TD : Algèbre Générale

Partie A : Structure de groupes

Exercice 1 : Indice d'un sous-groupe

Soit $(G,\cdot)$ un groupe, et H un sous-groupe de G. On définit sur G une relation d'équivalence (à vérifier quand-même) : $x\mathcal{R}y \Leftrightarrow \exists h \in H$ tel que $y = x.h$. On montre facilement que pour tout $x \in G$, la classe de x est $\dot{x} = x.H$. On pose alors $G/H = \{\dot{x} \text{ tel que } x \in G\}$, appelé ensemble quotient de G par H. L'indice de H dans G, noté $[G : H]$, est éventuellement infinie et définie par $[G : H] = \text{card}(G/H)$.

1. On suppose que H dit distingué dans G ($H \triangleleft G$), i.e., $g.H.g^{-1} \subset H$, $\forall g \in G$. Dire comment munir G/H d'une structure de groupe.
2. Montrer que dans, $(\mathbb{R},+)$, on a $[\mathbb{R},\mathbb{Z}] = +\infty$. Considérer les $\dot{x}$, où $x \in]0,1[$.
3. Montrer $(\mathbb{Z},+)$, on a $[\mathbb{Z},n\mathbb{Z}] = n$ et $[\mathbb{Z} : \{0\}] = +\infty$.
4. **Théorème de Lagrange**. On suppose que G est fini.
   - a. Montrer que $[G : H]$ est fini, avec $[G : H] = \dfrac{\text{card}(G)}{\text{card}(H)}$.
   - b. En déduire que $\text{card}(H)$ divise $\text{card}(G)$.
5. **Formule des indices (Multiplicativité)** : Soit $K \subset H \subset G$ trois sous-groupes emboîtés. Montrer que : $[G : K] = [G : H] \times [H : K]$.
6. **Sous-groupes d'indice 2** : Montrer que tout sous-groupe d'indice 2 dans G est distingué dans G.

Exercice 2 : Union de sous-groupes

1. Soit $(G,\cdot)$ un groupe, et soient H_1 et H_2 deux sous-groupes de G.
   - a. Montrer que $H_1 \cup H_2$ est un sous-groupe de G si et seulement si $H_1 \subseteq H_2$ ou $H_2 \subseteq H_1$.
     ☞ **Indication** : Raisonner par l'absurde.
   - b. On suppose qu'il existe un sous-groupe H de G tel que : $H \subset H_1 \cup H_2$. Montrer alors que H est inclus dans l'un des H_i.
     ☞ **Indication** : Raisonner par l'absurde.
2. **Théorème d'évitement** : On se propose de montrer par récurrence le cas général $n \geq 2$.
   Soient $H_1, H_2, \ldots, H_n$ des sous-groupes de G. On suppose qu'il existe un sous-groupe H de G tel que $H \subset \bigcup_{i=1}^{n} H_i$ et que que H n'est inclus dans aucun H_i
   On suppose de plus que tout élément dans G est d'ordre fini.
   - a. Justifier que pour chaque $i \in \{1,\ldots,n\}$, on peut trouver un élément $x_i \in H \setminus \left(\bigcup_{j\neq i} H_j\right)$. On pose alors $y_k = x_1^k \cdot x_2$ pour tout $k \geq 1$.
   - b. Montrer que $y_k \notin H_1$, pour tout $k \in \mathbb{N}^*$.
   - c. Montrer que pour tout $k \in \mathbb{N}^*$ tel que $\text{pgcd}(k,|x_1|) = 1$, on a $y_k = x_1.x_2 \notin H_2$,
   - d. En utilisant judicieusement le lemme des tiroirs, montrer que $\exists y_k \neq y_m$ appartiennent au même sous-groupe H_j ($j \geq 3$).
   - e. En déduire une contradiction, puis conclure.

Exercice 3 : Union de sous-groupes (quelques extensions)

1. On se propose de montrer dans cette question le théorème d'évitement, sans la condition que tout élément du groupe est d'ordre fini.
On reprend les mêmes notations que l'exercice précédent et on pose alors $y_k = x_1^k \cdot x_2$ pour tout $k \geq 1$.

   a. Montrer que le cas $y_k \in H_1$ est impossible.

   b. Montrer que le cas $y_k \in H_2, y_{k+1} \in H_2$ est aussi impossible.

   c. En déduire que parmi $2N$ éléments $(y_k)_{1 \leqslant k \leqslant 2N}$, le sous-groupe H_2 ne peut contenir que la moitié au maximum.

   d. En utilisant judicieusement le lemme des tiroirs, montrer que $\exists y_k \neq y_m$ appartiennent au même sous-groupe H_j $(j \geq 3)$.

   e. En déduire une contradiction, puis conclure.

2. On se propose de montrer dans cette question le théorème d'évitement dans le cas de sous-espaces vectoriels.
Plus précisément, on se propose de montrer par récurrence sur $n \geq 2$, le résultat suivant : Soit E un espace vectoriel. S'ils existent $F_1, F_2, \ldots, F_n$ des sous-espaces vectoriels de E tel que $E = \bigcup_{i=1}^{n} F_i$, alors l'un des F_i est égal à E.

   a. Discuter le cas $n = 2$. On suppose dans la suite le résultat vrai pour $n-1$ et on se propose de le montrer pour n.

   b. Discuter le cas où l'un des F_i est inclus dans la réunion des autres.
   On suppose dans la suite qu'aucun des F_i n'est inclus dans la réunion des autres.
   On suppose de plus que qu'aucun des F_i n'est égal à E.

   c. Justifier qu'on peut prendre $u \in E \setminus F_1$ et $v \in F_1 \setminus \bigcup_{i=2}^{n} F_i$.
   On pose alors $D = \{u + \lambda v \mid \lambda \in \mathbb{K}\}$ où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

   d. Montrer que $D \cap F_1 = \emptyset$.

   e. Montrer que pour tout $i \geqslant 2$, $D \cap F_i$ ne peut pas contenir deux éléments.

   f. En déduire une contradiction puis conclure.

Exercice 4 : Sous-groupes usuels

1. Montrer que tout sous-groupe (non nul) H de $(\mathbb{Z}, +)$ est de la forme $H = n\mathbb{Z}$, où $n \in \mathbb{N}^*$. Considérer $a = \min H \cap \mathbb{N}^*$.

2. Montrer que tout sous-groupe (non nul) H de $(\mathbb{R}, +)$ est soit de la forme $H = a\mathbb{Z}$, où $n \in \mathbb{R}^{+*}$, soit dense dans $\mathbb{R}$. Considérer $a = \inf H \cap \mathbb{R}^{+*}$.

3. Soit $f : \mathbb{R} \to \mathbb{R}$ fonction périodique. On pose $T_f = \{T \text{ période de } f\}$, c'est un sous groupe de $(\mathbb{R}, +)$.

   a. On suppose T_f dense dans $\mathbb{R}$ et f continue, montrer alors que $f = cte$.

   b. Soit $f, g : \mathbb{R} \to \mathbb{R}$ fonctions périodiques, telle que $T_f = a\mathbb{Z}$ et $T_g = b\mathbb{Z}$, avec $\frac{a}{b} \in Q$, montrer alors que $f + g$ et $f.g$ sont périodiques.

   c. Soit $(a, b) \in \mathbb{R}^* \times \mathbb{R}^*$, montrer que $\cos(ax) + \cos(bx)$ est périodique $\Leftrightarrow \frac{a}{b} \in \mathbb{Q}$.

   d. Donner un exemple de deux fonctions périodiques, dont la somme et produit ne sont pas périodiques.

