Tous les corps considérés dans ce sujet seront implicitement supposés commutatifs.

Puissances d'une matrice

Soit $A = \begin{pmatrix} 3 & 2 & 1 \\ 0 & 3 & 2 \\ 0 & 0 & 3 \end{pmatrix} \in M_3(\mathbb{R})$. Calculer A^n en fonction de n pour tout entier naturel n.

Matrices de carré nul

Soit K un corps, et soit n un entier naturel non nul. Montrer qu'une matrice A de $M_n(K)$ vérifie $A^2 = 0$ si et seulement si il existe $r \leqslant n/2$, éventuellement nul, tel que A soit semblable à $\begin{pmatrix} 0 & I_r \\ 0 & 0 \end{pmatrix}$.

Crochet de Lie dans $M_n(K)$

Soit K un corps de caractéristique nulle, et soit n un entier naturel non nul.

1. Soient A et B deux matrices de $M_n(K)$. On pose
$$[A, B] = AB - BA.$$
Quelle est la trace de $[A, B]$?
2. Montrer que réciproquement, si $M \in M_n(K)$ est de trace nulle, alors il existe des matrices A et B de $M_n(K)$ telles que $M = [A, B]$. On pourra commencer par montrer que M est semblable à une matrice de diagonale nulle.

Bézout matriciel

1. Soit A un anneau commutatif unitaire. Pour tout entier naturel non nul n, on note $GL_n(A)$ le groupe des éléments inversibles de l'anneau $M_n(A)$ des matrices carrées de taille n à coefficients dans A. Caractériser $GL_n(A)$.
2. Soient n entiers relatifs $x_1, \cdots, x_n$ premiers entre eux dans leur ensemble. Montrer qu'il existe une matrice de $GL_n(\mathbb{Z})$ dont la première colonne est
$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$
Peut-on la choisir dans $SL_n(\mathbb{Z})$?

Théorème de Frobenius-Zolotarev

1. Soient n et m deux entiers naturels tous non nuls. Déterminer tous les morphismes de groupes de $GL_n(\mathbb{R})$ vers $\mathfrak{S}_m$. (Cette question sert juste à donner des idées ; à part ça, elle n'a rien à voir avec la suivante.)
2. Soit p un nombre premier différent de 2, et soit n un entier naturel non nul. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le coprs à p éléments. Comme toute matrice A de $GL_n(\mathbb{F}_p)$ définit une bijection de l'espace vectoriel $V = \mathbb{F}_p^n$ dans lui-même, on peut voir $GL_n(\mathbb{F}_p)$ comme un sous-groupe du groupe $\mathfrak{S}(V)$ des permutations de l'ensemble fini V. Montrer alors que $A \in GL_n(\mathbb{F}_p)$ est dans le groupe alterné $\mathfrak{A}(V)$ si et seulement si son déterminant est un carré dans $\mathbb{F}_p$.

Matrice magique

Soient $(a_1, \cdots, a_n)$ et $(b_1, \cdots, b_n)$ deux familles de n réels. On suppose les a_i et les b_i tous distincts, et on note $M \in M_n(\mathbb{R})$ la matrice de coefficients $a_i + b_j$. Montrer que si le produit des éléments d'une ligne de M est une constante qui ne dépend pas de la ligne, alors il en va de même pour les colonnes de M.

Déterminant de Cauchy

Soient K un corps, n un entier naturel non nul, et $a_1, \cdots, a_n, b_1, \cdots, b_n$ $2n$ éléments de K tels que $a_i + b_j$ ne soit jamais nul. Calculer le *déterminant de Cauchy*

$$\begin{vmatrix} \frac{1}{a_1+b_1} & \cdots & \frac{1}{a_1+b_n} \\ \vdots & \ddots & \vdots \\ \frac{1}{a_n+b_1} & \cdots & \frac{1}{a_n+b_n} \end{vmatrix}.$$

