Lycée Lakanal, Sceaux
MP – Mathématiques
A. Troesch

2024/2025

Programme des colles de la semaine 9 (25/11 – 29/11)

Chapitre 7 : Structures algébriques

On pourra à l'occasion de ce chapitre redonner (plutôt en fin de colle) des exercices de révision en arithmétique et sur les polynômes. Ces révisions n'ont pas été reprises cette année.

Exercices de la banque CCINP associés au chapitre : 84, 85, 86, 87, 90, 94

1. **Groupes**
   - Rappels
     - Définitions : groupe, groupe abélien, notation multiplicative, additive.
     - Morphismes de groupe, isomorphismes, endomorphismes, automorphismes.
     - Composée de morphisme, réciproque d'isomorphismes.
   - Sous-groupes
     - Sous-groupe, caractérisations
     - Images directes et réciproques de sous-groupes par un morphisme.
     - Noyau d'un morphisme. Caractérisation de l'injectivité.
     - Intersection de sous-groupes
     - Sous-groupe engendré par une partie : définition par minimalité, existence par intersection, description explicite par produit d'éléments de X et de leurs inverses.
     - Partie génératrice d'un groupe.
     - Sous-groupes de $\mathbb{Z}$. *La description des sous-groupes de $\mathbb{R}$ n'est pas au programme.*
   - Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
     - Définition par classes de congruence, définition de l'opération. Structure de groupe.
     - CNS sur $\mathrm{Ker}(\varphi)$ pour que le morphisme $\varphi : \mathbb{Z} \to G$ se factorise par $\mathbb{Z}/n\mathbb{Z}$.
     - Isomorphisme entre $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{U}_n, \times)$
     - Les groupes quotients, et le premier théorème d'isomorphisme, sous-jacents à certaines construction et certains résultats de ce paragraphe ne sont pas au programme !
   - Groupes monogènes
     - Groupe monogène, groupe cyclique, générateur d'un groupe monogène
     - Description explicite par les puissances de x.
     - Tout groupe monogène est isomorphe à $\mathbb{Z}$ ou $\mathbb{Z}/\ \mathbb{Z}$.
   - Ordre d'un élément
     - Ordre d'un élément, lien avec l'ordre du sous-groupe monogène engendré.
     - Caractérisation des k tels que $x^k = e$.
     - Théorème de Lagrange dans un groupe fini : l'ordre de x divise l'ordre de G.

       Démonstration exigible seulement dans le cas abélien.

       Le théorème de Lagrange pour l'ordre des sous-groupes n'est pas au programme. Il a été évoqué et démontré, de sorte à avoir dans le cours une preuve complète du théorème de Lagrange pour l'ordre des éléments, mais cette preuve est hors-programme et non exigible. L'idée importante de partitionnement en classes aH pourra cependant être retenue par les meilleurs élèves.

2. **Anneaux et idéaux**
   - Rappels
     - Définition d'un anneau, d'un corps.
     - Groupe des inversibles
     - Propriété de régularité, diviseurs de 0, lien entre les deux.

    * Anneaux intègre (par définition un anneau intègre sera supposé commutatif)
    * Rappels calculatoires : formule du binôme, factorisation de $a^n - b^n$, avec l'hypothèse idoine.
    * Homomorphismes d'anneaux
    * Sous-anneaux, caractérisation
    * Anneau produit, groupe des inversibles de $A \times B$.
  - Idéaux
    * Définition d'un idéal d'un anneau commutatif. *Le cas des idéaux à gauche, droite, bilatère d'un anneau non commutatif n'est pas au programme*
    * Le noyau d'un morphisme d'anneau est un idéal.
    * xA est un idéal. Minimalité parmi les idéaux contenant x. Notion d'idéal principal.
    * Anneau principal (par définition un anneau principal est supposé intègre, donc aussi commutatif).
    * Divisibilité dans un anneau intègre. Caractérisation par les idéaux principaux.
    * Somme d'un nombre fini d'idéaux (démonstration faite pour 2)
  - Idéaux de $\mathbb{Z}$ et arithmétique
    * Décription des idéaux de $\mathbb{Z}$. $\mathbb{Z}$ est principal.
    * Définition par les idéaux du pgcd de n entiers non tous nuls. Interprétation en terme de divisibilité. Rapport avec Bézout
    * (HP) Définition d'un pgcd et d'un ppcm dans un anneau principal.

