HAX501X – Groupes et anneaux 1
Feuilles de TD

Clément Dupont
Université de Montpellier
2023-2024

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.

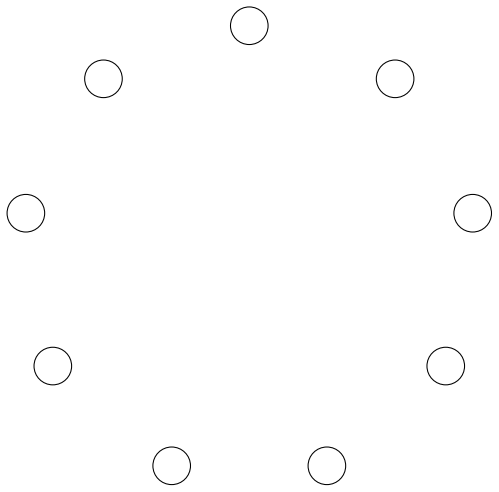
7. Racine. Soit $n \in \mathbb{N}$ qui n'est pas le carré d'un entier. Montrer que $\sqrt{n}$ est irrationnel.

8. 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.

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. 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.

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 $\overline{2}^{2023}$.

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

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

6. 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.

Exercices supplémentaires, et approfondissement

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

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

$$ax = \overline{0},$$

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.

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

8. 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.

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 l'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) 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 $g : E \to f(E)$.)

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

3 Introduction à la théorie des groupes

1. Exemples de 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. Sous-groupes d'ordre 4. On se place dans le groupe $G = (\mathbb{Z}/20\mathbb{Z})^\times$. Trouver deux sous-groupes d'ordre 4 de G, l'un cyclique et l'autre non cyclique.

6. Exemples de morphismes de groupes ? Ces choses-là sont-elles des morphismes de groupes ?

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

7. Inversion. Soit G un groupe et soit $\iota : G \to G$ l'application définie par $\iota(x) = x^{-1}$. Montrer que :

$$G \text{ est abélien} \iff \iota \text{ est un automorphisme de groupes.}$$

8. 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 ?)

3) Calculer le reste dans la division euclidienne de 6^{800} par 91.

9. 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) Déterminer le centre du groupe $\mathrm{GL}_n(\mathbb{R})$ pour $n \geqslant 1$, et montrer qu'il est isomorphe au groupe $\mathbb{R}^*$.
3) Montrer que $Z(\mathfrak{S}_n)$ est le groupe trivial pour tout $n \geqslant 3$.
4) 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.

10. Groupe des automorphismes, et conjugaison. Pour un groupe G on note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de groupes de G.

1) Montrer que $\mathrm{Aut}(G)$ est un sous-groupe de $\mathrm{Bij}(G)$.
2) Pour un élément $g \in G$ on définit une application

$$\gamma_g : G \to G\ ,\ x \mapsto gxg^{-1}.$$

Montrer qu'il s'agit d'un automorphisme de G. On l'appelle la *conjugaison* par g dans G.

3) Montrer que l'application

$$C : G \to \mathrm{Aut}(G)\ ,\ g \mapsto \gamma_g$$

est un morphisme de groupes. Quel est son noyau ?

11. Morphismes de groupes.

1) Soit $f : G \to G'$ un morphisme de groupes. Pour $x \in G$, montrer que l'ordre de $f(x)$ divise $|G|$ et $|G'|$.
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. 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 $2 \leqslant i < j \leqslant n$.

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

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

14. Réflexions. Soient deux réflexions $s_1, s_2 \in \mathrm{O}_2(\mathbb{R})$. Démontrer que

$$s_1 s_2 = s_2 s_1 \quad \Longleftrightarrow \quad s_1 = \pm s_2.$$

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

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

17. Un exercice de l'examen 2022-23 : la "réciproque du théorème de Lagrange" est fausse !

Le but de cet exercice est de montrer que la "réciproque du théorème de Lagrange" est fausse, c'est-à-dire qu'il existe un groupe fini G et un entier d qui divise $|G|$ tels que G n'a aucun sous-groupe d'ordre d.

Plus spécifiquement, on démontre que le groupe alterné $\mathfrak{A}_4$, qui est d'ordre 12, n'a aucun sous-groupe d'ordre 6. On rappelle que $\mathfrak{A}_4$ est défini comme le noyau du morphisme "signature" $\mathrm{sgn} : \mathfrak{S}_4 \to \{-1, 1\}$.

