Rectorat de Grenoble / Université Grenoble Alpes

Préparation à l'agrégation interne 2023-2024

Anneaux, corps, espaces vectoriels et nombres algébriques.

Parties du programme abordées : parties 3.1 (extensions de la notion de nombre), 3.2 (anneaux et corps) et 3.3 (Polynômes à une indéterminée sur un corps commutatif K).

Idéaux d'un anneau commutatif. Anneaux quotients. Anneaux commutatifs intègres. Morphismes d'anneaux. Isomorphisme entre $\mathrm{Im}(f)$ et $A/\ker(f)$ pour f morphisme d'anneaux de A dans A'. Anneaux principaux.

Polynômes à une indéterminée sur un corps commutatif K. Algèbre $K[X]$. Idéaux de $K[X]$. Plus grand commun diviseur (PGCD) et plus petit commun multiple (PPCM). Théorème de Bézout. Polynômes irréductibles. Décomposition en produit de facteurs irréductibles.

Sous-corps. Corps premier. Caractéristique d'un corps. Corps des fractions d'un anneau intègre. Éléments algébriques, transcendants sur un sous-corps. Dénombrabilité du corps des nombres algébriques sur $\mathbb{Q}$.

Dans cette feuille :

— L'exercice 1 permet de maitriser les structures algébriques.

— L'exercice 2 est une sorte de "rappel de cours", il fait partie du programme, c'est la base de la notion d'extension de corps et de nombres algébriques.

— Les exercices 3 et 4 permettent de maitriser la structure d'espace vectoriel et d'algèbre d'une extension de corps (algébrique).

— L'exercice 5 est le début d'un sujet de concours (qui a d'ailleurs motivé le thème de cette séance).

— L'exercice 6 avait été traité à la prépa il y a quelques années, il y a un lien intéressant entre la question 6 de cet exercice et le début de la feuille.

À connaître pour cette feuille d'exercice :

— les définitions des structures algébriques groupe, anneau, corps, espace vectoriel, algèbre, leurs morphismes et leurs quotients.

— la notion d'élément irréductible (au moins dans un anneau de polynômes sur un corps).

Dans toute cette feuille, les anneaux sont commutatifs et intègres.

Exercice 1 : Travail préliminaire sur les structures algébriques.

1. Rappeler la définition d'un morphisme $\phi : A \to B$, les propriétés (structure algébrique) du noyau et le premier théorème d'isomorphisme dans les cas où A et B sont :
   (a) des groupes.
   (b) des anneaux.
   (c) des espaces vectoriels sur un corps $\mathbb{K}$.
   (d) des algèbes sur un corps $\mathbb{K}$.
2. Soient $A \subset B$ deux anneaux commutatifs. Soit $\omega \in B$. Décrire les éléments des ensembles suivants :
   (a) Le sous-groupe additif de B engendré par ω.
   (b) L'idéal de B engendré par ω.
   (c) Le sous-anneau de B engendré par ω.
   (d) Le sous-anneau de B engendré par A et ω.
   (e) Dans le cas où A est un corps, le sous-A-espace vectoriel de B engendré par ω, et dans le cas général, le sous-A-module [1] de B engendré par ω.
   (f) La sous-A-algèbre [2] de B engendré par ω.

   Décrire ces ensembles pour $A = \mathbb{Z}$, $B = \mathbb{Q}$, $\omega = \frac{1}{2}$.
3. Soit K un corps et $P \in K[X]$.
   (a) (Structure d'anneau du quotient $K[X]/(P)$) Montrer que $K[X]/(P)$ est un corps si et seulement si P est un polynôme irréductible de $K[X]$ (indication : dans un sens, utiliser un diviseur de zéro, dans l'autre sens, utiliser une identité de Bezout).
   (b) (Structure d'espace vectoriel du quotient $K[X]/(P)$) Montrer que $K[X]/(P) = \{\overline{R},\ R \in K[X], \deg(R) < \deg(P)\}$. En déduire la dimension du K-espace vectoriel $K[X]/(P)$.

Exercice 2 : Extension de corps

Soit K un corps et A un anneau commutatif intègre contenant K comme sous-anneau :

$$K \subset A.$$

Lorsque A est lui-même un corps, on dit que A est une extension de K.

1. Montrer que A possède naturellement une structure de K-algèbre.

On note $[A : K] = \dim_K A$ la dimension du K-espace vectoriel A. Lorsque A est un corps, on appelle $[A : K]$ le *degré* de l'extension $K \subset A$, et on dit que l'extension $K \subset A$ est finie si c'est un nombre fini.

