HAX501X – Groupes et anneaux 1
Feuilles de TD

Clément Dupont
Université de Montpellier
2024-2025

1 Rappels d'arithmétique des entiers

1. Résoudre les exercices du chapitre 1 du poly.

2. Résoudre, pour $x \in \mathbb{Z}$:

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

3. Congruences. Résoudre, pour $x \in \mathbb{Z}$:

$$12\,x \equiv 9 \pmod{21} \qquad \text{puis} \qquad 12\,x \equiv 11 \pmod{21}.$$

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

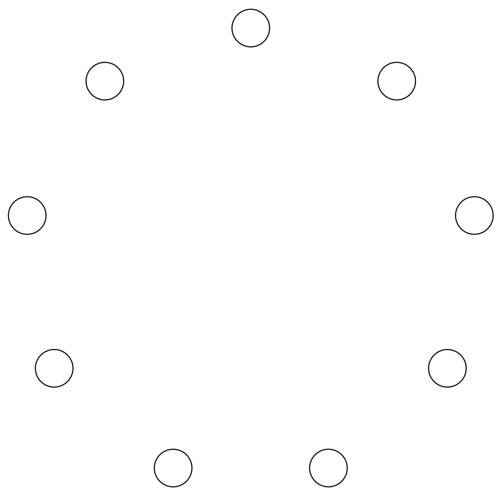
5. Inversibilité modulo un entier. Est-ce que 18 est inversible modulo 49 ? Si oui, en calculer un inverse. Mêmes questions avec 42 modulo 135.

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.

7. Racine. Soit $n \in \mathbb{N}$ qui n'est pas le carré d'un entier. Montrer que $\sqrt{n}$ est irrationnel.

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

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 coloriages différents ?

2) Soit C un coloriage. On obtient d'autres coloriages en faisant tourner C d'un angle multiple de $2\pi/n$. Soit k le nombre de coloriages *différents* qu'on obtient ainsi. Montrer que k est un diviseur de n. Combien y a-t-il de coloriages pour lesquels $k = 1$?

3) Supposons maintenant que $n = p$ est un nombre premier. Déduire des questions précédentes que p divise $a^p - a$.

10. Des congruences (contrôle continu 2023-24).

1) Déterminer, suivant les valeurs de l'entier naturel n, le reste de la division euclidienne de 3^n par 5.

2) Pour quels entiers naturels n a-t-on à la fois $n \equiv 2 \pmod 5$ et $3^n \equiv 2 \pmod 5$? Justifier.

3) Déterminer l'ensemble des entiers naturels n qui vérifient :

$$3^n \equiv n \pmod 5.$$

11. Triplets pythagoriciens. 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 $k \geqslant 2$ 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 $m > n \geqslant 1$. On pose

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

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) Déduire de la question précédente que a et b sont de parités différentes (c'est-à-dire que l'un est pair et l'autre impair), puis que c est impair.

8) Quitte à échanger les rôles joués par a et b on peut donc 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 $m > n \geqslant 1$ 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.

2 Étude de $\mathbb{Z}/n\mathbb{Z}$

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

$$f : \mathbb{Z} \longrightarrow \mathbb{U}_n \ , \ k \mapsto e^{\frac{2i\pi k}{n}}$$

passe au quotient par la relation de congruence modulo n et induit une application

$$g : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{U}_n \ , \ \overline{k} \mapsto e^{\frac{2i\pi k}{n}}.$$

Montrer que g est bijective.

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

3. Puissance. On se place dans $\mathbb{Z}/41\mathbb{Z}$. Calculer $\overline{2}^{2024}$.

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

5. Théorème de Wilson. Le but de cet exercice est de démontrer le théorème de Wilson [1] : pour un entier $n \geqslant 2$, on a l'équivalence :

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

1) Soit un nombre premier p.
   a) Quels éléments $x \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{\overline{0}\}$ sont égaux à leur inverse ?
   b) En calculant le produit de tous les éléments de $(\mathbb{Z}/p\mathbb{Z}) \setminus \{\overline{0}\}$, montrer qu'on a

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

2) Soit un nombre n composé. Montrer que $(n-1)!$ n'est pas congru à -1 modulo n. En déduire le théorème de Wilson.

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 cette formule 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.

1. Nommé en l'honneur du mathématicien anglais John Wilson (1741-1793), même si le théorème était connu bien avant lui, notamment par le mathématicien arabe Alhazen qui vécut autour de l'an mil.

