[\sqrt{2}]$  n'est pas isomorphe à  $\mathbb{Z}[i]$  en tant qu'anneaux, simplement que  $\varphi$  n'est pas un morphisme d'anneaux.

Montrons que  $\mathbb{Z}[\sqrt{2}]$  n'est pas isomorphe à  $\mathbb{Z}[i]$  en tant qu'anneaux.

Par l'absurde, supposons qu'il existe un isomorphisme d'anneaux  $f : \mathbb{Z}[i] \rightarrow \mathbb{Z}[\sqrt{2}]$ . Alors

$$f(i)^2 = f(i^2) = f(-1) = -1.$$

donc  $(f(i))^2 = -1$  donc  $f(i) = \pm i$ .

Absurde car  $f(i) \in \mathbb{Z}[\sqrt{2}]$  et  $i \notin \mathbb{Z}[\sqrt{2}]$ .

3. Comme

$$(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$$

on a que  $1 + \sqrt{2}$  est inversible.

On en déduit que

$$\forall n \in \mathbb{N}, \quad (1 + \sqrt{2})^n \in \mathbb{Z}[\sqrt{2}]^\times.$$

Comme ils sont tous distincts,  $\mathbb{Z}[\sqrt{2}]^\times$  est infini.

**Remarque.** Cela donne une autre preuve du fait que  $\mathbb{Z}[\sqrt{2}]$  et  $\mathbb{Z}[i]$  ne sont pas isomorphes en tant qu'anneaux, puisque  $\mathbb{Z}[i]^\times$  est fini.

En effet, si  $f : A \rightarrow B$  est un isomorphisme d'anneaux, alors il induit un isomorphisme de groupes  $f^\times : A^\times \rightarrow B^\times$ .

**Remarque.** On peut montrer que

$$\mathbb{Z}[\sqrt{2}]^\times = \{ \varepsilon (1 + \sqrt{2})^n \mid \varepsilon \in \{-1, 1\}, n \in \mathbb{Z} \}.$$

#### Exercice 4.6 Idéaux et inversibles. Énoncé à remplir

**Solution.** Soit  $A$  un anneau commutatif.

1. Evident

2. Deux cas :

▷ Si  $I = A$ , alors  $1 \in I$  et 1 est inversible.

▷ Si  $I$  contient un inversible  $u \in A^\times$ , alors  $u^{-1}u \in I$  (car  $I$  est un idéal) et donc  $1 \in I$  et donc  $I = A$ .

3. Soit  $a \in A$

▷ Si  $(a) = A$ , alors  $1 \in (a)$  et donc il existe  $b \in A$  tel que  $ab = 1$ , donc  $a$  est inversible.

▷ Si  $a$  est inversible, alors  $(a) = A$  par la question 2

4. On suppose que  $A \neq \{0\}$ .

▷ On suppose que  $A$  est un corps.

Soit  $I$  un idéal de  $A$  qui n'est pas  $\{0\}$ .

Alors  $I$  contient un élément non nul  $a$  qui est inversible car  $A$  est un corps. Donc  $I = A$ .

▷ On suppose que les seuls idéaux de  $A$  sont  $\{0\}$  et  $A$ .

Soit  $a \in A \setminus \{0\}$ .

L'idéal  $(a)$  est non nul, donc  $(a) = A$ .

Donc  $a$  est inversible. Donc  $A$  est un corps.

**Exercice 4.7 Un corps.** Pouvez-vous construire un corps  $K$  qui contient  $\mathbb{C}$  comme sous-corps et tel qu'il existe  $\alpha \in K \setminus \mathbb{C}$  tel que  $\alpha^2 = i$  ?

**Solution.** NON! Il existe déjà un  $z \in \mathbb{C}$  tel que  $z^2 = 1$ .

$$z = e^{i\frac{\pi}{4}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}.$$

Supposons qu'il existe un corps  $K$  contenant  $\mathbb{C}$  comme sous-corps et tel qu'il existe  $\alpha \in K \setminus \mathbb{C}$  tel que  $\alpha^2 = 1$ .

Alors  $\alpha^2 = z^2$  et donc  $\alpha = z$  ou  $\alpha = -z$  car un corps est intègre.