Exercice 5 : Surjection et injection des translations

Soit G un ensemble non vide muni d'une loi de composition interne . associative. Pour tout $a \in G$, on pose : $\phi_a : \begin{array}{ccc} G & \to & G \\ x & \mapsto & a.x \end{array}$ $\psi_a : \begin{array}{ccc} G & \to & G \\ x & \mapsto & x.a \end{array}$

1. On suppose que toutes les translations à gauche et à droite sont surjectives, montrer alors que $(G, .)$ est un groupe.

2. On suppose que G est fini et que que toutes les translations à gauche et à droite sont injectives, montrer alors que $(G, .)$ est un groupe.

3. Montrer que la question précédente n'est plus vraie, si G est infini.

4. Soit H une partie finie de G non vide, stable par . . Montrer que H est un sous-groupe de $(G, .)$

5. Montrer, que ces questions ne sont plus vraies, si . est non associative.

Partie B : Ordre d'un élément

Dans toute la suite $(G,.)$ désigne un groupe. Pour tout $a \in G$.

☞ $|a|$ désigne l'ordre de a, éventuellement infini ;

☞ $< a >$ désigne le sous-groupe engendré par a ;

☞ Pour tout ensemble X, on pose $|X| = \text{card}(X)$, éventuellement infini.

Exercice 6 : Le Premier Théorème d'isomorphisme

(1) $f : G \to H$ un morphisme de groupes. Montrer que l'application

$$\begin{array}{rccc} \tilde{f} : & G/\ker f & \to & \text{Im f} \\ & \dot{x} & \mapsto & f(x) \end{array}$$

est un isomorphisme de groupe.

(2) En déduire que $[G : \ker f] = |\text{Im f}|$, et que dans le cas fini, on a $|G| = |\ker f|.|\text{Im f}|$.

(3) Application : Montrer que $|\mathfrak{A}_n| = \dfrac{n!}{2}$, où $\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n \text{ tel que } \varepsilon(\sigma) = 1\}$.

Exercice 7 : Un classique

Pour tout $n \in \mathbb{N}^*$, on pose $\mathbb{U}_n = \{z \in \mathbb{C}^* \text{ tel que } z^n = 1\}$ et $H = \bigcup_{n=1}^{+\infty} \mathbb{U}_n$.

(1) Montrer que H est un sous-groupe de $(\mathbb{C}^*, \times)$.

(2) Montrer que H est infini, alors que tous ses éléments sont d'ordre fini.

(3) Montrer que $H = \{z = \mathrm{e}^{2ir\pi} \text{ tel que } r \in \mathbb{Q}\}$.

(4) En déduire que H est dense dans $\mathbb{C}$.

Exercice 8 : Propriétés Classiques

Soit $(a, b) \in G^2$, d'ordres finis.

(1) Montrer que $< a^{-1} >=< a >$ puis que $|a^{-1}| = |a|$.

(2) **Théorème de Lagrange** On suppose G est fini, montrer que $|a|$ divise $\text{card}(G)$, en particulier $a^{\text{card}(G)} = e_G$.

(3) En déduire que tout groupe fini de cardinal premier est cyclique.

(4) Montrer que $|bab^{-1}| = |a|$.

(5) Montrer que $|a.b| = |b.a|$.

(6) On suppose dans cette question que $a.b = b.a$

- [a] Montrer que $|a.b|$ divise $\text{ppcm}(|a|, |b|)$.
- [b] Donner un exemple où $|a.b| \neq \text{ppcm}(|a|, |b|)$.
- [c] On suppose dans cette question que $< a > \cap < b >= \{e_G\}$. Montrer alors que : $|a.b| = \text{ppcm}(|a|, |b|)$

(7) Soit $f : G \to G'$ un morphisme de groupe.

- [a] Montrer que $|f(a)|$ divise $|a|$.
- [b] Donner un exemple où $|f(a)| \neq |a|$.
- [c] On suppose de plus f injective, montrer alors que $|f(a)| = |a|$.

(8)
- [a] Montrer que $\forall k \in N$, on a : $|a^k| = \frac{|a|}{\text{pgcd}(k,|a|)}$
- [b] En déduire que si G est cyclique de cardinal n, alors il admet exactement $\varphi(n)$ générateurs.
  ☞ **Rappel** : $\varphi(n) = \text{card}\{k \in [|1, n|] \text{ tel que } \text{pgcd}(k, n) = 1\}$, désigne la fonction indicatrice d'Euler.
- [c] Par n points fixes sur un le cercle unité, combien peut-on dessiner de polygones réguliers à n-cotés.

(9) Énoncer et démontrer le petit et grand théorèmes de Fermat.

Exercice 9 : Action d'un groupe (les basics)

Soit $(G,.)$ un groupe et X un ensemble non vide.

- ☞ Une action (à gauche) de G sur X est une application $\begin{array}{ccc} G\times X & \longrightarrow & X \\ (g,x) & \longmapsto & g\cdot x \end{array}$, vérifiant les deux axiomes :
  - ✌ $\forall x\in X,\quad e_G\cdot x=x$
  - ✌ $\forall g,h\in G,\ \forall x\in X,\quad (gh)\cdot x=g\cdot(h\cdot x)$
- ☞ Pour tout $x\in X$, $\mathcal{O}(x)=G\cdot x=\{g\cdot x\mid g\in G\}\subset X$, désigne l'orbite de x.
- ☞ Pour tout $x\in X$, $\mathrm{Stab}(x)=G_x=\{g\in G\mid g\cdot x=x\}\subset G$, désigne le stabilisateur de x.
- ☞ Pour tout $g\in G$, on pose $X^g=\mathrm{Fix}(g)=\{x\in X\mid g\cdot x=x\}\subset X$.
- ☞ On pose aussi $X^G=\mathrm{Fix}(G)=\{x\in X\mid \forall g\in G, g\cdot x=x\}\subset X$.
- ☞ L'action est dite libre quand $\forall x\in X,\quad \mathrm{Stab}(x)=\{e\}$.
- ☞ L'action est dite transitive s'il n'y a qu'une seule orbite : $X=\mathcal{O}(x),\forall x\in X$.
- ☞ L'action est dite simplement transitive, quand elle est à la fois transitive et libre.

1. Montrer que définir une action de G sur X équivaut à définir un morphisme de groupes $\phi: G\longrightarrow \mathfrak{S}(X)$, où $\mathfrak{S}(X)$ est le groupe des bijections de X dans lui-même.
2. Montrer alors que $\ker(\phi)=\bigcap_{x\in X}\mathrm{Stab}(x)$.
3. Montrer que la relation $x\sim y \iff \exists g\in G, y=g\cdot x$ est une relation d'équivalence sur X, dont les classes d'équivalence sont les orbites $\mathcal{O}(x)$.
4. Montrer que l'action est fidèle si et seulement si ϕ est injectif.
5. Montrer que l'action est transitive $\Leftrightarrow \forall x,y\in X,\exists g\in G,$ tel que $y=g\cdot x$.
6. Montrer que l'action est simplement transitive si et seulement si $\forall x,y\in X,\exists! g\in G,$ tel que $y=g\cdot x$.