Exercices supplémentaires, et approfondissement

7. Équations.

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 $x^2 - \overline{6}x + \overline{10} = \overline{0}$.

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
$$ax = \overline{0},$$
2) résoudre l'équation
$$x^2 + \overline{2}x - \overline{3} = \overline{0}.$$

9. Fonction de Möbius.
On définit la fonction de Möbius [2] $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ par la formule :
$$\mu(n) = \begin{cases} (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers distincts}\,; \\ 0 & \text{sinon.} \end{cases}$$
On a $\mu(1) = 1$ par convention (car 1 est égal au produit de 0 nombre premier).

1) Calculer $\mu(n)$ pour $n \in \{1, \dots, 12\}$.
2) Soient $m, n \in \mathbb{N}^*$ tels que $m \wedge n = 1$. Montrer que $\mu(mn) = \mu(m)\mu(n)$.
3) Montrer qu'on a, pour $n \in \mathbb{N}^*$:
$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1\,; \\ 0 & \text{sinon.} \end{cases}$$
4) En déduire la formule d'*inversion de Möbius* : pour deux fonctions $f, g : \mathbb{N}^* \to \mathbb{R}$ on a l'équivalence :
$$\left(\forall n \in \mathbb{N}^*,\ f(n) = \sum_{d|n} g(d) \right) \iff \left(\forall n \in \mathbb{N}^*,\ g(n) = \sum_{d|n} \mu(\tfrac{n}{d}) f(d) \right).$$
5) En déduire grâce à un exercice précédent une formule pour l'indicatrice d'Euler en termes de la fonction de Möbius :
$$\forall n \in \mathbb{N}^*,\ \varphi(n) = \sum_{d|n} \mu(\tfrac{n}{d}) d\,.$$

10. Comment "rendre une application injective". Soit une application $f : E \to F$. On définit une relation $\sim$ sur E par :
$$x \sim x' \iff f(x) = f(x').$$
1) Montrer qu'il s'agit d'une relation d'équivalence.

2. Nommée en l'honneur du mathématicien allemand Ferdinand Möbius (1790-1868) qui l'introduisit.

2) Montrer que f passe au quotient par cette relation d'équivalence et que l'application induite $g : E/\sim \to F$ est injective.

(Moralité : on peut "rendre une application injective" en remplaçant l'ensemble de départ par un quotient. Vous pourrez remarquer une analogie avec un fait que vous connaissez : on peut "rendre une application surjective" en remplaçant l'ensemble d'arrivée par un sous-ensemble. Plus précisément, si $f : E \to F$ est une application, alors elle induit une application surjective $g : E \to f(E)$.)

3 Introduction à la théorie des groupes

1. Groupes ? Ces choses-là 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.
- ▷ L'ensemble des parties d'un ensemble fixé E, muni de l'union des parties.
- ▷ L'ensemble des permutations $\sigma \in \mathfrak{S}_6$ telles que $\sigma^2 = \mathrm{id}$, muni de la composition.

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

3. Petits groupes. Déterminer toutes les tables de multiplication possibles pour des groupes d'ordre $\leqslant 5$. (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 d'ordre 4, et un seul d'ordre 5.
- ▷ Remarquer que tous ces groupes sont abéliens.

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

5. 24 heures chrono (contrôle continu 2023-24)

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.)

6. Union de sous-groupes (contrôle continu 2023-24).

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 $H \subset K$ ou $K \subset H$.
2) Donner un exemple de groupe G et de trois sous-groupes H, K, L qui sont tous les trois différents de G et tels que $G = H \cup K \cup L$.

7. Morphismes de groupes ? Ces choses-là sont-elles des morphismes de groupes ?

- ▷ $f : \mathbb{Z} \to \mathbb{Z}^*$, $n \mapsto 2^n$.
- ▷ $g : \mathbb{C}^* \to \mathbb{C}^*$, $z \mapsto z^3$.
- ▷ $h : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}$, $\overline{k} \mapsto k$.
- ▷ $i : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}$, $A \mapsto \mathrm{tr}(A)$.
- ▷ $j : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$, $\overline{k} \mapsto \widetilde{k}$.
- ▷ $k : \mathfrak{S}_4 \to \mathfrak{S}_4$, $\sigma \mapsto \sigma(1\ 2)$.
- ▷ $l : \mathfrak{S}_4 \to \mathfrak{S}_4$, $\sigma \mapsto (1\ 2)\sigma(1\ 2)$.