1) Soit G un groupe d'ordre pair, qu'on note $|G| = 2n$ avec $n \in \mathbb{N}^*$. Soit H un sous-groupe de G qui est d'ordre n. Soit $x \in G \setminus H$. On définit

$$Hx = \{hx,\ h \in H\}.$$

   a) Établir une bijection entre H et Hx. On justifiera bien qu'il s'agit d'une bijection.

   b) Démontrer que $H \cap Hx = \varnothing$.

   c) En déduire qu'on a $G = H \cup Hx$.

   d) Soit $h \in H$. Montrer que $(hx)^2 \in H$.
   (On pourra procéder par l'absurde en utilisant la question précédente.)

   e) En déduire que pour tout $g \in G$, $g^2 \in H$.

2) a) On considère maintenant le groupe $G = \mathfrak{A}_4$. Lister les éléments de $\mathfrak{A}_4$, et calculer leurs carrés.

   b) On suppose qu'il existe un sous-groupe H de $\mathfrak{A}_4$ qui est d'ordre 6. En utilisant la question 1)e), obtenir une contradiction.

Exercices supplémentaires, et approfondissement

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

19. 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 $(\mathbb{Z}/2\mathbb{Z})^E$.

20. 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 $\{x, x^{-1}\}$.)*

21. 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.

22. Un exercice de contrôle continu 2022-23 : $\mathrm{SL}_2(\mathbb{Z})$.

1) Soit une matrice
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
avec $a, b, c, d \in \mathbb{R}$. À quelle condition sur a, b, c, d a-t-on que A est inversible ? Exprimer alors l'inverse de A en fonction de a, b, c, d.

2) On définit
$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \;\middle|\; a, b, c, d \in \mathbb{Z} \;\text{ et }\; \det(A) = 1 \right\}.$$
Montrer que $\mathrm{SL}_2(\mathbb{Z})$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.

3) On définit les matrices
$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$
Vérifiez mentalement que S et T sont dans $\mathrm{SL}_2(\mathbb{Z})$.

a) Calculer S^{-1} et T^{-1}.

b) Pour $n \in \mathbb{Z}$, exprimer S^n en fonction de n. Déterminer l'ordre de S dans $\mathrm{SL}_2(\mathbb{Z})$.

c) Pour $n \in \mathbb{Z}$, exprimer T^n en fonction de n. Déterminer l'ordre de T dans $\mathrm{SL}_2(\mathbb{Z})$.

d) Pour une matrice
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
dans $\mathrm{SL}_2(\mathbb{Z})$, calculer SA et $T^n A$, pour $n \in \mathbb{Z}$.

4) Le but de cette question est de montrer que S et T engendrent le groupe $\mathrm{SL}_2(\mathbb{Z})$:
$$\mathrm{SL}_2(\mathbb{Z}) \stackrel{?}{=} \langle S, T \rangle.$$

a) Soit une matrice $A \in \mathrm{SL}_2(\mathbb{Z})$ de la forme
$$A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$
Montrer que $A \in \langle S, T \rangle$.

b) Soit maintenant une matrice $A \in \mathrm{SL}_2(\mathbb{Z})$ de la forme
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$
avec $c \neq 0$. On écrit la division euclidienne de a par c sous la forme $a = cq + r$. Grâce à la question 3)d), montrer qu'on peut trouver une matrice $X \in \langle S, T \rangle$ telle que le produit XA soit de la forme
$$XA = \begin{pmatrix} -c & -d \\ r & b' \end{pmatrix}.$$

c) Grâce à l'algorithme d'Euclide, montrer qu'il existe une matrice $Y \in \langle S, T \rangle$ telle que YA soit comme dans la question 4)a).

d) Déduire des questions précédentes que S et T engendrent $\mathrm{SL}_2(\mathbb{Z})$.

e) En suivant les étapes des questions précédentes, exprimer la matrice

$$A = \begin{pmatrix} 5 & 7 \\ 2 & 3 \end{pmatrix}$$

en fonction de S et T.

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 :

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

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

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

1) Soit $z \in \mathbb{C}$. Montrer qu'il existe $z' \in \mathbb{Z}[i]$ tel que $|z - z'| \leqslant \frac{\sqrt{2}}{2}$ · (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

$$1 - ab \in A^\times \quad \Longleftrightarrow \quad 1 - ba \in A^\times.$$

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.