Révisions 4 : Algèbre générale

I — Le B.A.BA

1) Définitions théorèmes :

Liste non exhaustive des éléments du cours à maîtriser :

- Définition d'un groupe, d'un sous groupe, d'un morphisme de groupes. Image et noyau d'un morphisme.
- Caractérisation d'un morphisme de groupes injectif.
- Intersection de sous groupes. Sous groupe $< X >$ engendré par une partie X.
- Groupe monogène, groupe cyclique. Exemples finis et infinis. Racines de l'unité.
- Classification des groupes monogènes : tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$ et tout groupe monogène fini est isomorphe à un $(\mathbb{Z}/n\mathbb{Z}, +)$
- Permutations. Calcul d'une signature.
- Élement d'ordre fini. Caractérisation de l'ordre d'un élément.
- Théorème de Lagrange (ordre d'un élément, ordre d'un sous groupe)
- Construction de $\mathbb{Z}/n\mathbb{Z}$: compatibilité de la somme et du produit de classes d'équivalence (**Exo 66**) .
- Définition d'un anneau. Anneau intègre. Diviseurs de 0. Identités remarquables pour des éléments qui commutent.
- Arithmétique dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$. Division euclidienne, PGCD, PPCM.
- Relation de Bézout. Théorème de Gauss.
- Polynômes irréductibles de $\mathbb{R}[X]$ puis de $\mathbb{C}[X]$.
- Théorème fondamental de l'analyse de d'Alembert et Gauss.
- L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier (**Exo 66**).
- Morphisme d'anneau. Idéal. Toute intersection d'ideaux est un idéal. Idéal engendré.
- Idéaux de $(\mathbb{Z}, +\times)$ et de $\mathbb{K}[X], +, \times)$.
- Générateurs de $\mathbb{Z}/n\mathbb{Z}$. Indicatrice d'Euler.
- Théorème des restes chinois. Version groupe et version anneau. L'indicatrice d'Euler est "multiplicative".
- Formule d'Euler. Petit théorème de Fermat (**Exo 86**).
- Formule de Taylor exacte pour les polynômes.
- Racines de polynômes. Caractérisation de l'ordre de multiplicité d'une racine de P.

II — Méthodes :

• Pour montrer que G est une groupe, on revient) la définition d'un groupe ou on montrer que G est un sous groupe d'un groupe usuel.
• Pour montrer que H est un sous-groupe de G, on peut utiliser la caractérisation des sous groupes ou montrer que H est le noyau ou l'image d'un morphisme de groupes.
• Pour exploiter que G est un groupe, on envisage au moins deux éléments et on fait leur produit (ou somme), ou bien on envisage un élément et on envisage ses puissances (ou multiples).
• Pour montrer que ϕ est un morphisme de groupes, on montre que $\phi(x \star y) = \phi(x) \triangle \phi(y)$
• Pour montrer que 2 groupes ne sont pas isomorphes, on raisonne par l'absurde en considérant un isomorphisme ϕ et on établie une contradiction.
• Pour montrer que A est un anneau, on vérifie la définition d'un anneau ou bien on montrer que A est un sous anneau d'un anneau usuel.
• Pour exploiter la structure d'anneau, on envisage au moins deux éléments a, b et on manipule $a + b$, ab, $1 - a$ ou $1 + a$.
• Si un anneau vérifie une hypothèse, penser à l'appliquer à $a + b$, $1 - a$ ou $1 + a$.
• Pour montrer que B est un sous anneau de A, on n'oublie pas de montrer que $1_A \in B$
• Pour montrer que ϕ est un morphisme d'anneaux, on n'oublie pas de vérifier que $\phi(1_A) = 1_B$.
• En particulier, le noyau d'un morphisme d'anneaux N'EST PAS une sous anneau, mais c'est un IDEAL.
• Pour exploiter qu'un anneau ou un groupe est fini, on peut considérer les "translations" : $\tau_a : x \mapsto a \cdot x$ ou bien les automorphismes de conjugaison $\phi_a : x \mapsto axa^{-1}$
• Pour résoudre un système de congruences, on utilise le lemme chinois.