8. Transformations affines (contrôle continu 2023-24).

1) Pour (a, b) et (a', b') deux éléments de $\mathbb{R}^* \times \mathbb{R}$, on définit

$$(a, b)\#(a', b') = (aa', b + ab').$$

a) Montrer que $\mathbb{R}^* \times \mathbb{R}$, muni de la loi de composition interne $\#$, est un groupe.

b) Ce groupe est-il abélien ? On justifiera.

2) Pour $(a, b) \in \mathbb{R}^* \times \mathbb{R}$ on considère l'application

$$f_{a,b} : \mathbb{R} \longrightarrow \mathbb{R}\ ,\ x \mapsto ax + b.$$

On remarque (on ne demande pas de justification) que c'est une application bijective. On rappelle la notation $\mathrm{Bij}(E)$ pour le groupe des permutations d'un ensemble E.

a) Montrer que l'application

$$\Phi : \mathbb{R}^* \times \mathbb{R} \longrightarrow \mathrm{Bij}(\mathbb{R})\ ,\ (a, b) \mapsto f_{a,b}$$

est un morphisme de groupes, où la structure de groupe de $\mathbb{R}^* \times \mathbb{R}$ est celle de la question précédente.

b) Montrer que ce morphisme de groupes est injectif.

9. Retour sur le petit théorème de Fermat, et le théorème d'Euler.

1) Soit p un nombre premier. En appliquant le théorème de Lagrange dans le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$, redémontrer le petit théorème de Fermat.

2) Soit $n \in \mathbb{N}^*$. Montrer que pour tout $x \in \mathbb{Z}$ tel que $x \wedge n = 1$ on a :

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

(On appelle ce résultat le *théorème d'Euler*. Quel est le rapport avec le petit théorème de Fermat ?)

10. Centre. Soit G un groupe. On définit le *centre*[3] de G :

$$Z(G) = \{x \in G \mid \forall y \in G,\ xy = yx\}.$$

1) Montrer que $Z(G)$ est un sous-groupe abélien de G, et que G est abélien si et seulement si $Z(G) = G$.

2) Montrer que $Z(\mathfrak{S}_n)$ est le groupe trivial pour tout $n \geqslant 3$.

3) On considère un sous-groupe $H \subset G$. Montrer que $Z(H)$ et $Z(G) \cap H$ sont reliés par une inclusion. Montrer grâce à un contre-exemple que l'inclusion réciproque est fausse en général.

4) (Bonus) Déterminer le centre du groupe $\mathrm{GL}_n(\mathbb{R})$ pour $n \geqslant 1$, et montrer qu'il est isomorphe au groupe $\mathbb{R}^*$.

11. Morphismes de groupes.

1) Soit $f : G \to G'$ un morphisme de groupes, avec G et G' finis. Pour $x \in G$, montrer que l'ordre de $f(x)$ divise $|G|$ et $|G'|$.

3. La notation Z vient de l'allemand *Zentrum*.

2) En déduire qu'il n'existe pas de morphisme de groupes non trivial d'un groupe d'ordre m vers un groupe d'ordre n si $m \wedge n = 1$.

12. Générateurs du groupe symétrique.

1) Soit un k-cycle $(i_1\ i_2\ \cdots\ i_k)$ et une permutation σ dans $\mathfrak{S}_n$. Montrer qu'on a l'égalité :
$$\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k)).$$

2) En déduire que $\mathfrak{S}_n$ est engendré par la transposition $(1\ 2)$ et le n-cycle $(1\ 2\ \cdots\ n)$.

13. Réflexions. Soient deux réflexions $s_1, s_2 \in \mathrm{O}_2(\mathbb{R})$. Démontrer que
$$s_1 s_2 = s_2 s_1 \quad \Longleftrightarrow \quad s_1 = \pm s_2.$$

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

15. Autour du groupe produit (examen 2023-24). Pour un groupe G et deux sous-groupes H, K de G, on considère les conditions suivantes.

(i) Pour tout $x \in G$, il existe $y \in H$ et $z \in K$ tels que $x = yz$.

(ii) $H \cap K = \{e\}$.