1. la notion de module sur un anneau est élémentaire mais n'est pas au programme de l'agrégation.
2. On peut supposer que A est un corps si on veut éviter la notion de A-module.

2. Calculer les degrés des extensions suivantes :
   (a) $\mathbb{R} \subset \mathbb{C}$,
   (b) $\mathbb{R} \subset \mathbb{R}(X)$ où $\mathbb{R}(X)$ désigne le corps des fractions rationnelles à coefficients dans $\mathbb{R}$,
   (c) $\mathbb{Q} \subset \mathbb{R}$ (indication : penser au cardinal),
   (d) $\mathbb{F}_2 \subset \mathbb{F}_8$ où $\mathbb{F}_q$ désigne le corps à q éléments.

   Soit $\alpha \in A$. On rappelle que l'application suivante :

$$\begin{array}{rccc} \Phi_\alpha & : & K[X] & \to & A \\ & & P & \mapsto & P(\alpha) \end{array}$$

   est un morphisme de K-algèbre. On l'appelle morphisme d'évaluation en α.

   On note $K[\alpha]$ l'image de Φ_α. On dit que α est *transcendant* sur K si le morphisme Φ_α est injectif, sinon on dit que α est *algébrique* sur K. Dans ce cas, on appelle *polynôme annulateur* de α tout polynôme de $\ker \Phi_\alpha$ et *polynôme minimal* de α le générateur unitaire de l'idéal $\ker \Phi_\alpha$ de $K[X]$. On le notera π_α.

3. Si α est algébrique sur K, montrer que π_α est un polynôme irréductible de $K[X]$. En déduire qu'un polynôme de $K[X]$ est soit un multiple de π_α, soit premier avec π_α.
4. Montrer réciproquement que si α est algébrique sur K et si P est un polynome annulateur de α unitaire et irréductible, alors $P = \pi_\alpha$.
5. Montrer que $K[\alpha]$ est isomorphe à un quotient de l'anneau $K[X]$.
6. *(Caractérisation d'un élément algébrique α par la structure algébrique de $K[\alpha]$)* Montrer que α est algébrique sur K si et seulement si $K[\alpha]$ est un corps. Indication : utiliser la question 3 et l'identité de Bezout.
7. **Extensions du corps $\mathbb{Q}$.**
   (a) Montrer qu'un corps $\mathbb{K}$ contenant $\mathbb{Q}$ comme sous-corps ne possède qu'un nombre dénombrable d'éléments algébriques sur $\mathbb{Q}$. En déduire qu'il y a une infinité de nombres réels transcendants sur $\mathbb{Q}$.
   (b) Déterminer les polynômes minimaux de $\sqrt{2}$ et de $i\sqrt{2}$ sur $\mathbb{Q}$, écrire les anneaux suivants comme quotients de $\mathbb{Q}[X]$ et en déterminer la dimension et une base en tant que $\mathbb{Q}$-espaces vectoriels :
   (i) $\mathbb{Q}[\sqrt{2}]$. (ii) $\mathbb{Q}[i\sqrt{2}]$. (iii) $\mathbb{Q}[\alpha]$ pour $\alpha \in \mathbb{C}$ transcendant sur $\mathbb{Q}$.
8. Soit $\alpha \in A$ un élément algébrique sur K. Montrer que $\deg(\pi_\alpha) = [K[\alpha] : K]$ et donner une base de $K[\alpha]$.
9. *(Caractérisation d'un élément algébrique α par la dimension de $K[\alpha]$)* Montrer que $\alpha \in A$ est algébrique sur K si et seulement si $K[\alpha]$ est de dimension finie sur K.
10. **L'extension $\mathbb{R} \subset \mathbb{C}$.** Montrer que $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{R}[X]/(X^2+X+1)$ en tant que $\mathbb{R}$-algèbres. Indication : chercher des morphismes d'évaluation dans $\mathbb{C}$.

Exercice 3 : Extensions algébriques et applications linéaires.

On reprend les notations et les résultats de l'exercice 2.

1. Montrer que $\mathbb{Q}[\sqrt[3]{2}]$ est un corps et un $\mathbb{Q}$-espace vectoriel de dimension finie. Donner le polynôme minimal de $\sqrt[3]{2}$ et une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\sqrt[3]{2}]$.
2. Montrer que l'application :

$$\begin{array}{rccc} P_{\sqrt[3]{2}} & : & \mathbb{Q}[\sqrt[3]{2}] & \to & \mathbb{Q}[\sqrt[3]{2}] \\ & & x & \mapsto & \sqrt[3]{2}\,x \end{array}$$

   est bien définie et qu'elle est $\mathbb{Q}$-linéaire.
3. Calculer la trace et le déterminant de $P_{\sqrt[3]{2}}$.
4. Déterminer les valeurs propres et le polynôme minimal de $P_{\sqrt[3]{2}}$. Cet endomorphisme est-il diagonalisable ?