Exercice 10 : Action d'un groupe (les classics)

Soit $(G,.)$ un groupe qui agit sur X un ensemble fini non vide.

1. Fixons $x\in X$ et posons $H=\mathrm{Stab}(x)$. Notons $G/H=\{gH\mid g\in G\}$ et considérons l'application : $f:\ \begin{array}{ccc} G/H & \longrightarrow & \mathcal{O}(x) \\ gH & \longmapsto & g\cdot x \end{array}$.
   Montrer que f est bien définie et bijective.
2. En déduire que $|\mathcal{O}(x)|=\dfrac{|G|}{|\mathrm{Stab}(x)|}, \forall x\in X$ (**Théorème Orbite-Stabilisateur**).
3. soit $\mathcal{R}\subset X$ est un système de représentants des différentes orbites X.
   Montrer que $|X|=\displaystyle\sum_{x\in\mathcal{R}}|\mathcal{O}(x)|=\sum_{x\in\mathcal{R}}\frac{|G|}{|\mathrm{Stab}(x)|}$ (**Formule des orbites**).
4. Soit $(G,*)$ un groupe fini de cardinal n, qui agit sur lui-même par translation à gauche $(g\cdot x=g*x)$.
   - a Montrer que cette action est libre, fidèle et transitive.
   - b En déduire que G est isomorphe à $\mathfrak{S}_n$ (**Théorème de Cayley**).

Exercice 11 : Lemme de Burnside

Soit G un groupe fini agissant sur un ensemble fini X.
$X/G|$ désigne le nombre d'orbites de cette action.
Considérons l'ensemble $E=\{(g,x)\in G\times X\mid g\cdot x=x\}$.

1. Vérifier que $|E|=\displaystyle\sum_{g\in G}|X^g|=\sum_{x\in X}|\mathrm{Stab}(x)|$.
2. En déduire que $|X/G|=\frac{1}{|G|}\sum_{g\in G}|X^g|$.
   - ☞ **Indication** : Utiliser le théorème orbite-stabilisateur

Exercice 12 : Quelques propriétés du groupe symétrique

1. On pose $Z(\mathfrak{S}_n) = \{\sigma \in \mathfrak{S}_n \mid \forall \tau \in \mathfrak{S}_n,\ \sigma\tau = \tau\sigma\}$. (Centre de $\mathfrak{S}_n$).
On suppose ici que $n \geqslant 3$ et que $Z(\mathfrak{S}_n) \neq \{\text{id}\}$.
   - a. Justifier l'existence de $\sigma \in Z(\mathfrak{S}_n)$, $i, j \in \{1, \dots, n\}$ tel que $j = \sigma(i) \neq i$ et $k \in \{1, \dots, n\}$ distinct de i et de j. On pose $\tau = (j\ k)$.
   - b. Calculer $(\sigma \circ \tau)(i)$, et $(\tau \circ \sigma)(i)$. En déduire une contradiction.
2. On suppose $n \geqslant 2$. Montrer que $\sigma(i\ j)\sigma^{-1} = (\sigma(i)\ \sigma(j))$, pour tout $\sigma \in \mathfrak{S}_n$, et tous $i, j \in [|1, n|]$. (**Formule de conjugaison**)
3. Généraliser cette formule pour tous les k-cycles.
4. Calculer $(1\ i) \circ (1\ j) \circ (1\ i)^{-1}$. En déduire que $\{(1\ i) \mid 2 \leq i \leq n\}$ engendre $\mathfrak{S}_n$
5. On pose $\tau = (1\ 2)$ et $c = (1\ 2\ \dots\ n)$.
   - a. Calculer $(i\ i+1) \circ (1\ i) \circ (i\ i+1)^{-1}$
   - b. Montrer que $\forall k \in \{0, 1, \dots, n-2\}$, on a $c^k(1) = 1 + k$, $c^k(2) = 2 + k$.
   - c. En déduire que $\mathfrak{S}_n = \langle \tau, c \rangle$

Exercice 13 : Quelques propriétés du groupe alterné

Soit $n \geqslant 2$. On pose $\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n \text{ tel que } \varepsilon(\sigma) = 1\}$

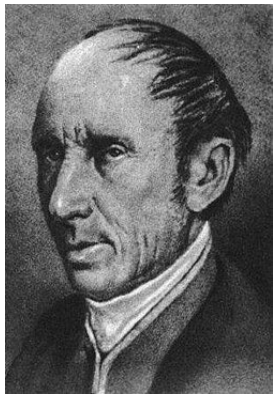
1. Justifier que $\mathfrak{A}_n$ est un sous-groupe de $(\mathfrak{S}_n, \circ)$.
2. Montrer que l'application $f : \begin{array}{ccc} \mathfrak{A}_n & \to & \mathfrak{S}_n \setminus \mathfrak{A}_n \\ \sigma & \mapsto & (1\ 2).\sigma \end{array}$ est bien définie et bijective.
3. En déduire que $|\mathfrak{A}_n| = \dfrac{n!}{2}$.
4. On suppose $n \geqslant 3$. Montrer que $\mathfrak{A}_n$ est engendré par les 3-cycles.
   - ☞ **Indication** : Considérer a, b, c, d des éléments distincts de $\{1, \dots, n\}$. Exprimer les produit $(a\ b)(c\ d)$ et $(a\ b)(a\ c)$ sous la forme d'un unique 3-cycle.

Exercice 14 : Théorème de Cauchy

Soient G un groupe fini et p un nombre premier divisant l'ordre de G.
Soit $X = \{(x_1, \dots, x_p) \in G^p \mid x_1.x_2 \cdots x_p = e\}$.
On fait agir le groupe $\mathbb{Z}/p\mathbb{Z}$ sur X par décalage circulaire, par exemple

- ☞ $\dot{1} \cdot (x_1, x_2, \dots, x_p) = (x_2, \dots, x_p, x_1)$
- ☞ $\dot{2} \cdot (x_1, x_2, \dots, x_p) = (x_3, \dots, x_1, x_2)$

1. Donner la forme générale de $\dot{k} \cdot (x_1, x_2, \dots, x_p)$.
2. Justifier que $|X| = |G|^{p-1}$.
3. Justifier que p divise $\mathcal{O}(x)$, $\forall x \in X \setminus \text{Fix}(\mathbb{Z}/p\mathbb{Z})$.
4. En déduire que p divise $|\text{Fix}(\mathbb{Z}/p\mathbb{Z})|$.
   - ☞ **Indication** : Utiliser la formule des orbites.
5. Vérifier que $\text{Fix}(\mathbb{Z}/p\mathbb{Z}) = \{(x, x, \dots, x) \in G^p \text{ tel que } x^p = e\}$
6. Vérifier que $\text{Fix}(\mathbb{Z}/p\mathbb{Z})$ est non vide, puis en déduire que $|F| \geq p \geq 2$.
7. En déduire qu'il existe donc au moins un élément $x \neq e$ tel que $x^p = e$.
8. Conclure alors G contient au moins un élément d'ordre p.