(iii) Les éléments de H et K commutent entre eux : $\forall y \in H$, $\forall z \in K$, $yz = zy$.

Les quatre questions sont indépendantes.

1) Soit $G = (\mathbb{Z}/11\mathbb{Z})^\times$, soit H le sous-groupe engendré par $\overline{3}$, et K le sous-groupe engendré par $\overline{10}$. Lister les éléments de H et K, et démontrer que H et K vérifient les conditions (i), (ii), (iii).

2) Soient G_1, G_2 deux groupes, et soit $G = G_1 \times G_2$ leur produit. On note e_1 et e_2 les éléments neutres respectifs de G_1 et G_2. Montrer que les ensembles $H = G_1 \times \{e_2\}$ et $K = \{e_1\} \times G_2$ sont deux sous-groupes de G qui vérifient les conditions (i), (ii), (iii).

3) Soit G un groupe et H, K deux sous-groupes qui vérifient les conditions (i), (ii), (iii).

   a) Démontrer que pour un élément $x \in G$, l'écriture $x = yz$ avec $y \in H$ et $z \in K$ est unique.

   b) Démontrer qu'il existe un isomorphisme entre le groupe produit $H \times K$ et G.

4) On pose $G = D_4$, le groupe diédral à 8 éléments. Trouver deux sous-groupes H, K de G, différents de $\{e\}$ et G, pour lesquels (i) et (ii) sont vrais mais pas (iii). On justifiera soigneusement ces faits.

Exercices supplémentaires, et approfondissement

16. Finitude. Soit G un groupe. Montrer que G est fini si et seulement s'il a un nombre fini de sous-groupes.

17. Différence symétrique. Soit E un ensemble. Pour des parties A, B de E on définit leur *différence symétrique*
$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

1) Démontrer que $(\mathcal{P}(E), \triangle)$ est un groupe abélien.

2) Démontrer qu'il est isomorphe au groupe $(\mathbb{Z}/2\mathbb{Z})^E$.

18. Générateurs du groupe alterné.

1) Démontrer qu'un produit de deux transpositions dans le groupe symétrique $\mathfrak{S}_n$ peut s'écrire comme un produit de 3-cycles.

2) En déduire que le groupe alterné $\mathfrak{A}_n$ est engendré par les 3-cycles.

3) Montrer que $\mathfrak{A}_n$ est engendré par les 3-cycles de la forme $(1\ i\ j)$ avec $2 \leqslant i < j \leqslant n$.

4) Montrer que $\mathfrak{A}_n$ est engendré par les 3-cycles de la forme $(1\ 2\ i)$ avec $3 \leqslant i \leqslant n$.

19. Groupe d'ordre pair. Soit G un groupe fini d'ordre pair. Montrer que G contient un élément d'ordre 2. *(Indication : considérer la partition de G dont les blocs sont les ensembles $\{x, x^{-1}\}$.)*

20. Sur l'ordre. Soit G un groupe, soient $a, b \in G$ tels que ab est d'ordre fini n. Montrer que ba est aussi d'ordre n.

21. Sur les axiomes des groupes (contrôle continu 2023-24). Les deux questions de cet exercice sont indépendantes. Dans la première question on montre qu'on peut simplifier l'axiomatique des groupes en demandant seulement l'existence d'un "neutre à gauche" et d'"inverses à gauche". Dans la deuxième question on voit que ça ne fonctionne pas si l'on mélange gauche et droite.

1) Soit G un ensemble muni d'une loi de composition interne $*$ qui vérifie les axiomes :

(i) Associativité : pour tous $x, y, z \in G$, $(x * y) * z = x * (y * z)$.

(ii) Neutre à gauche : il existe un élément $e \in G$ tel que pour tout $x \in G$, $e * x = x$.

(iii) Inverses à gauche : pour tout $x \in G$, il existe $x^{-1} \in G$ tel que $x^{-1} * x = e$.

a) Soit $y \in G$ tel que $y * y = y$. Montrer que $y = e$.

b) En utilisant la question précédente, montrer que pour tout $x \in G$ on a $x * x^{-1} = e$.

c) En déduire que pour tout $x \in G$ on a $x * e = x$.