III — Interrogations de cours quotidiennes :

Série 1

1. Quels sont les idéaux de $\mathbb{R}[X]$?
2. Citer le théorème d'Euler dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.
3. Citer le théorème de Lagrange pour les groupes.
4. Donner la définition de $\varphi(n)$ pour $n \in \mathbb{N}^*$ (indicatrice d'Euler).
5. Citer le théorème des restes chinois et donner un exemple d'application.
6. Si a, b sont des éléments d'un groupe non forcément commutatif, que vaut $(a \cdot b)^{-1}$?

Série 2

1. Calculer la signature de la permutation
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}.$$
2. Citer quelques exemples de sous groupes de $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$, $(\mathcal{M}_n(\mathbb{K}), +)$, $(GL_n(\mathbb{R}), x)$, $(\mathbb{U}, \cdot)$.
3. Quels sont les sous groupes de $(\mathbb{Z}, +)$? Le démontrer.
4. Donner la définition de $\varphi(n)$ pour $n \in \mathbb{N}^*$ (indicatrice d'Euler).
5. Citer la formule des coefficients du produit de deux polynômes $P = \sum a_k X^k$ et $Q = \sum b_k X^k$.
6. Citer les formules des degrés de la somme, d'un produit de deux polynômes.

Série 3

1. Quels sont les idéaux de $\mathbb{R}[X]$?
2. Donner la définition d'un groupe. On écrira les propriétés à vérifier en langage mathématique.
3. $O^+(\mathbb{R}) = SO_n(\mathbb{R})$ est-il un groupe ? $O^-(\mathbb{R})$ est-il un groupe ?
4. Donner l'exemple d'un groupe de cardinal 6 non commutatif.
5. Quel est le reste de la division euclidienne de P par $(X-a)(X-b)$? de P par $(X-a)$? de P par $(X-a)^2$? Exprimer les résultats en fonction de $P(a)$, $P'(a)$ et $P(b)$.

Série 4

1. Citer le théorème d'Euler dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.
2. Si $a^2 4 = e_G$. Que peut-on dire de l'ordre de a ?
3. Que vaut $\varphi(24)$? Quel est le cardinal de $\mathbb{U}_{24}^*$?
4. Quels sont les sous groupes finis de $(\mathbb{C}^*, \times)$?
5. Montrer que l'ensemble des éléments inversibles d'un anneau A est un groupe pour la loi multiplicative.
6. Factoriser $X^5 - 1$ dans $\mathbb{R}[X]$.

Série 5

1. Donner la définition d'un groupe. On écrira les propriétés à vérifier en langage mathématique.
2. Citer le théorème des restes chinois et donner un exemple d'application.
3. Citer le théorème de Lagrange pour les groupes.
4. Justifier qu'il n'existe qu'un morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.
5. Factoriser $X^8 - 1$.
6. Factoriser $X^{2n} - 2\cos(na)X^n + 1$.

Corrections

Série 1

1. Quels sont les idéaux de $\mathbb{R}[X]$?
Les idéaux de $\mathbb{R}[X]$ sont exactement les idéaux monogènes.
En particulier, si I est un idéal, il existe un polynôme $P_0 \in \mathbb{R}[X]$ tel que $I = (P_0)$.

2. Citer le théorème d'Euler dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.
Soit $n \in \mathbb{N}^*$. Pour $x \in \mathbb{Z}$, si x est premier avec n, alors $x^{\varphi(n)} \equiv 1[n]$.

3. Citer le théorème de Lagrange pour les groupes.
Soit $(G, \cdot)$ un groupe fini dont le neutre est noté e_G. Alors $\forall x \in G, x^{Card(G)} = e_G$

4. Donner la définition de $\varphi(n)$ pour $n \in \mathbb{N}^*$ (indicatrice d'Euler).
$\varphi(n)$ désigne le nombre d'entiers $k \in [1, n-1]$ qui sont premiers avec n.
C'est aussi le nombre de classes inversibles dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.
C'est aussi le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

5. Citer le théorème des restes chinois et donner un exemple d'application.
Si n et p sont premiers entre eux, l'application $\phi : \mathbb{Z}/np\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times Z/p\mathbb{Z}$ définie par $\phi(x \bmod np) = (x \bmod n, x \bmod p)$ est un isomorphisme d'anneaux.
Si $nu + pv = 1$, les solutions du système $\begin{cases} x \equiv a[n] \\ x \equiv b[p] \end{cases}$ sont les $x \equiv x_0[np]$ où $x_0 = nub + pva$.