Augustin-Louis Cauchy (1789-1857) est un mathématicien français majeur, pionnier de l'analyse moderne et de l'analyse complexe, auquel on doit la définition rigoureuse des notions de limite, de continuité et de convergence des séries, ainsi que le célèbre théorème de Cauchy en théorie des groupes finis et la formule intégrale de Cauchy.
Esprit exceptionnellement prolifique, il est le deuxième mathématicien le plus publié de l'histoire derrière Leonhard Euler, avec près de 800 articles et un cours d'Analyse rédigé pour l'École Polytechnique.
Son nom figure parmi les 72 savants inscrits sur la tour Eiffel en hommage à ses contributions exceptionnelles.

Partie C : Structures d'anneau et corps

Exercice 15 : Caractéristique d'un anneau commutatif

Soit $(A, +, .)$ un anneau commutatif.
On pose $\text{car}(A) = \min\{k \in \mathbb{N}^* \text{ tel que } k.1_A = O_A\}$, quand c'est bien défini. Dans le cas contraire, on pose $\text{car}(A) = 0$. $\text{car}(A)$ s'appelle la **caractéristique** de A.

1. Montrer que $\text{car}(\mathbb{Z}/n\mathbb{Z}) = n$. Donner $\text{car}(\mathbb{Z})$.
2. Montrer que si B est un sous-anneau de A, alors $\text{car}(B) = \text{car}(A)$.
3. En déduire $\text{car}(\mathbb{Q})$, $\text{car}(\mathbb{R})$ et $\text{car}(\mathbb{C})$.
4. On suppose que A est intègre (resp. corps). Montrer que $\text{car}(A)$ est nul ou nombre premier.
5. On suppose $\text{car}(A) \neq 0$.
   Soit $k \in \mathbb{N}^*$ tel que $k.1_A = 0_A$, montrer que $\text{car}(A)$ divise k.
6. On suppose qu'il existe $f : A \to B$ un morphisme d'anneau.
   a. Montrer que si $\text{car}(B) \neq 0$, alors $\text{car}(B)$ divise $\text{car}(A)$.
   b. Montrer que si $\text{car}(B) = 0$, alors $\text{car}(A) = 0$.
7. Montrer qu'il n'existe pas de morphisme de corps entre deux corps n'ayant pas la même caractéristique
8. Soient A et B deux anneaux de caractéristiques non nulles.
   Monter que $\text{car}(A \times B) = \text{ppcm}(\text{car}(A), \text{car}(B))$.
9. Montrer que la relation est encore valable si l'une des caractéristiques est nulle.

Exercice 16 : Morphismes d'anneaux usuels

1. Soit $f : \mathbb{Z} \to \mathbb{Z}$ un morphisme d'anneaux, montrer que $f(n) = n$, $\forall n \in \mathbb{Z}$.
2. Soit $f : \mathbb{Q} \to \mathbb{Q}$ un morphisme d'anneaux, montrer que $f(r) = r$, $\forall r \in \mathbb{Q}$.
3. Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme d'anneaux.
   Montrer que $f(x) \geqslant 0$, $\forall x \geqslant 0$. En déduire que f est croissante, puis que $f = \text{id}_{\mathbb{R}}$.

   ☞ **Indication** : Utiliser la densité de $\mathbb{Q}$ dans $\mathbb{R}$.
4. Soit $f : \mathbb{C} \to \mathbb{C}$ un morphisme d'anneaux.
   Montrer que $f(i) = \pm i$. En déduire que $f(z) = z$ ou bien $f(z) = \overline{z}$, $\forall z \in \mathbb{C}$.
5. En déduire qu'on ne peut pas trouver d'isomorphisme d'anneaux entre deux ensembles parmi les suivants : $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.

Exercice 17 : Anneau de Gauss

Soit $\omega \in \mathbb{C} \setminus \mathbb{Z}$ tel que $\omega^2 \in \mathbb{Z}$, on pose $\mathbb{Z}[\omega] = \{z = a + b\omega \text{ tel que } (a, b) \in \mathbb{Z}^2\}$.
Pour tout $z = a + b\omega \in \mathbb{Z}[\omega]$, on pose $\overline{z} = a - b\omega$ et $N(z) = a^2 - b^2w^2$.

1. Vérifier que $\mathbb{Z}[\omega]$ est un sous-anneau de $(\mathbb{C}, +, .)$.
2. Vérifier que $N(z) = z.\overline{z}$, pour tout $z \in \mathbb{Z}[\omega]$.
3. Vérifier que $\overline{z.z'} = \overline{z}.\overline{z'}$, pour tout $(z, z') \in \mathbb{Z}[\omega]^2$.
4. En déduire que $N(z.z') = N(z).N(z')$, pour tout $(z, z') \in \mathbb{Z}[\omega]^2$.
5. En déduire que z est inversible dans $\mathbb{Z}[\omega] \Leftrightarrow N(z) = \pm 1$
6. Donner tous les éléments inversible de $\mathbb{Z}[i]$.

Carl Friedrich Gauss (1777-1855) est un mathématicien, astronome et physicien allemand, considéré comme l'un des plus grands génies de l'histoire.
Surnommé le « Prince des mathématiciens », il a démontré un talent prodigieux pour le calcul mental dès son plus jeune âge.

Partie D : Notion d'idéal

Exercice 18 : Opérations sur les idéaux

Soient I et J deux idéaux d'un anneau commutatif A.

1. Montrer que l'intersection $I \cap J$ est un idéal de A.
2. Montrer que la somme $I + J = \{x + y \mid x \in I, y \in J\}$ est un idéal de A.
3. Montrer que la réunion $I \cup J$ est un idéal de A si et seulement si $I \subset J$ ou $J \subset I$.

Exercice 19 : Idéaux d'un corps

Soit I un idéal d'un anneau commutatif A.

1. Montrer que $I = A$ si et seulement si I contient 1_A.
2. Montrer que $I = A$ si et seulement si I contient un élément inversible de A.
3. En déduire que les seuls idéaux d'un corps K sont $\{0_K\}$ et K.
4. En déduire que tout morphisme de corps est soit nul soit injectif.

Exercice 20 : Idéaux vs. morphismes d'anneaux

Soit A, B deux anneaux commutatifs, $\varphi : A \longrightarrow B$ un morphisme d'anneaux et $\mathcal{I}, \mathcal{J}$ deux idéaux de A et B respectivement

1. Montrer que $\varphi^{-1}(\mathcal{J})$ est un idéal de A.
2. On suppose que φ est surjectif, montrer alors que $\varphi(\mathcal{I})$ est un idéal de B.
3. Montrer à l'aide d'un contre-exemple, que ce résultat n'est pas toujours vrai quand φ n'est pas surjective.