2) Soit G un ensemble non vide dont on note e un des éléments. On définit une loi de composition interne $*$ sur G par la formule : $x * y = y$.

a) Montrer que cette loi vérifie les axiomes (i) et (ii) ci-dessus ainsi que l'axiome :
(iv) Inverses à droite : pour tout $x \in G$, il existe $x^{-1} \in G$ tel que $x * x^{-1} = e$.

b) Montrer que si G a au moins deux éléments alors $(G, *)$ n'est pas un groupe.

22. Groupe diédral et groupe symétrique. Montrer que D_n est isomorphe à un sous-groupe de $\mathfrak{S}_n$, pour $n \geqslant 3$.

23. Sous-groupes finis de $\mathrm{O}_2(\mathbb{R})$ (examen 2023-24). On rappelle la notation $\mathrm{O}_2(\mathbb{R})$ pour le groupe des automorphismes orthogonaux de $\mathbb{R}^2$, dont les éléments sont les rotations r_θ, pour $\theta \in \mathbb{R}$, et les réflexions s_Δ, pour Δ une droite vectorielle de $\mathbb{R}^2$. Les rotations forment le sous-groupe $\mathrm{SO}_2(\mathbb{R})$. Le but de cet exercice est de classifier les sous-groupes *finis* de $\mathrm{O}_2(\mathbb{R})$.

Plus précisément, on va montrer que les sous-groupes finis de $\mathrm{O}_2(\mathbb{R})$ sont les groupes cycliques C_n et les *conjugués* (définis ci-dessous) des groupes diédraux D_n.

Partie 1 : questions préliminaires sur les sous-groupes

1) Soit G un groupe et G' un sous-groupe de G. Pour H un autre sous-groupe de G, montrer que l'intersection $H \cap G'$ est un sous-groupe de G'.
2) Soit G un groupe et H un sous-groupe de G. Soit un élément $x \in G$. On note

$$xHx^{-1} = \{xhx^{-1},\, h \in H\},$$

qu'on appelle le *conjugué* de H par x.
   a) Montrer que xHx^{-1} est un sous-groupe de G.
   b) Montrer que les groupes H et xHx^{-1} sont isomorphes.

Partie 2 : sous-groupes finis de $\mathrm{SO}_2(\mathbb{R})$

Pour tout $n \in \mathbb{N}^*$ on note C_n l'ensemble des $f \in \mathrm{SO}_2(\mathbb{R})$ qui vérifient $f^n = \mathrm{id}_{\mathbb{R}^2}$.

3) Montrer que C_n est un sous-groupe cyclique de $\mathrm{SO}_2(\mathbb{R})$ et en donner un générateur.
4) Soit H un sous-groupe fini de $\mathrm{SO}_2(\mathbb{R})$. On note $n = |H|$ et on écrit $H = \{f_1, \ldots, f_n\}$.
   a) Justifier que pour tout $i \in \{1, \ldots, n\}$, f_i est d'ordre fini dans H.
   b) Pour tout $i \in \{1, \ldots, n\}$, on note k_i l'ordre de f_i dans H et on pose $N = k_1 \cdots k_n$. Montrer que pour tout $i \in \{1, \ldots, n\}$ on a $f_i^N = \mathrm{id}_{\mathbb{R}^2}$.
   c) En conclure que $H \subset C_N$, puis que $H = C_n$.

Partie 3 : sous-groupes finis de $\mathrm{O}_2(\mathbb{R})$

Pour la fin de l'exercice, soit H un sous-groupe fini de $\mathrm{O}_2(\mathbb{R})$.

5) Grâce aux questions 1) et 4)c), montrer qu'il existe $n \in \mathbb{N}^*$ tel que $H \cap \mathrm{SO}_2(\mathbb{R}) = C_n$.
6) On suppose maintentant que H n'est pas inclus dans $\mathrm{SO}_2(\mathbb{R})$, c'est-à-dire que H contient une réflexion s_Δ, pour Δ une droite vectorielle de $\mathbb{R}^2$. On note θ l'angle orienté entre l'axe des abscisses et la droite Δ. Le but de cette question est de montrer l'égalité :
$$H \stackrel{?}{=} r_\theta D_n r_\theta^{-1}.$$
On rappelle la notation $D_n \subset \mathrm{O}_2(\mathbb{R})$ pour le groupe diédral à $2n$ éléments. Il est engendré par la rotation d'angle $2\pi/n$, qu'on note r, et la réflexion le long de l'axe des abscisses, qu'on note s.
   a) On note $H' = r_\theta^{-1} H r_\theta$. En calculant $r_\theta^{-1} r r_\theta$ et $r_\theta^{-1} s_\Delta r_\theta$, montrer que $r \in H'$ et $s \in H'$.
   b) En conclure que $D_n \subset H'$.
   c) Montrer que $H' \subset D_n$. *(Indication : pour un élément $f \in H'$, faire une disjonction de cas selon $\det(f)$, et dans les deux cas se ramener à la question 5).)*
   d) En conclure que $H = r_\theta D_n r_\theta^{-1}$.