3. **L'anneau** $(\mathbb{Z}/n\mathbb{Z}, +, \times)$
  - Propriétés d'inversibilité
    * Structure d'anneau. Description des éléments inversibles. Trouver un inverse à l'aide d'une relation de Bézout.
    * CNS pour que $\mathbb{Z}/n\mathbb{Z}$ soit un corps. Notation $\mathbb{F}_p$.
  - Théorème des restes chinois
    * Théorème choinois : isomophisme entre $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, sous les bonnes conditions.
    * Application à la résolution de systèmes de congruences dont les modules de congruence sont 2 à 2 premiers entre eux.
    * Cas de systèmes avec des modules de congruence non premiers entre eux (uniquement vu au travers d'exemples).
  - Indicatrice d'Euler φ
    * Définition
    * Théorème d'Euler, lien avec le théorème de Fermat.
    * Multiplicativité arithémtique de φ, calcul de $\varphi(p^k)$, puis de $\varphi(n)$ en fonction de la décomposition en produit de facteurs premiers.

4. **Arithmétique dans l'anneau** $\mathbb{K}[X]$

   Selon le programme officiel, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

   Il a été signalé aux élèves que toutes les notions ci-dessous se généralisent à un corps quelconque, mais qu'en revanche, il fallait faire attention dès qu'il intervient des racines et des multiplicité, des dérivations et des primitivations.

   La notion de caractéristique d'un corps n'est pas au programme.
  - Idéaux de $\mathbb{K}[X]$.
    * $\mathbb{K}[X]$ est principal
    * Divisibilité dans $\mathbb{K}[X]$, caractérisation en terme d'idéaux.
    * Définition du PGCD par les idéaux, caractérisation par la divisibilité.
  - Décomposition en facteurs irréductibles
    * Polynôme irréductible. Description des polynômes irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$.

      Le théorème de d'Alembert-Gauss est admis.
    * Existence d'un diviseur irréductible ($\mathbb{K}$ sous-corps de $\mathbb{C}$)
    * Lemme de Gauss, lemme d'Euclide
    * Existence et unicité (à permutation près) d'une décomposition en produit de polynômes irréductibles unitaires.

Chapitre 8 : Compléments d'algèbre linéaire

Les notions d'algèbre linéaire vues en Sup (voir liste ci-dessous) ne sont pas reprises, mais elles pourront faire l'objet d'un petit exercice de révision.

Thèmes de sup à revoir :

- Définitions générales d'algèbre linéaire, bases, dimension finie
- Applications linéaires, détermination sur une base, théorème du rang. Projecteurs et symétries.
- Représentation matricielle dans une base. Formule de changement de base. Matrices équivalentes, matrices semblables
- Déterminants

Exercices de la banque CCINP associés au chapitre : 60, 62, 64, 71, 93

(Pas encore les exercices 62 et 93 cette semaine)

ENCORE PEU D'EXERCICES traités en cours sur les notions qui suivent.

1. **Sommes directes et blocs**
   - Sommes directes.