Donc  $\alpha \in \mathbb{C}$ , contradiction.

**Exercice 4.8 Idéaux des polynômes à facteurs relatifs.** On travaille dans l'anneau  $\mathbb{Z}[X]$ .

1. Montrer que l'idéal  $(2, X)$  n'est pas principal.
2. Soit  $I$  l'ensemble des polynômes  $f \in \mathbb{Z}[X]$  tels que  $f(1)$  et  $f(-1)$  soient pairs. Montrer que  $I$  est un idéal de  $\mathbb{Z}[X]$  et donner des générateurs de  $I$ .  
On pourra commencer par faire les échauffements suivant :
  - (a) Soit  $I = \{f \in \mathbb{R}[X] \mid f(1) = 0\}$ . Montrer que c'est un idéal de  $\mathbb{R}[X]$  et en donner un système de générateurs.
  - (b) Pareil avec  $\mathbb{R} \rightsquigarrow \mathbb{Z}$ .

**Solution.**

1. On a que

$$A = (2, X) = \{2k + k'X \mid k, k' \in \mathbb{Z}\}.$$

Supposons que  $A$  est principal. Alors il existe  $f \in A$  tel que  $A = (f)$ . Donc  $2 \in (f)$  et  $X \in (f)$ .

Plus précisément, on a  $f|2$  et  $f|X$ , donc

$$f \in \{1, -1, 2, -2\}, \quad \text{et} \quad f \in \{1, -1, X, -X\}$$

Donc  $f \in \{1, -1\}$ . En particulier, on a  $1 \in (2, X)$ , ce qui veut dire qu'il existe  $u, v \in \mathbb{Z}[X]$  tels que  $1 = 2u + Xv$ . En évaluant en  $X = 0$ , on a  $1 = 2u(0)$ , contradiction.

2. Echauffements :

- (a)  $I$  est clairement un sous-groupe de  $\mathbb{R}[X]$ , montrons qu'il est stable par multiplication.  
Soit  $f \in I$  et  $g \in \mathbb{R}[X]$ . Alors

$$(fg)(1) = f(1)g(1)$$

est pair. Donc  $fg \in I$ .

Donc  $I = (X - 1)$ .

- (b) Même raisonnement pour montrer que  $I$  est un idéal. On a  $I = (X - 1)$  car on peut effectuer la division euclidienne de  $f$  par  $X - 1$ .

On peut facilement vérifier que cet ensemble est un idéal de  $\mathbb{Z}[X]$ .

Soit  $f \in I$ , on écrit sa division euclidienne par  $X - 1$  :

$$f = (X - 1)q + r, \quad q \in \mathbb{Z}[X], r \in \mathbb{Z}.$$

donc  $r = f(1)$  est pair et alors il existe  $k \in \mathbb{Z}$  tel que

$$f = (X - 1)q + 2k.$$

Alors  $f \in (X - 1, 2)$ .

On a montré que  $I \subset (X-1, 2)$ .  
 Montrons maintenant que  $(X-1, 2) \subset I$ .  
 Comme  $X-1 \in I$  et  $2 \in I$ , on a  $(X-1, 2) \subset I$ .  
 Donc  $I = (X-1, 2)$ .

**Exercice 4.9 Entiers de Gauss, bis.** On se place dans l'anneau des entiers de Gauss

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}.$$

On note  $|z|$  le module d'un nombre complexe  $z$ . On rappelle la *norme*  $N(z) = z\bar{z} = |z|^2 = a^2 + b^2$  pour  $z = a + ib \in \mathbb{Z}[i]$ . On a montré qu'on a  $N(zz') = N(z)N(z')$  et

$$z \in \mathbb{Z}[i]^\times \iff N(z) = 1 \iff z \in \{1, -1, i, -i\}.$$

1. Soit  $z \in \mathbb{C}$ . Montrer qu'il existe  $z' \in \mathbb{Z}[i]$  tel que  $|z - z'| \leq \frac{\sqrt{2}}{2}$ . (Un dessin pourra être utile !)
2. En déduire que  $\mathbb{Z}[i]$  est un anneau euclidien pour la jauge euclidienne  $v(z) = N(z)$ .  
Calculer une division euclidienne de  $17 + 4i$  par  $1 - i$ .
3. Montrer que pour  $z \in \mathbb{Z}[i]$ , si  $N(z)$  est premier alors  $z$  est irréductible.
4. Calculer le PGCD de  $11 + 7i$  et  $18 - i$ .