4 Introduction à la théorie des anneaux et des corps

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 $(x, y)(x', y') = (xx' - yy', xy' + x'y)$. Montrer que $\mathbb{R}^2$ muni de ces deux lois est un corps.

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

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

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

1) Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$. Est-il commutatif ? Est-il intègre ? Est-ce un corps ?
2) Pour $z = a + bi \in \mathbb{Z}[i]$ on pose $N(z) = |z|^2 = a^2 + b^2$, qu'on appelle la *norme*. Montrer qu'on a pour $z, z' \in \mathbb{Z}[i]$: $N(zz') = N(z)N(z')$.
3) Montrer que $z \in \mathbb{Z}[i]$ 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* :

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

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

4. 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.

5. Anneaux intègres finis. Soit A un anneau intègre *fini*. Montrer que A est un corps.

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

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

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.

7. Inversibles de $\mathbb{Z}/p\mathbb{Z}$. Soit p un nombre premier. Le but de cet exercice est de démontrer le résultat suivant :

Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

On démontre en fait un résultat plus général : pour un corps K et un sous-groupe fini $G \subset K^*$, G est cyclique. L'application au résultat ci-dessus est le cas $K = \mathbb{Z}/p\mathbb{Z}$ et $G = K^*$.

Soit donc K un corps, G un sous-groupe fini de K^*, et notons $n = |G|$.

1) Soit $d \in \mathbb{N}^*$ un diviseur de n.
   a) Montrer qu'il existe au plus d éléments $x \in G$ qui vérifient $x^d = 1$.
   b) Supposons qu'il existe un élément $g \in G$ d'ordre d. On note $\langle\, g \,\rangle$ le sous-groupe de G engendré par g. Montrer que $\langle\, g \,\rangle$ est égal à l'ensemble des éléments $x \in G$ qui vérifient $x^d = 1$.
   c) En déduire que s'il existe un élément d'ordre de d dans G alors il y a exactement $\varphi(d)$ éléments d'ordre d dans G.
2) Pour $d \in \mathbb{N}^*$ qui divise n on note X_d l'ensemble des éléments d'ordre d dans G. Montrer qu'on a une partition
$$G = \bigsqcup_{d|n} X_d.$$
En utilisant la formule de Gauss $\sum_{d|n} \varphi(d) = n$ (vue plus tôt dans le semestre), en déduire qu'il existe un élément d'ordre d dans G pour tout diviseur d de n. En déduire que G est cyclique.
3) Déterminer un générateur de $(\mathbb{Z}/7\mathbb{Z})^\times$.

8. Idéaux et inversibles. Soit A un anneau commutatif.

1) Soit I un idéal de A. Montrer que $I = A$ si et seulement si $1 \in I$.
2) Soit I un idéal de A. Montrer que $I = A$ si et seulement si I contient un inversible de A.
3) Soit $a \in A$. Montrer que $(a) = A$ si et seulement si a est inversible dans A.
4) Supposons que $A \neq \{0\}$. Montrer que A est un corps si et seulement si les seuls idéaux de A sont $\{0\}$ et A.

9. Idéaux de $\mathbb{Z}[X]$. 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 $f(-1)$ sont pairs. Montrer que I est un idéal de $\mathbb{Z}[X]$ et donner des générateurs de I.

10. Entiers de Gauss, bis. On se place dans l'anneau des entiers de Gauss
$$\mathbb{Z}[i] = \{a + bi\ ,\ a, b \in \mathbb{Z}\}\ .$$
On note $|z|$ le module d'un nombre complexe z. On rappelle la *norme* $N(z) = z\overline{z} = |z|^2 = a^2 + b^2$ pour $z = a + bi \in \mathbb{Z}[i]$. 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 $|z - z'| \leqslant \frac{\sqrt{2}}{2}\cdot$ (Un dessin pourra être utile !)