6. Si a, b sont des éléments d'un groupe non forcément commutatif, que vaut $(a \cdot b)^{-1}$?
L'inverse de $(a \cdot b)$ est égal à $(b^{-1} \cdot a^{-1})$

Série 2

1. Calculer la signature de la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}.$$

$\sigma = (1,3,4) \circ (5,6)$. *Donc $\varepsilon(\sigma) = \varepsilon(1,2,3) \cdot \varepsilon(5,6) = (-1)^2 \cdot (-1)^1 = (-1)$*

2. Citer quelques exemples de sous groupes de $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$, $(\mathcal{M}_n(\mathbb{K}), +)$, $(GL_n(\mathbb{R}), x)$, $(\mathbb{U}, \cdot)$.
pour $(\mathbb{R}, +)$: *on rappelle qu'on peut montrer que les sous groupes de $(\mathbb{R}, +)$ sont soit monogènes (ex : $\mathbb{Z}, n\mathbb{Z}, \sqrt{2}\mathbb{Z}, \pi\mathbb{Z}$... soit denses (ex : $\mathbb{Z} + \sqrt{2}\mathbb{Z}$, $\mathbb{Q}$...).*
Attention toute partie dense de $\mathbb{R}$ n'est pas nécessairement un sous groupe : par exemple, $\mathbb{R} \setminus \mathbb{Q}$ est dense mais n'est pas un sous groupe.
pour $(\mathbb{R}^*, \cdot)$: *par exemple $\{2^n | n \in \mathbb{Z}\}$, plus généralement $\{a^n | n \in \mathbb{Z}\}$ pour $a > 0$.*
pour $(\mathcal{M}_n(\mathbb{K}), +)$: *par exemple l'ensemble des matrices triangulaires supérieures, des matrices diagonales...*
pour $(GL_n(\mathbb{R}), x)$: *par exemple le groupe orthogonal $O_n(\mathbb{R}) = \{M | M^t M = I_n\}$, le groupe spécial linéaire $Sl_n(\mathbb{R}) = \{M | det(M) = 1\}$*
pour $(\mathbb{U}, \cdot)$: *par exemple les $U_n = \{z \in \mathbb{C} | z^n = 1\}$ ou racines de l'unité.*

3. Quels sont les sous groupes de $(\mathbb{Z}, +)$? Le démontrer.
Les sous groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$ pour $n \in \mathbb{N}$.
Soit G un sous groupe de $\mathbb{Z}$. Montrons qu'il existe n tel que $G = n\mathbb{Z}$.
Si $G = \{0\}$, alors $G = 0\mathbb{Z}$.
Sinon il existe $g \in G$ non nul. Comme G est un sous groupe additif, $-g \in G$.
Soit $A = G \cap \mathbb{N}^*$. A n'est pas vide, donc est une partie non vide et minorée de $\mathbb{N}^*$, donc admet un minimum noté n.
Si $p \in G$, d'après le théorème de division euclidienne dans $\mathbb{Z}$, il existe q, r tels que $p = nq + r$. Comme G est un sous groupe et $r = p - nq$, alors $r \in G$. Or $0 \leqslant r < n$. Par statut de n, $r = 0$ et finalement, $p \in n\mathbb{Z}$. Donc $G \subset n\mathbb{Z}$.
Réciproquement, $n\mathbb{Z} \subset G$ car G est un sous groupe.
Donc $G = n\mathbb{Z}$.

4. Donner la définition de $\varphi(n)$ pour $n \in \mathbb{N}^*$ (indicatrice d'Euler).
$\varphi(n)$ désigne le nombre d'entiers $k \in [1, n-1]$ qui sont premiers avec n.
C'est aussi le nombre de classes inversibles dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.
C'est aussi le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

5. Citer la formule des coefficients du produit de deux polynômes $P = \sum a_k X^k$ et $Q = \sum b_k X^k$.
$c_n = \sum_{k=0}^{n} a_k b_{n-k}$: c'est la formule du produit de Cauchy !

6. Citer les formules des degrés de la somme, d'un produit de deux polynômes.
$deg(P+Q) \leqslant \max(deg(P), deg(Q))$ et $deg(PQ) = deg(P) + deg(Q)$.

Série 3

1. Quels sont les idéaux de $\mathbb{R}[X]$?
Les idéaux de $\mathbb{R}[X]$ sont exactement les idéaux monogènes.
En particulier, si I est un idéal, il existe un polynôme $P_0 \in \mathbb{R}[X]$ tel que $I = (P_0)$.