Exercice 4 : Des mini-groupes de Galois.

On reprend les notations et résultats de l'exercice 2. Dans cet exercice, on utilise des morphismes de corps et d'algèbre pour permuter des racines de polynômes.

1. Montrer que si $P \in \mathbb{R}[X]$ possède une racine complexe $\alpha \in \mathbb{C}$, alors son conjugué $\overline{\alpha}$ est aussi racine de P.

Soit d un entier naturel non nul sans facteur carré, c'est-à-dire dont la décomposition en facteurs premiers ne contient qu'une seul fois chaque facteur premier.

2. Montrer que $\mathbb{Q}[\sqrt{d}]$ est un $\mathbb{Q}$-espace vectoriel de base $(1, \sqrt{d})$.
3. Soit $P \in \mathbb{Q}[X]$. Montrer, de deux façons différentes, que si $\sqrt{d}$ est racine de P, alors $-\sqrt{d}$ est également racine de P :
   (a) en développant $P(\sqrt{d})$ à l'aide des coefficients de P.
   (b) en utilisant le polynôme minimal de $\sqrt{d}$ (sur $\mathbb{Q}$).

   Nous allons généraliser ce résultat en utilisant un morphisme de conjugaison.
4. Montrer que l'application suivante :

$$\begin{array}{rccc} \sigma & : & \mathbb{Q}[\sqrt{d}] & \to & \mathbb{Q}[\sqrt{d}] \\ & & a + b\sqrt{d} & \mapsto & a - b\sqrt{d} \end{array}$$

   est bien définie et est un morphisme de corps de $\mathbb{Q}[\sqrt{d}]$ dans lui-même laissant $\mathbb{Q}$ invariant (c'est donc un morphisme de $\mathbb{Q}$-algèbre).
5. En déduire que si $a + b\sqrt{d}$, avec $a, b \in \mathbb{Q}$, est racine d'un polynôme P de $\mathbb{Q}[X]$, alors $a - b\sqrt{d}$ est également racine de P (indication : appliquer le morphisme σ à $P(a + b\sqrt{d})$, comme cela a été fait à la question 1).
6. (a) Montrer que $\mathbb{Q}$ est exactement l'ensemble des éléments de $\mathbb{Q}[\sqrt{d}]$ invariant par σ.

(b) Application : montrer que $1+\sqrt{3}$ est algébrique sur $\mathbb{Q}$ (indication : plonger le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[1+\sqrt{3}]$ dans une extension finie de $\mathbb{Q}$) et donner son polynôme minimal.

7. (a) Montrer que les extensions $\mathbb{Q}[\sqrt[3]{2}]$, $\mathbb{Q}[j\sqrt[3]{2}]$ et $\mathbb{Q}[j^2\sqrt[3]{2}]$ de $\mathbb{Q}$ dont finies et donner une base de ces $\mathbb{Q}$-espaces vectoriels.

   (b) Montrer qu'il existe un unique morphisme de corps σ de $\mathbb{Q}[\sqrt[3]{2}]$ dans $\mathbb{Q}[j\sqrt[3]{2}]$ qui laisse $\mathbb{Q}$ invariant et qui envoie $\sqrt[3]{2}$ sur $j\sqrt[3]{2}$, et un unique morphisme de corps σ' de $\mathbb{Q}[\sqrt[3]{2}]$ dans $\mathbb{Q}[j^2\sqrt[3]{2}]$ qui laisse $\mathbb{Q}$ invariant et qui envoie $\sqrt[3]{2}$ sur $j^2\sqrt[3]{2}$.

   (c) En déduire que si $1+\sqrt[3]{2}-\sqrt[3]{4}$ est racine d'un polynôme P de $\mathbb{Q}[X]$, alors $1+j\sqrt[3]{2}-j^2\sqrt[3]{4}$ et $1+j^2\sqrt[3]{2}-j\sqrt[3]{4}$ sont également racines de P.

   (d) Montrer que $1+\sqrt[3]{2}-\sqrt[3]{4}$ est algébrique sur $\mathbb{Q}$ et donner son polynôme minimal.