Exercice 21 : Idéaux et arithmétique

Soient $m, n \geq 2$ deux entiers naturels

1. Montrer que $n\mathbb{Z} \cap m\mathbb{Z} = \text{ppcm}(n, m)\mathbb{Z}$ et que $n\mathbb{Z} + m\mathbb{Z} = \text{pgcd}(n, m)\mathbb{Z}$.
2. En déduire une démonstration du théorème de Bezout

Exercice 22 : Radical d'un idéal

Soit I un idéal d'un anneau commutatif A. On définit le radical de I, noté $\sqrt{I}$, par :

$$\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N}^*, x^n \in I\}$$

1. Montrer que $I \subset \sqrt{I}$.
2. Montrer que $\sqrt{I}$ est un idéal de A.
3. Déterminer $\sqrt{\{0_A\}}$.
4. En déduire que, dans le cas où ils commutent, le produit et somme de deux éléments nilpotents sont aussi nilpotents
5. Donner deux matrices nilpotentes dont la somme et le produit ne le sont pas.
6. Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.
7. Montrer que $I = A \Leftrightarrow \sqrt{I} = A$.
8. Soit J un autre idéal de A.
   - [a] Montrer que $I \subset J \Rightarrow \sqrt{I} \subset \sqrt{J}$.
   - [b] Montrer que $\sqrt{I.J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
   - [c] Montrer que $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.
9. Soit $n \in \mathbb{Z}$ un entier relatif supérieur ou égal à 2. On considère sa décomposition en facteurs premiers : $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad (\alpha_i \geq 1)$.
   Montrer que $\sqrt{n\mathbb{Z}} = (p_1 p_2 \cdots p_k)\mathbb{Z}$.

Exercice 23 : Un classic

Soit A un anneau intègre ayant un nombre fini d'idéaux. Montrer que A est un corps.

☞ **Indication** : Soit $a \in A \setminus \{0\}$. Considérons la suite d'idéaux principaux $(\langle a^n \rangle)_{n\geq 1}$, puis montrer que A est inversible.

Exercice 24 : Anneau quotient

Soit A un anneau commutatif, I un idéal de A. On définit la relation équivalence (à vérifier quand même) sur A par :

$$\text{Pour tout}(x,y) \in A^2,\ x\mathcal{R}y \Leftrightarrow x-y \in I.$$

On pose alors $A/I = \{\dot{x} \text{ tel que } x \in A\}$, appelé **ensemble quotient**.

(1) Donner $\dot{x}$, pour tout $x \in A$. En déduire que $\dot{0} = I$.

(2) Vérifier que $\dot{x} = \dot{0} = I \Leftrightarrow x \in I$.

(3) Sur A/I, on définit les opérations suivantes : $\dot{x} + \dot{y} = \dot{\overline{x+y}},\ \dot{x}.\dot{y} = \dot{\overline{x.y}}$

[a] Montrer que ces opérations sont bien définies, et qu'elle définissent des lois de composition internes sur A/I.

[b] Vérifier$(A/I, +, .)$ est un anneau commutatif.

(4) soit $f : A \to B$ un morphisme d'anneaux commutatifs. On pose

$$\begin{array}{rccc} \overline{f}: & A/\ker(f) & \to & \mathrm{Im}(f) \\ & \overline{x} & \mapsto & \overline{f}(\overline{x}) = f(x) \end{array}$$

[a] Montrer que $\overline{f}$ est bien définie.

[b] Vérifier que $\overline{f}$ est un isomorphisme d'anneaux.

(5) Montrer que $A/\sqrt{0}$ ne contient pas d'éléments nilpotents non nuls

Exercice 25 : Théorème de correspondance des idéaux

Soient A un anneau commutatif unitaire, J un idéal de A.
On considère les applications suivantes :

☞ $\begin{array}{rccc} \pi: & A & \to & A/I \\ & x & \mapsto & \dot{x} \end{array}$

☞ $\begin{array}{rccc} \phi: & \{J \text{ idéal de } A \text{ tel que } I \subset J\} & \to & \{K \text{ idéal de } A/I\} \\ & J & \mapsto & J/I \end{array}$

☞ $\begin{array}{rccc} \psi: & \{K \text{ idéal de } A/I\} & \to & \{J \text{ idéal de } A \text{ tel que } I \subset J\} \\ & K & \mapsto & \pi^{-1}(K) \end{array}$

(1) Montrer que ces trois applications sont bien définies.

(2) Vérifier que $\phi \circ \psi = \mathrm{Id}$ et $\psi \circ \phi = \mathrm{Id}$.

(3) Conclure un résultat.

Exercice 26 : Idéal Premier

Soit A un anneau commutatif.
Un idéal $I \neq A$ est dit premier si et seulement si il vérifie : $x.y \in I \Rightarrow x \in I$ ou $y \in I$.
Un élément non nul et non inversible $x \in A$ est dit premier si et seulement si il vérifie : x divise $a.b \Rightarrow x$ divise a ou x divise b.

(1) Montrer que I est premier $\Leftrightarrow A/I$ est un anneau intègre.

(2) Montrer que I est premier $\Leftrightarrow A \setminus I$ est stable pour la loi .

(3) Montrer que x est premier $\Leftrightarrow \langle x \rangle = xA$ est premier.

(4) Donner les éléments premiers de $\mathbb{Z}$, puis ceux de $\mathbb{K}[X]$.

(5) On suppose que tout idéal de A est premier.

[a] Montrer que A est intègre.

[b] $x \in A \setminus \{0_A\}$. Montrer que $x \in \langle x^2 \rangle$.
En déduire que x est inversible, puis conclure un résultat.

Exercice 27 : Idéal Maximal

Soit A un anneau commutatif.
Un idéal $I \neq A$ est dit maximal si et seulement si il est maximal (pour l'inclusion) parmi les idéaux distincts de A.
Autrement dit : si J est un idéal tel que $I \subset J$, alors $J = A$ ou $J = I$.
Un élément non nul et non inversible $x \in A$ est dit premier si et seulement si il vérifie : x divise $a.b \Rightarrow x$ divise a ou x divise b.

1. Montrer que I est maximal $\Leftrightarrow A/I$ est un corps.
2. En déduire que tout idéal maximal est premier.
3. Donner un exemple d'idéal premier non maximal.
4. On suppose que contient un nombre fini d'idéaux.
   Montrer que tout idéal premier de A est maximal.

Exercice 28 : Éléments Irréductibles

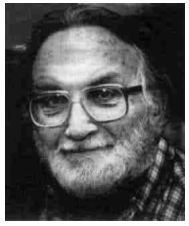
Soit A anneau intègre
$x \in A$ est dit irréductible si et seulement si x est non inversible, et si $x = a.b$, alors a ou bien b est inversible.

1. Préciser les éléments irréductibles dans Z, Z/nZ, $\mathbb{K}[X]$ et $\mathcal{M}_n(\mathbb{K})$.
2. Montrer que $x \in A$ est irréductible si et seulement si $\langle x \rangle$ est non nul et maximal (pour l'inclusion) parmi les idéaux de A qui sont principaux et distincts de A.
3. Montrer que dans un anneau intègre, un élément premier est toujours irréductible.
4. Montrer que dans un anneau principal et intègre, tout élément irréductible est premier.
5. Donner un exemple d'élément irréductible, mais non premier.

Exercice 29 : Théorème de Krull

Soit A un anneau commutatif, non nul.
On rappelle d'abord le **lemme de Zorn** :
Soit $(E, \leq)$ un ensemble ordonné non vide.
Si E est inductif (c'est-à-dire si tout sous-ensemble totalement ordonné de E admet un majorant dans E), alors E admet au moins un élément maximal.