**Solution.**

1. Soit  $z \in \mathbb{C}$ . On écrit  $z = x + iy$  avec  $x, y \in \mathbb{R}$ . Il existe  $a \in \mathbb{Z}$  tel que  $|x - a| \leq \frac{1}{2}$ .  
Il existe  $b \in \mathbb{Z}$  tel que  $|y - b| \leq \frac{1}{2}$ .  
On pose  $z' = a + ib \in \mathbb{Z}[i]$ . Alors

$$\begin{aligned} |z - z'| &= |(x - a) + i(y - b)| \\ &= \sqrt{(x - a)^2 + (y - b)^2} \\ &\leq \sqrt{\frac{1}{4} + \frac{1}{4}} \\ &= \frac{\sqrt{2}}{2}. \end{aligned}$$

2. Soient  $z, w \in \mathbb{Z}[i]$  avec  $w \neq 0$ . On considère  $\frac{z}{w} \in \mathbb{C}$ .  
Par la question précédente, il existe  $z' \in \mathbb{Z}[i]$  tel que  $|\frac{z}{w} - z'| \leq \frac{\sqrt{2}}{2}$ .  
On pose  $z'' = z - wz'$  de sorte que

$$z = wz' + z'' \quad \text{et} \quad z', z'' \in \mathbb{Z}[i].$$

où  $z'$  joue le rôle du quotient et  $z''$  le rôle du reste.  
Il reste à vérifier que  $N(z'') < N(w)$ .

$$N(z'') = |z''|^2 = |z - wz'|^2$$

Or on a

$$\left| \frac{z - wz'}{w} \right| \leq \frac{\sqrt{2}}{2}$$

donc

$$\frac{|z - wz'|}{|w|} \leq \frac{\sqrt{2}}{2}$$

donc

$$|z - wz'| \leq \frac{\sqrt{2}}{2} |w|$$

d'où

$$N(z'') = |z - wz'|^2 < \frac{1}{2}|w|^2 < |w|^2 = N(w).$$

Conclusion :  $\mathbb{Z}[i]$  est un anneau euclidien pour la jauge euclidienne  $v(z) = N(z)$ . Il est donc principal.

On a

$$\begin{aligned}\frac{17+4i}{1-i} &= \frac{(17+4i)(1+i)}{(1-i)(1+i)} \\ &= \frac{13+21i}{2} \\ &= \frac{13}{2} + \frac{21}{2}i.\end{aligned}$$

On pose ici  $z' = 6 + 10i$  et alors

$$17 + 4i = (1 - i)(6 + 10i) + 1.$$

où 1 joue le rôle du reste.

Comme  $N(1) = 1$  et  $N(1 - i) = 2$ , on a bien  $N(1) < N(1 - i)$  et on a bien effectué une division euclidienne.

**Remarque.** Il y a 3 autres divisions euclidiennes possibles avec les quotients :

$$6 + 11i, \quad 7 + 10i, \quad 7 + 11i.$$

3. On raisonne par contraposée.

Soit  $z \in \mathbb{Z}[i]$  non irréductible.

- ▷ Si  $z = 0$ , alors  $N(z) = 0$  n'est pas premier.
- ▷ Si  $z$  est inversible, alors  $N(z) = 1$  n'est pas premier.
- ▷ Si  $z$  n'est pas inversible, alors il existe  $z_1, z_2 \in \mathbb{Z}[i]$  tels que  $z = z_1 z_2$  avec  $z_1, z_2$  non inversibles. Alors

$$N(z) = N(z_1)N(z_2) \quad \text{composé}$$

On en conclut que si  $N(z)$  est premier alors  $z$  est irréductible.