2) En déduire que $\mathbb{Z}[i]$ est un anneau euclidien pour la jauge euclidienne $\nu(z) = N(z)$. 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 $18 - i$.

11. 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 de nombres entiers si et seulement si $p \equiv 1 \pmod 4$.

1) Vérifier que ce théorème est vrai pour les nombres premiers $\leqslant 19$.

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, on écrit $p = 4n + 1$. On pose $x = (2n)!$.

   a) Montrer que $x^2 \equiv (p-1)! \pmod p$.

   b) En utilisant le théorème de Wilson (feuille de TD 2), en déduire que p divise $x^2 + 1$ dans $\mathbb{Z}$.

   c) En utilisant le lemme d'Euclide dans $\mathbb{Z}[i]$, en déduire que p n'est pas irréductible dans $\mathbb{Z}[i]$.

   d) En utilisant la norme N, déduire que p peut s'écrire comme somme de deux carrés de nombres entiers.

12. Polynômes à coefficients entiers.

1) Soit p un nombre premier. Soit $f \in \mathbb{Z}[X]$ un polynôme unitaire, et notons $\overline{f} \in (\mathbb{Z}/p\mathbb{Z})[X]$ sa réduction modulo p. Montrer que si $\overline{f}$ est irréductible alors f l'est aussi.

2) Montrer que les polynômes $X^3 + 27X^2 + 5X + 97$ et $X^4 + 6X^2 + 7$ sont irréductibles dans $\mathbb{Z}[X]$.

Exercices supplémentaires, et approfondissement

13. $1 - ab$ et $1 - ba$. Soit A un anneau et $a, b \in A$. Montrer que

$$1 - ab \in A^\times \iff 1 - ba \in A^\times.$$

14. Polynômes irréductibles. Soit K un corps. Montrer qu'il y a une infinité de polynômes irréductibles à coefficients dans K.

15. Idéaux de $K[X, Y]$. Soit K un corps.

1) Montrer que l'idéal (X, Y) de $K[X, Y]$ n'est pas principal.

2) Soit $n \in \mathbb{N}^*$ un entier. Trouver un idéal de $K[X, Y]$ qui peut être engendré par n éléments mais pas par $n - 1$ éléments.

16. Critère d'Eisenstein.

1) Soit $n \geqslant 1$, montrer que le polynôme $f_n = X^n + 2$ est irréductible dans $\mathbb{Z}[X]$. (Indication : réduire modulo 2).

2) Soit p un nombre premier. Montrer que le polynôme

$$\Phi_p = 1 + X + X^2 + \cdots + X^{p-1}$$

est irréductible dans $\mathbb{Z}[X]$. (Indication : appliquer la stratégie de la question précédente à $\Phi_p(X+1)$.)

17. Pas de Bézout ? On a vu en cours qu'il y a une notion de PGCD dans $\mathbb{Z}[X]$ puisque $\mathbb{Z}[X]$ est un anneau factoriel. Montrer que l'analogue du théorème de Bézout est faux dans cet anneau. De même dans $K[X, Y]$ avec K un corps.

18. Inversibles de $\mathbb{Z}[\sqrt{2}]$ (contrôle continu 2023-24). On définit :

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

On rappelle (vu en TD) que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$.

1) Montrer que l'application $\varphi : \mathbb{Z}^2 \to \mathbb{Z}[\sqrt{2}]$ défini par $\varphi(a, b) = a + b\sqrt{2}$ est un isomorphisme de groupes.
2) Montrer que les anneaux $\mathbb{Z}^2$ et $\mathbb{Z}[\sqrt{2}]$ ne sont pas isomorphes.
3) a) Pour un élément $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, on définit son *conjugé* $c(x) = a - b\sqrt{2}$. Montrer qu'on a la formule, pour $x, x' \in \mathbb{Z}[\sqrt{2}]$: $c(xx') = c(x)c(x')$.
   b) Pour un élément $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, on définit sa *norme* $N(x) = a^2 - 2b^2$. Montrer qu'on a les formules :

$$\forall x \in \mathbb{Z}[\sqrt{2}],\ N(x) = x\, c(x)$$

$$\forall x, x' \in \mathbb{Z}[\sqrt{2}],\ N(xx') = N(x)N(x')\ .$$

4) Montrer qu'un élément $x \in \mathbb{Z}[\sqrt{2}]$ est inversible si et seulement si $N(x) \in \{-1, 1\}$.