1. Vérifier que l'ensemble $\mathcal{E} = \{J \text{ idéal de } A \text{ tel que } J \neq A\}$, ordonné par l'inclusion $\subset$, satisfait les conditions du lemme de Zorn.
2. Montrer que A admet au moins un idéal maximal (**Théorème de Krull**).
3. En déduire que si $I \neq A$ est un idéal de A, il existe un idéal maximal de A contenant I.
4. Soit $x \in A$, un élément non nilpotent, on pose : $S = \{x^n \text{ tel que } n \in \mathbb{N}\}$.
   - a. Vérifier que l'ensemble $\mathcal{F} = \{J \text{ idéal de } A \text{ tel que } J \cap S = \emptyset\}$, ordonné par l'inclusion $\subset$, satisfait les conditions du lemme de Zorn.
   - b. En déduire $\mathcal{F}$ admet un élément maximal P.
   - c. Montrer que P est premier.
   - d. En déduire que l'intersection de tous les idéaux premiers de A est égale à $\sqrt{0_A}$.
5. Soit I un idéal de A.
   Montrer qu'en général l'intersection de tous les idéaux premiers de A contenant I est égale à $\sqrt{I}$.



Max Zorn (1906-1993) : Mathématicien allemand. Exilé aux États-Unis, il fuit l'Allemagne nazie en 1933 et réalise toute la suite de sa carrière universitaire aux États-Unis (Yale, UCLA, Indiana).
Il est surtout connu pour le lemme de Zorn, qui est équivalent à l'axiome du choix modulo les axiomes de la théorie des ensembles de Zermelo-Fraenkel et qui trouve des applications dans des domaines très variés.

Partie E : Arithmétique dans Z

Exercice 30 : Classic

Soit p nombre premier

1. Justifier que p divise $\mathcal{A}_p^k$ pour tout $k \in [|1, p-1|]$.
2. En déduire que p divise $\binom{k}{p}$ pour tout $k \in [|1, p-1|]$.
3. En déduire que $(x+y)^p \equiv x^p + y^p \pmod{p}$ pour tout $(x, y) \in Z^2$.

Exercice 31 : Classic

Soient $a \in \mathbb{N}, a \geq 2$, $(m, n) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $m \geq n$.
On pose $m = qn + r$ avec $0 \leq r < n$.

1. Montrer que : $\exists b \in \mathbb{N}$; $a^m - 1 = (a^n - 1)b + a^r - 1$.
2. Montrer que : $(a^m - 1) \wedge (a^n - 1) = a^{m \wedge n} - 1$.

   ☞ **Indication** : Penser à utiliser l'algorithme d'Euclide.
3. Montrer que : $(a^n - 1)$ divise $(a^m - 1) \iff n$ divise m
4. Soit N_k le nombre qui s'écrit en base 10 avec k chiffres tous égaux à 1.
   Montrer que : N_h divise $N_k \iff h$ divise k.

Exercice 32 : Nombres de Mersenne

Ils sont de la forme $M_p = 2^p - 1$ tel que p est premier.

1. Montrer que ces nombres sont premiers entre eux deux à deux.
2. Soit $b \in \mathbb{N}^*$ tel que $2^b - 1$ est premier, montrer que b est premier.

Exercice 33 : Nombres de Fermat

Ils sont de la forme : $F_n = 2^{2^n} + 1$

1. Montrons par récurrence sur $n \geq 1$ que $\prod_{k=0}^{n-1} F_k = F_n - 2$.
2. Montrer alors que tous les F_n sont premiers entre eux deux à deux.
3. Soit $a \in \mathbb{N}^*$, tel que $2^a + 1$ est premier.
   - a. Justifier l'existence de $(n, m) \in \mathbb{N}^2$ tel que $a = 2^n(2m+1)$.
   - b. Montrer que si $m \neq 0$, alors $x^{2m+1} + 1$ n'est jamais premier.
   - c. Conclure alors a est une puissance de 2

Exercice 34 : Théorème de Wilson

1. Soit n premier.
   - a. Montrer que $\forall x \in [|2, n-2|]$, $\exists! y \in [|2, n-2|]$ tel que $x.y \equiv 1 \pmod{n}$.
   - b. en déduire que $(n-2)! \equiv 1 \pmod{n}$, puis que $(n-1)! \equiv -1 \pmod{n}$
2. Inversement, soit $n \in \mathbb{N}^*$ tel que $(n-1)! \equiv -1 \pmod{n}$. On considère $1 \leqslant d < n$ qui divise n. Montrer que $d = 1$. Énoncer le théorème de Wilson.

Exercice 35 : Fonction indicatrice d'Euler (une formule populaire)

Soit $n \geqslant 2$ tel que $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $p_1 < \cdots p_r$ (nombres premiers) et $\alpha_i \in \mathbb{N}^*$.

1. Montrer que $p_i \geqslant 1 + i$ pour tout $1 \leqslant i \leqslant r$.
2. En déduire que $\varphi(n) \geqslant \dfrac{n}{r+1}$. Montrer aussi que $n \geqslant 2^r$.
3. Conclure enfin que $\varphi(n) \geqslant \dfrac{n.\ln 2}{n + \ln 2}$.

Exercice 36 : Fonction indicatrice d'Euler : Formule de Gauss

1. Soit $G = \langle x \rangle$ un groupe cyclique d'ordre n. Si d est un diviseur positif de n, alors il existe un et un seul sous-groupe de G d'ordre d.
2. En déduire que tout sous groupe d'un groupe cyclique est cyclique.
3. Soit $n \geqslant 2$. Montrer que pour tout sous groupe H de $(\mathbb{Z}/n\mathbb{Z}, +)$, il existe $a \in \mathbb{N}$ tel que $H = \langle \overline{a} \rangle$. Que peut on dire alors de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.
4. Soit d un diviseur de n.
   - a. Montrer que $\langle \overline{n/d} \rangle$ est le seul sous groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ de cardinal d.
   - b. En déduire que $\mathbb{Z}/n\mathbb{Z}$ possède exactement $\varphi(d)$ éléments d'ordre d.
5. En déduire la formule classique suivante : $n = \sum_{d|n} \varphi(d)$

Exercice 37 : Classic Concours : Fonction indicatrice d'Euler vs. Probas

Soit $n \in \mathbb{N}^*$ un entier supérieur ou égal à 2. On note $p_1, p_2, \ldots, p_k$ les facteurs premiers distincts de n.
On choisit au hasard et de manière équiprobable un entier $x \in \{1, 2, \ldots, n\}$.
Pour tout $i \in \{1, \ldots, k\}$, on note A_i l'événement : « x est divisible par p_i ».

1. Calculer la probabilité $\mathbb{P}(A_i)$ pour tout $i \in \{1, \ldots, k\}$.
2. Soit $\{i_1, i_2, \ldots, i_m\} \subset \{1, \ldots, k\}$ un sous-ensemble fini d'indices distincts. Montrer que : $\mathbb{P}(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_m}) = \mathbb{P}(A_{i_1}) \times \mathbb{P}(A_{i_2}) \times \cdots \times \mathbb{P}(A_{i_m})$.
   Que peut-on en déduire pour la famille d'événements $(A_i)_{1 \leq i \leq k}$?
3. On note E l'événement : « x est premier avec n ».
   - a. Exprimer E et $\overline{E}$ à l'aide des $A_1, A_2, \ldots, A_k$.
   - b. En utilisant l'indépendance des événements $\overline{A_i}$, retrouver la formule du cours : $\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$

Exercice 38 : Nombres parfaits vs. Nombres d'Euclide

- ☞ Soit $n \in \mathbb{N}^*$, on pose : $\phi(n) = \sum_{d|n} d$
- ☞ On admet que $n \wedge m = 1 \Rightarrow \phi(nm) = \phi(n)\phi(m)$.
- ☞ Soit $n \in \mathbb{N}^*$. On dit que n est **parfait** si et seulement si $\phi(n) = 2n$.
- ☞ On appelle **Nombre d'Euclide** tout entier naturel de la forme $2^{p-1}(2^p - 1)$ tel que p et $2^p - 1$ soient premiers.