2. Donner la définition d'un groupe. On écrira les propriétés à vérifier en langage mathématique.
Soit G un ensemble non vide. Le couple $(G, \cdot)$ est un groupe ssi :
— *$\forall (x,y) \in G^2, x \cdot y \in G$ (loi interne)*
— *$\forall (x,y,z) \in G^3, (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (loi associative)*
— *$\exists e \in G, \forall x \in G, x \cdot e = e \cdot x = x$ (il existe un neutre)*
— *$\forall x \in G, \exists y \in G, x \cdot y = y \cdot x = e$ (tout élément admet un symétrique)*

3. $O^+(\mathbb{R}) = SO_n(\mathbb{R})$ est-il un groupe ? $O^-(\mathbb{R})$ est-il un groupe ?
La fonction déterminant est un morphisme de groupes de $(O_n(\mathbb{R}), \times)$ dans $(\{-1,1\}, \times)$ car $det(AB) = det(A)det(B)$.
Alors $O^+(\mathbb{R}) = SO_n(\mathbb{R}) = \{M \in O_n(\mathbb{R}) | det(M) = 1\}$ est un sous groupe de $O_n(\mathbb{R})$ car c'est le noyau de ce morphisme.
Par contre, $O^-(\mathbb{R}) = \{M \in O_n(\mathbb{R}) | det(M) = -1\}$ n'est pas un sous groupe car il ne contient pas le neutre multipicatif qui est I_n.

4. Donner l'exemple d'un groupe de cardinal 6 non commutatif.
Le groupe des permutations de $[1,3]$.

5. Quel est le reste de la division euclidienne de P par $(X-a)(X-b)$? de P par $(X-a)$? de P par $(X-a)^2$? Exprimer les résultats en fonction de $P(a)$, $P'(a)$ et $P(b)$.
$P = Q(X-a)(X-b) + R_1$ avec $deg(R_1) \leqslant 1$ donc $R_1 = cX + d$ tel que $P(a) = 0 + R_1(a) = R(a)$ et $P(b) = 0 + R_1(b) = R(b)$.

Donc $ca + d = P(a)$ et $cb + d = P(b)$ et $c = \dfrac{P(a) - P(b)}{a - b}$ et $d = \dfrac{aP(b) - bP(a)}{a - b}$

De la même manière, le reste la division euclidienne de P par $X - a$ est $R_2 = P(a)$ (c'est d'ailleurs une formule du cours !).

Enfin le reste de la division euclidienne de P par $(X-a)^2$ vérifie $R_3 = c'X + d'$ avec $c'a + d' = P(a)$ et $d' = P'(a)$ donc $c' = \dfrac{P(a) - P'(a)}{a}$.

Série 4

1. Citer le théorème d'Euler dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.
Soit $n \in \mathbb{N}^*$. Pour $x \in \mathbb{Z}$, si x est premier avec n, alors $x^{\varphi(n)} \equiv 1[n]$.

2. Si $a^2 4 = e_G$. Que peut-on dire de l'ordre de a ?
D'après la caractérisation de l'ordre d'un élément, l'ordre de a est fini et divise 24 : il est donc égal à 1,2,3,4,6,8,12 ou 24.

3. Que vaut $\varphi(24)$? Quel est le cardinal de $\mathbb{U}_{24}^*$?
$24 = 2^3 * 3^1$. *Or $\varphi(p_1^{n_1} p_2^{n_2} = \varphi(p_1^{n_1}) \cdot \phi(p_2^{n_2}) = p^{n_2 - n_2 - 1}$.*
Ici : $\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$ et $\varphi(3) = 3 - 1 = 2$. Donc $\varphi(24) = \varphi(3)\varphi(8) = 4 \cdot 2 = 8$.
L'ensemble des inversibles de $(\mathbb{U}_{24}, \cdot)$ (on dit aussi racines primitives de l'unité) est en bijection avec les inversibles de $(\mathbb{Z}/24\mathbb{Z}, +)$ et sont au nombre de $\varphi(24) = 8$.