4. On utilise l'algorithme d'Euclide.

$$N(11 + 7i) = 11^2 + 7^2 = 170$$

$$N(18 - i) = 18^2 + (-1)^2 = 325.$$

On va donc calculer la division euclidienne de  $18 - i$  par  $11 + 7i$ .

$$\begin{aligned}\frac{18-i}{11+7i} &= \frac{(18-i)(11-7i)}{170} \\ &= \frac{191-137i}{170} \\ &= \frac{191}{170} - \frac{137}{170}i. \\ &\rightsquigarrow 1 - i \quad \text{quotient}\end{aligned}$$

On pose ici  $z' = 1 - i$  et alors

$$18 - i = (11 + 7i)(1 - i) + 3i.$$

où  $3i$  joue le rôle du reste.

Comme  $N(3i) = 9$  et  $N(11 + 7i) = 170$ , on a bien  $N(3i) < N(11 + 7i)$  et on a bien effectué une division euclidienne.

On continue avec  $11 + 7i$  et  $3i$ .

$$\begin{aligned}\frac{11 + 7i}{3i} &= \frac{(11 + 7i)(-i)}{3} \\ &= \frac{7 - 11i}{3} \\ &= \frac{7}{3} - \frac{11}{3}i. \\ &\leadsto 2 - 4i \quad \text{quotient}\end{aligned}$$

On pose ici  $z'' = 2 - 4i$  et alors

$$11 + 7i = 3i(2 - 4i) + (-1 + i).$$

où  $-1 + i$  joue le rôle du reste.

Comme  $N(-1 + i) = 2$  et  $N(3i) = 9$ , on a bien  $N(-1 + i) < N(3i)$  et on a bien effectué une division euclidienne.

On continue avec  $3i$  et  $-1 + i$ .

$$\begin{aligned}\frac{3i}{-1 + i} &= \frac{3i(-1 - i)}{2} \\ &= \frac{3 - 3i}{2} \\ &= \frac{3}{2} - \frac{3}{2}i. \\ &\leadsto 1 - i \quad \text{quotient}\end{aligned}$$

On pose ici  $z''' = 1 - i$  et alors

$$3i = (1 - i)(-1 + i) + i.$$

où  $i$  joue le rôle du reste.

Comme  $N(i) = 1$  et  $N(1 - i) = 2$ , on a bien  $N(i) < N(1 - i)$  et on a bien effectué une division euclidienne.

UN PGCD est donc le dernier reste non nul, ici  $i$ . Les autres PGCD possibles sont  $-i, 1, -1$ .

Dit autrement,  $11 + 7i$  et  $18 - i$  sont premiers entre eux.

**Remarque.** Pour l'instant on ne sait pas encore classer les éléments irréductibles de  $\mathbb{Z}[i]$ .

On sait juste que pour  $z \in \mathbb{Z}[i]$ , si  $N(z)$  est premier alors  $z$  est irréductible.

La réciproque est fautive (montrer que 3 est irréductible dans  $\mathbb{Z}[i]$  alors que  $N(3) = 9$ )

**Exercice 4.10 Théorème des deux carrés de Fermat.** Le but de cet exercice est de montrer le *théorème des deux carrés* de Fermat : un nombre premier impair  $p$  peut s'écrire comme somme de deux carrés si et seulement si  $p \equiv 1 \pmod{4}$ .

1. Vérifier que ce théorème est vrai pour les nombres premiers  $\leq 19$ .
2. Montrer qu'un nombre impair qui est une somme de deux carrés est nécessairement congru à 1 modulo 4.
3. Soit  $p$  un nombre premier congru à 1 modulo 4, qu'on écrit  $p = 4n + 1$ . On pose  $x = (2n)!$ .
  - (a) Montrer que  $x^2 \equiv (p - 1)! \pmod{p}$ .

**Solution.**

1. On a le tableau suivant :

$p$	$p \equiv 1 \pmod{4}$	$p = a^2 + b^2$
2 pair	Faux	Faux
3	Faux	Faux
5	Vrai	Vrai, $1^2 + 2^2$
7	Faux	Faux
11	Faux	Faux
13	Vrai	Vrai, $2^2 + 3^2$
17	Vrai	Vrai, $1^2 + 4^2$
19	Faux	Faux

Le théorème est vrai pour les nombres premiers  $\leq 19$ .