1. Soit $E_p = 2^{p-1}(2^p - 1)$ un nombre d'Euclide. Trouver tous les diviseurs de E_p.
2. En déduire que les nombres d'Euclide sont tous parfaits
3. Soit N un nombre parfait pair.
   - a. Montrer que : $\exists m \in \mathbb{N}, \quad \exists q \quad$ *impair* tel que : $N = 2^m q$
   - b. Montrer que $\exists r \in \mathbb{N}^*$ tel que $q = (2^{m+1} - 1)r$ et $\phi(q) = 2^{m+1}r$.
     On pourra utiliser le fait que N est parfait.
   - c. Montrer que $r = 1$.
   - d. Montrer que $p, 2^p - 1$ sont premiser où $p = m + 1$
   - e. Conclure.

- ☞ Remarque : A l'heure actuelle on ne sait pas s'ils existent des nombres parfaits impairs.

Euclide d'Alexandrie (environ 300 av. J.-C.). Père de la géométrie. Mathématicien grec de l'Antiquité, Euclide a exercé à Alexandrie sous le règne de Ptolémée Ier.
Les Éléments constituent son œuvre majeure, structurée en 13 livres, c'est le traité fondateur de la géométrie axiomatique et de l'arithmétique théorique.

Exercice 39 : Cryptographie : Méthode RSA

Soit p et q deux nombres premiers, on pose $n = pq$. Soit M un entier naturel premier avec pq, qui représente le message à décoder, et C le message codé envoyé.

1. Dites pourquoi $\varphi(n) = (p-1)(q-1)$.
2. Soit e premier avec $\varphi(n)$, justifier l'existence de $d \in \mathbb{Z}$ tel que $ed \equiv 1 \pmod{\varphi(n)}$.
3. Le message M est codé en C tel que $C \equiv M^e \pmod{n}$. En déduire que : $C^d \equiv M \pmod{n}$.

   ☞ *Indication* : On pourra penser à utiliser le théorème d'Euler.

Exercice 40 : p-valuation

Soient $n \geq 2$ et p premier.
On pose $v_p(n) = \max\{k \in \mathbb{N} \text{ tel que } p^k \text{ divise } n\}$ (p-**valuation** de n).

1. Montrer que $v_p(n)$.
2. Montrer que pour tout $x \in \mathbb{R}$ et $n \in \mathbb{N}^*$, on a : $E\left(\frac{E(nx)}{n}\right) = E(x)$
3. En déduire que $\forall (i,j) \in \mathbb{N}^2$:

$$p^{i+j} \leq n \implies E\left(\frac{1}{p^j} E\left(\frac{n}{p^i}\right)\right) = E\left(\frac{n}{p^{i+j}}\right)$$

4. On pose $m = E\left(\frac{n}{p}\right)$, montrer que : $v_p(n!) = m + v_p(m!)$.
5. **Applications :**
   - ☞ Calculer $v_7(10000!)$.
   - ☞ Décomposer 16! en produits de facteurs premiers.
   - ☞ Montrer qu'en base 10, 1000! se termine par 249 zéros.

Exercice 41 : Fonction arithmétique multiplicative (un exemple)

- ☞ Une fonction $f : \mathbb{N}^* \longrightarrow \mathbb{N}$ est dite **arithmétique multiplicative** si et seulement si elle vérifie la relation suivante : $f(nm) = f(n)f(m)$, pour tous $(n,m) \in \mathbb{N}^* \times N^*$ tel que $n \wedge m = 1$.
- ☞ Pour tout $n \in \mathbb{N}^*$ on note par $\mathcal{D}_n$ l'ensemble de ses diviseurs dans $\mathbb{N}$
- ☞ Soit $n \in \mathbb{N}^*$, on note par $\phi(n)$ la somme des diviseurs de n dans $\mathbb{N}$: $\phi(n) = \sum_{d|n} d$.

1. Montrer que n est premier si et seulement si $\phi(n) = n + 1$.
2. Soit $(a,b,c) \in \mathbb{N}^{*3}$ tel que $a \wedge b = 1$.
   Montrer que : $a \wedge (bc) = a \wedge c$, $(ab) \wedge c = (a \wedge c)(b \wedge c)$
3. Soit $(m,n) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $n \wedge m = 1$.
   - **a** Montrer que les applications

$$\psi_1 : \begin{array}{ccc} \mathcal{D}_n \times \mathcal{D}_m & \longrightarrow & \mathcal{D}_{nm} \\ (p,q) & \longmapsto & pq \end{array} \quad \text{et} \quad \psi_2 : \begin{array}{ccc} \mathcal{D}_{nm} & \longrightarrow & \mathcal{D}_n \times \mathcal{D}_m \\ d & \longmapsto & (d \wedge n, d \wedge m) \end{array}$$

     sont réciproques l'une de l'autre.
   - **b** En déduire que : $\text{card}(\mathcal{D}_{nm}) = \text{card}(\mathcal{D}_n)\text{card}(\mathcal{D}_m)$.
   - **c** Montrer que tout diviseur d de nm s'écrit sous la forme $d_1 d_2$ où d_1 divise n et d_2 divise m.
   - **d** En déduire que l'application : $f : \begin{array}{ccc} \mathcal{D}_n \times \mathcal{D}_m & \longrightarrow & \mathcal{D}_{nm} \\ (d_1,d_2) & \longmapsto & d_1 d_2 \end{array}$
     est bijective.
   - **e** Conclure enfin que $\phi(nm) = \phi(n)\phi(m)$
4. Soit p premier et $\alpha \in \mathbb{N}$, Donner tous les diviseurs de p^α, puis en déduire $\phi(p^\alpha)$.
5. En déduire $\phi(n)$ où $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, avec p_i des nombres premiers et $\alpha_i \in \mathbb{N}^*$.

Partie F : Arithmétique dans IK[X]

Exercice 42 : Un peu de Calcul

1. Soit $n \in \mathbb{N}^*$. Calculer le reste de la division euclidienne de :
   - a. X^n par $(X-1)(X-2)$ et par $(X-1)^2$.
   - b. $(X\cos(\theta)+\sin(\theta))^n$ par X^2+1, où $\theta \in \mathbb{R}$
2. Pour quelles valeurs de $n \in \mathbb{N}^*$ le polynôme $(X+1)^n - X^n - 1$ est divisible par X^2+X+1 ?
3. Soit $n \in \mathbb{N}^*$. Calculer le quotient de $nX^{n+1} - (n+1)X^n + 1$ par $(X-1)^2$.
4. Décomposer en facteurs irréductibles dans $\mathbb{R}[X]$ puis $\mathbb{C}[X]$ les polynômes : X^6+1, X^8+X^4+1.