Remarque : dans la question 7, il serait plus "propre" de travailler sur le corps $\mathbb{Q}[\sqrt[3]{2}, j\sqrt[3]{2}] = \mathbb{Q}[\sqrt[3]{2}, j]$ qui contient toutes les racines du polynôme X^3-2, et de travailler sur le groupe, appelé groupe de Galois de l'extension $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}, j]$, des automorphismes de $\mathbb{Q}$-algèbre de ce corps. L'extension $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}, j]$ est de degré 6 (une base est formée par les nombres $j^k\sqrt[3]{2}^l$ avec $0 \leq k \leq 1, 0 \leq l \leq 2$) et son groupe de Galois est aussi de cardinal 6, isomorphe à S_3. On a utilisé le sous-groupe $\{\mathrm{id}, \sigma, \sigma^2 = \sigma'\}$ de cardinal 3 de ce groupe.

Exercice 5 : Valeurs propres de matrices symétriques à coefficients rationnels (d'après X-ENS 2020)

On note $\mathrm{M}_n(\mathbb{Q})$ l'ensemble des matrices $n \times n$ à coefficients dans $\mathbb{Q}$ et $\mathrm{Sym}_n(\mathbb{Q})$ l'ensemble des matrices symétriques de $\mathrm{M}_n(\mathbb{Q})$.

1. Donner une matrice $A \in \mathrm{Sym}_2(\mathbb{Q})$ dont $\sqrt{2}$ est valeur propre.
2. Donner une matrice $B \in \mathrm{M}_2(\mathbb{Q})$ dont $\sqrt{3}$ est valeur propre.
3. Le but de cette question est de montrer que $\sqrt{3}$ n'est pas valeur propre d'une matrice de $\mathrm{Sym}_2(\mathbb{Q})$. On suppose qu'il existe $M \in \mathrm{Sym}_2(\mathbb{Q})$ telle que $\sqrt{3}$ est valeur propre de M.
   (a) Montrer que le polynôme caractéristique de M est X^2-3 (indication : c'est une question de l'exercice précédent).
   (b) En étudiant les carrés dans $\mathbb{Z}/3\mathbb{Z}$, montrer qu'il n'existe pas de triplet d'entiers (x, y, z) premiers entre eux dans leur ensemble tel que $x^2+y^2 = 3z^2$.
   (c) Conclure.
4. Le but de cette question est de montrer que $\sqrt{3}$ est valeur propre d'une matrice symétrique à coefficients dans $\mathbb{Q}$. Soit $M \in \mathrm{Sym}_2(\mathbb{Q})$ telle que $\sqrt{2}$ est valeur propre de M.
   (a) Montrer que $M^2 = 2I_2$.
   (b) On note $N = \begin{pmatrix} M & I_2 \\ I_2 & -M \end{pmatrix}$, matrice par blocs de $M_4(\mathbb{Q})$. Déterminer N^2.
   (c) En déduire une matrice symétrique à coefficients rationnels ayant $\sqrt{3}$ comme valeur propre.

5. Le but de cette question est de montrer que $\sqrt[3]{2}$ n'est pas valeur propre d'une matrice symétrique à coefficients dans $\mathbb{Q}$. On raisonne par l'absurde, supposant l'existence d'une matrice $M \in \mathrm{Sym}_n(\mathbb{Q})$ (pour un certain n) dont $\sqrt[3]{2}$ est valeur propre.
   (a) Montrer que $X^3 - 2$ divise le polynôme caractéristique de M. Indication : chercher le polynôme minimal du nombre $\sqrt[3]{2}$ algébrique sur $\mathbb{Q}$ (voir exercices précédents).
   (b) Conclure (indication : utiliser le théorème spectral).

Exercice 6 : Résultant de deux polynômes et applications (d'après CCP2009)

I. Définition et propriétés

Soient p et q deux entiers naturels non nuls,

$$P = \sum_{k=0}^{p} a_k X^k \text{ et } Q = \sum_{k=0}^{q} b_k X^k$$

deux polynômes de $\mathbb{C}[X]$ avec $a_p \neq 0$ et $b_q \neq 0$.
Le résultant des polynômes P et Q est le nombre complexe noté $\mathrm{Res}(P, Q)$:

$$\mathrm{Res}(P,Q) = \begin{vmatrix} a_0 & & & & b_0 & & \\ a_1 & \ddots & & & b_1 & \ddots & \\ \vdots & & a_0 & & \vdots & & b_0 \\ a_p & & a_1 & a_0 & \vdots & & b_1 \\ & \ddots & \vdots & a_1 & b_q & & \vdots \\ & & a_p & \vdots & & \ddots & \vdots \\ & & & a_p & & & b_q \end{vmatrix}.$$