4. Quels sont les sous groupes finis de $(\mathbb{C}^*, \times)$?
Soit G un tel groupe. Soit n son cardinal.
Soit $g \in G$. D'après le théorème de Lagrange, $Card(< g >) = O(g)$ divise n. Donc $g^n = 1$. Donc g est une racine n-ème de l'unité.
Donc $G \subset \mathbb{U}_n$.
Or $\mathbb{U}_n$ est monogène et G est un sous groupe de $\mathbb{U}_n$, donc G est monogène.
Comme G est fini et monogène, G est cyclique de cardinal n, inclus dans $\mathbb{U}_n$, donc $G = \mathbb{U}_n$.
Les sous groupes finis de $(\mathbb{C}^*, \times)$ sont donc exactement les $(\mathbb{U}_n, \cdot)$ pour $n \in \mathbb{N}^*$.

5. Montrer que l'ensemble des éléments inversibles d'un anneau A est un groupe pour la loi multiplicative.
On note A^* l'ensemble des inversibles de A. Il faut vérifier les axiomes d'un groupe (ici, pas de sous groupe !!)
— *A^* n'est pas vide car 1_A est inversible ($1_A \cdot 1_A = 1_A$)*
— *Si $a, b \in (A^*)^2$, il existe a^{-1} et b^{-1} et $(ab) \cdot (b^{-1}a^{-1}) = abb^{-1}a^{-1} = 1_A$ par associativité. Finalement, (ab) est inversible.*

— *Si $a \in A^*$, alors $a^{-1} \in A^*$ également...*
Donc $(A^*, \cdot)$ est un groupe.

6. Factoriser $X^5 - 1$ dans $\mathbb{R}[X]$.
Les racines complexes du polynômes sont les éléments de $\mathbb{U}_5$ donc $X^5 - 1 = \prod_{k=0}^{4}(X - e^{2ik\frac{\pi}{5}}$.
Pour factoriser dans $\mathbb{R}[X]$, on apparie les racines deux à deux conjuguées et on utilise que $(X-a)(X-\overline{a}) = X^2 - 2Re(a)X + |a|^2$.
Faire un dessin si nécessaire.
On trouve $X^5 - 1 = (X-1)(X^2 - 2\cos(\frac{2\pi}{5}) \cdot X + 1)(X^2 - 2\cos(\frac{4\pi}{5}) \cdot X + 1)$

Série 5

1. Donner la définition d'un groupe. On écrira les propriétés à vérifier en langage mathématique.
Soit G un ensemble non vide. Le couple $(G, \cdot)$ est un groupe ssi :
— $\forall (x,y) \in G^2, x \cdot y \in G$ *(loi interne)*
— $\forall (x,y,z) \in G^3, (x \cdot y) \cdot z = x \cdot (y \cdot z)$ *(loi associative)*
— $\exists e \in G, \forall x \in G, x \cdot e = e \cdot x = x$ *(il existe un neutre)*
— $\forall x \in G, \exists y \in G, x \cdot y = y \cdot x = e$ *(tout élément admet un symétrique)*

2. Citer le théorème des restes chinois et donner un exemple d'application.
Si n et p sont premiers entre eux, l'application $\phi : \mathbb{Z}/np\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times Z/p\mathbb{Z}$ définie par $\phi(x \bmod np) = (x \bmod n, x \bmod p)$ est un isomorphisme d'anneaux.
Si $nu + pv = 1$, les solutions du système $\begin{cases} x \equiv a[n] \\ x \equiv b[p] \end{cases}$ *sont les $x \equiv x_0[np]$ où $x_0 = nub + pva$.*

3. Citer le théorème de Lagrange pour les groupes.
Soit $(G, \cdot)$ un groupe fini dont le neutre est noté e_G. Alors $\forall x \in G, x^{Card(G)} = e_G$

4. Justifier qu'il n'existe qu'un morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.
Le morphisme nul convient. Montrons que c'est le seul.
Soit ϕ un tel morphisme. Soit alors $a = \phi(1)$. $a \in \mathbb{Z}$ et $\phi(1/2) + \phi(1/2) = \phi(1/2 + 1/2) = \phi(1) = a$. Donc $\phi(1/2) = a/2 \in \mathbb{Z}$. Plus généralement pour tout entier $n \in \mathbb{N}^*$, $\phi(1/n) = \dfrac{a}{n} \in \mathbb{Z}$...
Or le seul entier $a \in \mathbb{Z}$ tel que pour tout $n \in \mathbb{N}^*$, $\dfrac{a}{n} \in \mathbb{Z}$ est l'entier $a = 0$.
Donc $\phi(1) = 0$. Mais alors $\phi(2) = \phi(1+1) = 0 + 0 = 0$ et même $\forall n \in \mathbb{Z}, \phi(n) = 0$.
Enfin, $q \cdot \phi(\dfrac{p}{q}) = \phi(q \cdot \dfrac{p}{q}) = \phi(p) = 0$ et $\phi(\dfrac{p}{q}) = \dfrac{0}{q} = 0$.
Bilan : $\phi(\mathbb{Q}) = 0$ et ϕ est bien le morphisme nul.