     Il s'agit de généraliser la notion de somme directe de deux sev vue en Sup, au cas d'un nombre fini quelconques de sev.
     * Somme d'un nombre fini de sous-espaces vectoriels de E
     * Somme directe d'un nombre fini de sev, définie par propriétés équivalentes (unicité de la décomposition d'un x, ou de 0, intersections nulles)
     * Majoration de la dimension d'une somme quelconque, avec égalité ssi la somme est directe.
     * Concaténations de base, base adaptée à une décomposition de E en somme directe (donné dans le cours en dimension finie uniquement, pour alléger les indexations).
     * Projecteurs associés à une somme directe. Description de leurs composées.
   - Détermination d'une application linéaire $u \in \mathcal{L}(E, F)$
     * Détermination d'un AL par ses restrictions aux facteurs d'une décomposition en somme directe de E.
     * Interprétation matricielle dans une base adaptée.
     * Composantes d'une AL sur les facteurs d'une décomposition en somme directe de F. Description matricielle dans une base adaptée
     * Expression de $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(u)$ en fonction des restrictions aux E_i des composantes sur les F_i, dans le cas où on dispose de décompositions en sommes directes de E et de F ($\mathcal{B}$ et $\mathcal{C}$ sont des bases adaptées).
     * Cas d'un endomorphisme laissant stable les facteurs d'une décomposition en $\oplus$ de E.
   - Calcul matriciel par blocs
     * Décomposition en blocs d'une matrice. Matrice diagonale par blocs, triangulaire par blocs (pour ces deux cas, les blocs diagonaux seront systématiquement carrés, donc les regroupements des lignes et des colonnes sont les mêmes).
     * Découpages par blocs de A et B compatibles pour le produit (mêmes regroupements sur les colonnes de A que sur les lignes de B)
     * Règle de produit matriciel par blocs.

       Démonstration faite en cours, mais non exigible, conformément au programme officiel.
     * Produits et puissances de matrices triangulaires par blocs, diagonales par blocs
   - Déterminants par blocs
     * Transvection par blocs $L_i \leftarrow L_i + TL_k$, $T \in \mathcal{M}_{m_i,m_k}(\mathbb{K})$ (les m_i étant les tailles des regroupements par lignes, les L_i représentant chacun des blocs de lignes).
     * Expression matricielle, et invariance du déterminant par transvection par blocs)
     * On pourra admettre une règle similaire pour les transvections par colonnes.
     * Déterminant d'une matrice triangulaire par blocs.

Liste des questions de cours à préparer.

Sauf mention explicite du contraire, les démonstrations des différents résultats cités sont aussi demandées

1. Définition, existence, et descriptions (par intersection ou par les éléments) du sous-groupe engendré par une partie
2. Description des sous-groupes de $\mathbb{Z}$. Conséquence sur la structure des groupes monogènes.
3. Définition de l'ordre d'un élément. Théorème de Lagrange (énoncé général, démonstration dans le cas où G est abélien, conformément au programme)
4. Définition d'un idéal d'un anneau. Idéal principal (définition et vérification du fait que c'est un idéal). Cas de $\mathbb{Z}$. Définition du PGCD à l'aide des idéaux.
5. Indicatrice d'Euler. Théorème d'Euler. Multiplicativité arithmétique.
6. Description des idéaux de $\mathbb{K}[X]$. Définition du PGCD d'une famille finie de polynômes.
7. Définition d'un polynôme irréductible, description des polynômes irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$ (le théorème de d'Alembert-Gauss est admis)
8. Existence et unicité de la décomposition en facteurs irréductibles unitaires dans $\mathbb{K}[X]$. Pour raccourcir un peu, le colleur pourra éventuellement demander uniquement la preuve de l'existence (incluant le lemme sur l'existence d'un diviseur irréductible), ou la preuve de l'unicité (sans inclure la démonstration des lemmes de Gauss et d'Euclide).
9. Cinq propriétés équivalentes définissant la somme directe d'un nombre fini de sev.
10. Détermination d'une AL $u \in \mathcal{L}(E, F)$ par ses restrictions aux facteurs d'une décomposition en somme directe de E.

Énoncé des exercices de la banque CCINP à préparer

Exercice – (Banque CCINP n° 60)

Soit la matrice $A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ et f l'endomorphisme de $\mathcal{M}_2(\mathbb{R})$ défini par : $f(M) = AM$.

1. Déterminer une base de $\mathrm{Ker} f$.
2. f est-il surjectif ?
3. Déterminer une base de $\mathrm{Im} f$.
4. A-t-on $\mathcal{M}_2(\mathbb{R}) = \mathrm{Ker} f \oplus \mathrm{Im} f$?