Le but de la suite de l'exercice est de montrer l'égalité :

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

5) Démontrer l'inclusion $\supset$.
6) Soit un élément $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ qui vérifie : $1 \leqslant a + b\sqrt{2} < 1 + \sqrt{2}$.
   a) Montrer qu'on a l'inégalité : $-1 \leqslant a - b\sqrt{2} \leqslant 1$.
   b) En déduire qu'on a nécessairement $a = 1$ puis $b = 0$.
7) Déduire de la question précédente que tout inversible de $\mathbb{Z}[\sqrt{2}]$ qui est $\geqslant 1$ est de la forme $(1 + \sqrt{2})^n$ pour un $n \in \mathbb{N}$.
8) En déduire l'égalité annoncée.

19. Sous-anneaux de $\mathbb{Z}^2$ (examen 2023-24). On se place dans l'anneau $\mathbb{Z}^2$. Pour tout $n \in \mathbb{N}$ on définit

$$A_n = \{(x, y) \in \mathbb{Z}^2 \mid x \equiv y \pmod{n}\}.$$

1) Montrer que A_n est un sous-anneau de $\mathbb{Z}^2$.
2) Soit A un sous-anneau de $\mathbb{Z}^2$. On veut montrer qu'il existe $n \in \mathbb{N}$ tel que $A = A_n$.
   a) Montrer que pour $k \in \mathbb{Z}$ on a : $(k, k) \in A$.
   b) Montrer que pour $k \in \mathbb{Z}$ on a : $(k, 0) \in A \iff (0, k) \in A$.

c) On suppose qu'il n'existe pas d'élément de A de la forme $(0,y)$ avec $y \neq 0$. Montrer que $A = A_0$. (Avant cela il est conseillé de réfléchir quelques instants à ce qu'est le sous-anneau A_0.)

d) On suppose qu'il existe un élément de A de la forme $(0,y)$ avec $y \neq 0$. Soit n le plus petit entier $\geqslant 1$ tel que $(0,n) \in A$. Montrer que $A = A_n$.

20. Quelques idéaux de $\mathbb{Z}[i]$ (examen 2023-24). On note

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

1) Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.
2) Soit I l'ensemble des $a + bi \in \mathbb{Z}[i]$ tels que a et b ont la même parité.
   a) Montrer que I est un idéal de $\mathbb{Z}[i]$.
   b) Montrer que $I = (1 + i)$.
3) Montrer que l'idéal $(3 + i, 5 + i)$ est égal à I.

21. Un anneau intègre qui n'est pas factoriel (examen 2023-24). On définit

$$\mathbb{Z}[i\sqrt{3}] = \{a + bi\sqrt{3}\ ,\ a, b \in \mathbb{Z}\}\ .$$

Pour gagner du temps, on admettra que $\mathbb{Z}[i\sqrt{3}]$ est un sous-anneau de $\mathbb{C}$. (Vous pouvez aussi le vérifier rapidement au brouillon.)

1) Pour un élément $z = a + bi\sqrt{3} \in \mathbb{Z}[i\sqrt{3}]$ on définit sa *norme*

$$N(z) = z\overline{z} = |z|^2 = a^2 + 3b^2\ .$$

   a) Montrer que pour tous $z, z' \in \mathbb{Z}[i\sqrt{3}]$ on a $N(zz') = N(z)N(z')$.
   b) Montrer qu'un $z \in \mathbb{Z}[i\sqrt{3}]$ est inversible si et seulement si $N(z) = 1$. Décrire le groupe $\mathbb{Z}[i\sqrt{3}]^\times$.
2) Dresser les listes des éléments de norme 2 et de norme 4 dans $\mathbb{Z}[i\sqrt{3}]$.
3) Montrer que tous les éléments de norme 4 sont irréductibles dans $\mathbb{Z}[i\sqrt{3}]$.
4) En déduire que $\mathbb{Z}[i\sqrt{3}]$ n'est pas un anneau factoriel. *(Indication : multiplier entre eux les éléments de norme 4.)*
5) (Question bonus) On a vu en TD que $\mathbb{Z}[i]$ est un anneau euclidien (et donc principal, donc factoriel). Si l'on essaye de copier la preuve de ce fait dans le cas de $\mathbb{Z}[i\sqrt{3}]$, qu'est-ce qui ne fonctionne pas ?