Exercice 43 : Critères d'Eisenstein

1. Soient $(p,q) \in \mathbb{Z}\times\mathbb{N}$ tel que $p\wedge q = 1$ et $(a_i)_{0\le i\le n} \in \mathbb{Z}^{n+1}$.
   Montrer que si $\frac{p}{q} \in \mathbb{Q}$ est solution de l'équation : $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 = 0$ alors : p divise a_0 et q divise a_n
2. Résoudre l'équation : $30X^3 - 37X^2 + 15X - 2 = 0$
3. Soit $n \in \mathbb{N}^*$ et $P(x) = \sum_{k=0}^{n} a_kX^k$ à coefficients dans $\mathbb{Z}$ tel qu'il existe p nombre premier vérifiant : p divise a_k pour tout $0 \le k \le n-1$ et p ne divise pas a_n et p^2 ne divise pas a_0.
   Montrer que le polynôme P est irréductible dans $\mathbb{Q}[X]$.
4. *Application* : Montrer que les polynômes suivant sont irréductibles sur $\mathbb{Q}$:
   - ☞ $X^p + p$ où p est premier.
   - ☞ $-3X^{14} + 2X^8 + 8X^3 - 26X^2 + 6$.

Exercice 44 : Contenu d'un polynômes (Classic Mines)

Pour tout $A = \sum_{k\ge 0} a_kX^k$ de $\mathbb{Z}[X]$, on note $c(A)$ le pgcd des coefficients a_k.
On dit que A est un polynôme **primitif** si $c(A) = 1$.
Si $A \neq 0$, on pose $\widehat{A} = \frac{A}{c(A)}$.

1. Justifier que $\widehat{A} \in \mathbb{Z}[X]$ et qu'il est primitif.
2. Montrer que si A et B sont primitifs.
   On suppose $c(AB) \neq 1$, et on considère p un nombre premier qui divise $c(AB)$.
   On pose $A = \sum_{i=0}^{n} a_iX^i$, $B = \sum_{j=0}^{m} b_jX^j$ et $AB = \sum_{k=0}^{n+m} c_kX^k$
   - a. Justifier l'existence de i le plus petit indice tel que $p \nmid a_i$.
   - b. Justifier l'existence de j le plus petit indice tel que $p \nmid b_j$.
   - c. Montrer que p divise a_ib_j, puis en déduire une contradiction.
   - d. Conclure que AB est primitif.
3. Vérifier que $c(mA) = m\,c(A)$ pour tout (m,A) de $\mathbb{N}\times\mathbb{Z}[X]$.
4. Montrer que dans le cas général, on a $c(AB) = c(A)c(B)$.
5. Soient P, Q deux polynômes unitaires dans $\mathbb{Q}[X]$, tel que PQ est dans $\mathbb{Z}[X]$.
   Soient $a, b \in \mathbb{N}^*$ les plus petits entiers non nuls tel que $aP \in \mathbb{Z}[X]$ et $bQ \in \mathbb{Z}[X]$.
   - a. Justifier l'existence de a puis celle de b.
   - b. On pose $d = c(aP)$. Justifier que d divise a et que $\frac{a}{d}P \in \mathbb{Z}[X]$.
   - c. En déduire que $c(aP) = 1$ puis que $c(bQ) = 1$.
   - d. Montrer que $a = b = 1$.
   - e. En déduire que P et Q sont dans $\mathbb{Z}[X]$.

Exercice 45 : Lemme de Gauss

Soient $P, Q \in \mathbb{Q}[X]$ tels que $PQ \in \mathbb{Z}[X]$
Montrer qu'il existe $P_1, Q_1 \in \mathbb{Z}[X]$ proportionnels à P et Q et tels que $PQ = P_1Q_1$.
Autrement dit : Un polynôme à coefficients entiers réductible sur $\mathbb{Q}$ est aussi réductible sur $\mathbb{Z}$.

Exercice 46 : Des classics division euclidienne

1. On se donne deux éléments A, B de $\mathbb{Z}[X]$, le polynôme B étant unitaire.
Soit $A = BQ + R$ la division euclidienne de A par B dans $\mathbb{C}[X]$.
Montrer que le quotient Q et le reste R sont dans $\mathbb{Z}[X]$.

2. Soit $B \in \mathbb{K}[X]$ de degré $n > 0$. On considère les applications :

$$\Phi : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}_{n-1}[X] \\ P & \longmapsto & R \end{array} \quad \text{et} \quad \Psi : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ P & \longmapsto & Q \end{array}$$

avec : $P = QB + R$.

   a. Montrer que Φ et Ψ sont linéaires. Donner leurs noyaux et images.

   b. Simplifier $\Phi(P_1P_2)$, pour tout $(P_1, P_2) \in \mathbb{K}[X]$.

3. Soient $A, B \in \mathbb{K}[X]$, $p = \deg A$ et $q = \deg B$.
On considère l'application : $\Phi : \begin{array}{ccc} \mathbb{K}_{q-1}[X] \times \mathbb{K}_{p-1}[X] & \longrightarrow & \mathbb{K}_{p+q-1}[X] \\ (U, V) & \longmapsto & UA + VB \end{array}$
Démontrer que : $A \wedge B = 1 \iff \Phi$ est bijective.

Partie G : Structure d'algèbre

Exercice 47 : Théorème de Skolem-Noether

Soit $\Phi : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C})$ un morphisme d'algèbres

1. Montrer que Φ est bijectif.

2. Pour $1 \leq i, j \leq n$, soit E_{ij} les matrices élémentaires. Déterminer $\text{rg}(\Phi(E_{11}))$.

3. En déduire que $\exists P \in \text{GL}_n(\mathbb{C}),\ \forall A \in \mathcal{M}_n(\mathbb{C}) : \Phi(A) = PAP^{-1}$. Conclure.

Exercice 48 : Algèbre commutative intègre

1. Montrer que tout anneau fini non nul et intègre est un corps.

2. En déduire que toute algèbre intègre de dimension finie non nulle est un corps.

3. Soit A une $\mathbb{R}$-algèbre intègre de dimension finie $n \geqslant 2$.

   a. Justifier l'existence de $a \in A \setminus \mathbb{R}$.

   b. Montrer que la famille $(1, a)$ est libre tandis que le famille $(1, a, a^2)$ est liée.

   c. En déduire l'existence de $\omega \in A$ tel que $\omega^2 = -1_A$, puis que $\dim A = 2$.

   d. En déduire que A est isomorphe à $\mathbb{C}$ en tant que corps.

Exercice 49 les hyperplans de matrices

Rappel : Soit E un $\mathbb{K}$-ev de dimension finie. On appelle hyperplan de E, tout sev H de E tel que $\dim H = \dim E - 1$. Dans ce cas $\forall a \in E \setminus H$, on a $E = H \otimes \mathbb{K}.a$
Dans la suite on considère $\mathcal{A}$ un hyperplan de $\text{M}_n(\mathbb{C})$ stable pour le produit matriciel.
On suppose de plus que $\text{I}_\text{n} \in \mathcal{A}$.

1. Soit $M \in \text{M}_n(\mathbb{C})$, montrer que si $M^2 \in \mathcal{A}$, alors $M \in \mathcal{A}$.

2. En déduire que $E_{i,j} \in \mathcal{A}$ pour tous $i \neq j$, puis que $E_{i,i} \in \mathcal{A}$ pour tout i

   ☞ **Indication** : on rappelle que $E_{i,j}.E_{k,l} = \delta j, kE_{i,l}$.

3. En déduire une contradiction, puis conclure un résultat.