5. Factoriser $X^8 - 1$.
Même méthode, on trouve : $X^8 - 1 = (X-1)(X+1)(X^2 - 2\cos(\frac{\pi}{4}) \cdot X + 1)(X^2+1)(X^2 - 2\cos(\frac{3\pi}{4}) \cdot X + 1)$

6. Factoriser $X^{2n} - 2\cos(na)X^n + 1$.
On ne calcule pas de discriminant !!! On reconnaît la forme $(X-a)(X-\overline{a}) = X^2 - 2Re(a)X + |a|^2$.
Alors $X^{2n} - 2\cos(na)X^n + 1 = (X^n)^2 - 2Re(e^{ina})(X^n) + |e^{ina}|^2 = (X^n - e^{ina})(X - e^{-ina})$
Puis on factorise pas racines n-ème de l'unité des nombres e^{ina} et e^{-ina}
On trouve alors

$$X^{2n} - 2\cos(na)X^n + 1 = \prod k = 0^{n-1}(X - e^{ia}e^{2ik\pi/n}) \prod k = 0^{n-1}(X - e^{-ia}e^{2ik\pi/n})$$

IV — Exercices :

1) Exercices d'échauffement :

(1) : **Exo 94** : système de congruence.

2) Exercices d'approfondissement :

Exercice 1 :

Soit x élément d'un groupe cyclique de cardinal n. Calculer x^n.

Exercice 2 :

Soit

$$M = \begin{pmatrix} 0 & 1 & & (0) \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ (0) & & & 0 \\ 1 & (0) & & \end{pmatrix} \in \mathcal{M}_n(\mathbb{C}).$$

1. *Calculer le polynôme caractéristique de M. La matrice M est-elle diagonalisable ? est-elle inversible ?*

2. *Soit $G = \left\{M^k \mid k \in \mathbb{Z}\right\}$. Montrer que G est une groupe cyclique et préciser son cardinal.*

Exercice 3 :

Soit $n \geqslant 2$.

(1) : *Montrer que les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont engendrés par les classes des diviseurs de n.*

(2) : *Combien le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ admet-il de sous-groupes ?*

Exercice 4 :

Soit $d \in \mathbb{N}$, on note $\mathbb{Z}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} \mid (a,b) \in \mathbb{Z}^2\right\}$.

Montrer que $\mathbb{Z}\left[\sqrt{d}\right]$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

Exercice 5 :

Résoudre les systèmes suivants :

(1) : $\begin{cases} x \equiv 1\ [6] \\ x \equiv 2\ [7] \end{cases}$

Réponse : $x \in 37 + 42\mathbb{Z}$. (2) : $\begin{cases} 3x \equiv 2\ [5] \\ 5x \equiv 1\ [6] \end{cases}$

Réponse : $29 + 30\mathbb{Z}$.

(3) : *Combien y a-t-il d'éléments inversibles dans $\mathbb{Z}/2200\mathbb{Z}$?*

(4) : *Soit $f(x) = \dfrac{1}{\cos x}$. Montrer l'existence d'un polynôme P_n tel que $f^{(n)}(x) = \dfrac{P_n(\sin x}{(\cos x)^{n+1}}$.*

Préciser P_1, P_2 et P_3.

V — Démonstrations classiques :

1. Sous groupes de $(\mathbb{Z}, +)$. Idéaux de $\mathbb{K}[X]$.

2. Dans un groupe fini, l'ordre d'un élément divise l'ordre du groupe. (démonstration dans le cas commutatif)

3. Résolution d'un système de congruence.

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

5. L'union de sous groupes n'est pas forcément un sous groupe. L'intersection est un sous groupe.

6. $(Q, +)$ et $(Q^*, \times)$ ne sont pas isomorphes.

7. Montrer qu'un sous groupe de $(\mathbb{R}, +)$ est soit monogène, soit dense.