Exercice – (Banque CCINP n° 64)

Soit f un endomorphisme d'un espace vectoriel E de dimension finie n.

1. Démontrer que : $E = \mathrm{Im} f \oplus \mathrm{Ker} f \Longrightarrow \mathrm{Im} f = \mathrm{Im} f^2$.
2. (a) Démontrer que : $\mathrm{Im} f = \mathrm{Im} f^2 \Longleftrightarrow \mathrm{Ker} f = \mathrm{Ker} f^2$.
   (b) Démontrer que : $\mathrm{Im} f = \mathrm{Im} f^2 \Longrightarrow E = \mathrm{Im} f \oplus \mathrm{Ker} f$.

Exercice – (Banque CCINP n° 71)

Soit P le plan d'équation $x + y + z = 0$ et D la droite d'équation $x = \dfrac{y}{2} = \dfrac{z}{3}$.

1. Vérifier que $\mathbb{R}^3 = P \oplus D$.
2. Soit p la projection vectorielle de $\mathbb{R}^3$ sur P parallèlement à D.
   Soit $u = (x, y, z) \in \mathbb{R}^3$.
   Déterminer $p(u)$ et donner la matrice de p dans la base canonique de $\mathbb{R}^3$.
3. Déterminer une base de $\mathbb{R}^3$ dans laquelle la matrice de p est diagonale.

Exercice – (Banque CCINP n° 84)

1. Donner la définition d'un argument d'un nombre complexe non nul (on ne demande ni l'interprétation géométrique, ni la démonstration de l'existence d'un tel nombre).
2. Soit $n \in \mathbb{N}^*$. Donner, en justifiant, les solutions dans $\mathbb{C}$ de l'équation $z^n = 1$ et préciser leur nombre.
3. En déduire, pour $n \in \mathbb{N}^*$, les solutions dans $\mathbb{C}$ de l'équation $(z+\mathrm{i})^n = (z-\mathrm{i})^n$ et démontrer que ce sont des nombres réels.

Exercice – (Banque CCINP n° 86)

1. Soit $(a,b,p) \in \mathbb{Z}^3$. Prouver que : si $p \wedge a = 1$ et $p \wedge b = 1$, alors $p \wedge (ab) = 1$.
2. Soit p un nombre premier.
   (a) Prouver que $\forall k \in [\![1, p-1]\!]$, p divise $\binom{p}{k} k!$ puis en déduire que p divise $\binom{p}{k}$.
   (b) Prouver que : $\forall n \in \mathbb{N},\ n^p \equiv n \mod p$.
   Indication : procéder par récurrence.
   (c) En déduire, pour tout entier naturel n, que : p ne divise pas $n \Longrightarrow n^{p-1} \equiv 1 \mod p$.

Exercice – (Banque CCINP n° 89)
Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. On pose $z = e^{\mathrm{i}\frac{2\pi}{n}}$.

1. On suppose $k \in [\![1, n-1]\!]$.
   Déterminer le module et un argument du complexe $z^k - 1$.
2. On pose $S = \displaystyle\sum_{k=0}^{n-1} \left|z^k - 1\right|$. Montrer que $S = \dfrac{2}{\tan \frac{\pi}{2n}}$.

Exercice – (Banque CCINP n° 94)

1. Énoncer le théorème de Bézout dans $\mathbb{Z}$.
2. Soit a et b deux entiers naturels premiers entre eux.
   Soit $c \in \mathbb{N}$.
   Prouver que : $(a|c \text{ et } b|c) \Longleftrightarrow ab|c$.
3. On considère le système (S) : $\left\{\begin{array}{lcll} x & \equiv & 6 & [17] \\ x & \equiv & 4 & [15] \end{array}\right.$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.
   (a) Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.
   (b) *Déduire des questions précédentes* la résolution dans $\mathbb{Z}$ du système (S).

Prévisions pour la semaine suivante :

- Reprise du chapitre d'algèbre linéaire + algèbres, polynômes de matrices et d'endormophismes.
- Début de la réduction des endomorphismes.