C'est un déterminant $q+p$ colonnes, dont les q premières colonnes représentent les coefficients du polynôme P et les p suivantes représentent les coefficients du polynôme Q ; les positions non remplies étant des zéros. Par exemple, si $P = 1 + 2X + 3X^2$ et $Q = 4 + 5X + 6X^2 + 7X^3$,

$$\mathrm{Res}(P,Q) = \begin{vmatrix} 1 & 0 & 0 & 4 & 0 \\ 2 & 1 & 0 & 5 & 4 \\ 3 & 2 & 1 & 6 & 5 \\ 0 & 3 & 2 & 7 & 6 \\ 0 & 0 & 3 & 0 & 7 \end{vmatrix}.$$

La matrice servant à définir $\mathrm{Res}(P, Q)$ pourra être notée $M_{P,Q}$:

$$\mathrm{Res}(P,Q) = \det M_{P,Q}.$$

On note $E = \mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X]$ et $F = \mathbb{C}_{p+q-1}[X]$ où $\mathbb{C}_k[X]$ désigne l'ensemble des polynômes à coefficients complexes de degré $\leq k$.

Soit u l'application de E dans F définie pour $(A, B) \in E$ par : $u(A, B) = PA + QB$.

1. **Cas où u est bijective**

   Pour quelle structure algébrique u est-elle un morphisme ? En déduire que u est bijective si et seulement si P et Q sont premiers entre eux.

2. **Matrice de u**

   On note $\mathcal{B} = ((1,0),(X,0),\ldots,(X^{q-1},0),(0,1),(0,X),\ldots,(0,X^{p-1}))$ une base de E et $\mathcal{B}' = (1,X,\cdots,X^{p+q-1})$ la base canonique de F.

   (a) Déterminer la matrice de u par rapport aux bases $\mathcal{B}$ et $\mathcal{B}'$.

   (b) Montrer que $\mathrm{Res}(P,Q) \neq 0$ si et seulement si P et Q sont premiers entre eux, donc que $\mathrm{Res}(P,Q) = 0$ si et seulement si P et Q ont au moins une racine complexe commune.

3. **Racine multiple**

   (a) Donner une condition nécessaire et suffisante en terme de résultant pour qu'un polynôme P de $\mathbb{C}[X]$ admette une racine multiple dans $\mathbb{C}$.

   (b) *Application* : étant donnés $a,b,c \in \mathbb{C}$, en déduire une condition nécessaire et suffisante pour que :

      i. le polynôme aX^2+bX+c admette une racine multiple.

      ii. le polynôme X^3+aX+b admette une racine multiple.

4. **Équation de Bézout**

   Montrer que les polynômes $P = X^4+X^3+1$ et $Q = X^3-X+1$ sont premiers entre eux et trouver une identité de Bézout $PA+QB=1$ avec A,B des polynômes de $\mathbb{C}[X]$:

   (a) en utilisant l'algorithme d'Euclide étendu,

   (b) en utilisant la première partie et à l'aide de l'application u.

II. Applications

5. **Matrices à valeurs propres toutes distinctes**

   (a) Montrer que l'ensemble D_0 des matrices carrées de $\mathcal{M}_n(\mathbb{C})$ à valeurs propres deux à deux distinctes forme un ouvert de $\mathcal{M}_n(\mathbb{C})$.

   (b) En déduire que D_0 est l'intérieur (topologique) de l'ensemble D des matrices diagonalisables de $\mathcal{M}_n(\mathbb{C})$.

6. **Nombre algébrique**

   En utilisant les polynômes $P(X) = X^2-3$ et $Q_x(X) = (x-X)^2-7$, $x \in \mathbb{C}$, déterminer un polynôme à coefficients entiers de degré 4 ayant comme racine $\sqrt{3}+\sqrt{7}$. Quelles sont les autres racines de ce polynôme ?

7. **Courbe algébrique paramétrée**

   Dans le plan $\mathbb{R}^2$, on considère la courbe paramétrée $t \mapsto (t^2+t, t^2-t+1)$ définie sur $\mathbb{R}$. On note $\mathcal{C}$ l'image de cette courbe. Montrer qu'il existe un polynome réel P à deux indéterminées tel qu'un point (x,y) du plan appartient à $\mathcal{C}$ si et seulement si ses coordonnées vérifient l'équation polynomiale $P(x,y)=0$ et donner un tel polynôme P.