En cas de besoin, on pourra considérer la fraction rationnelle

$$R(X) = \frac{(b_1 - X)\cdots(b_{n-1} - X)}{(X + a_1)\cdots(X + a_n)} \in K(X).$$

Déterminant de Hurwitz

Soit K un corps, et soient $a, b, x_1, \cdots, x_n$ des éléments de K. On cherche à calculer le déterminant de taille n

$$\Delta = \begin{vmatrix} x_1 & a & \cdots & \cdots & a \\ b & x_2 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & x_{n-1} & a \\ b & \cdots & \cdots & b & x_n \end{vmatrix}.$$

1. Dans cette question, on suppose $a \neq b$. En considérant le déterminant $\Delta(X)$ obtenu en ajoutant X à tous les coefficients de Δ, calculer Δ.
2. Si mantenant $a = b$, calculer Δ en remplaçant b par l'indéterminée X et en travaillant dans le corps $K(X)$.
3. Soit E l'ensemble $\{1, \cdots, n\}$. On suppose qu'il existe p parties $E_1, \cdots, E_p$ de E deux-à-deux distinctes telles qu'il existe un $c \in \mathbb{N}$ tel que pour tous $i \neq j$, $card\ E_i \cap E_j = c$. En considérant la matrice $(\mathbf{1}_{i \in E_j}) \in M_{n,p}(\mathbb{Q})$, montrer que $p \leqslant n$.

Déterminant de Schmidt

Calculer pour tout entier naturel non nul n les déterminants des matrices $(d_{i,j})_{1 \leqslant i,j \leqslant n}$ et $(\delta_{i,j})_{1 \leqslant i,j \leqslant n}$, où $d_{i,j}$ est le nombre de diviseurs communs à i et à j et $\delta_{i,j}$ est le pgcd de i et de j.

Lemme de Gauss et critère d'Eisenstein

Lorsque $P \in \mathbb{Z}[X]$ est un polynôme non nul à coefficients entiers, on appelle *contenu* de P et on note $c(P)$ le pgcd des coefficients de P.

1. Soient $P, Q \in \mathbb{Z}[X]$ tous non nuls. Montrer que $c(PQ) = c(P)c(Q)$. Ceci est le lemme de Gauss.
2. Soit $P \in \mathbb{Z}[X]$ un polynôme irréductible dans $\mathbb{Z}[X]$. Montrer qu'il est aussi irréductible dans $\mathbb{Q}[X]$.
3. Quel est le polynôme minimal sur $\mathbb{Q}$ de $\sqrt{2} + \sqrt{3}$?
4. Soit $P = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p qui divise tous les a_i sauf a_n, et dont le carré ne divise pas a_0 (on dit que P est *d'Eisenstein en p*). Montrer que P est irréductible dans $\mathbb{Q}[X]$.

Divination

Soit A un anneau unitaire, non supposé commutatif. Soient $a, b \in A$ tels que $1 - ab$ est inversible. $1 - ba$ est-il nécessairement inversible ?

Newton, polynômes et polygones

1. Soit K un corps. On se donne n éléments $a_1, \cdots, a_n$ de K, et on pose

$$P = \prod_{i=1}^{n} (X - a_i) \in K[X].$$

Pour tout entier naturel k, on appelle S_k la k-ième *somme de Newton*

$$S_k = a_1^k + \cdots + a_n^k = \sum_{i=1}^{n} a_i^k,$$

et pour $1 \leqslant k \leqslant n$, on note σ_k les *fonctions symétriques élémentaires*

$$\sigma_1 = \sum_{i=1}^{n} a_i,\ \sigma_2 = \sum_{i<j} a_i a_j,\ \cdots,\ \sigma_n = \prod_{i=1}^{n} a_i.$$

En considérant la *série génératrice* $X^n P\left(\dfrac{1}{X}\right) \displaystyle\sum_{m=0}^{+\infty} S_m X^m$,

démontrer les relations suivantes :

- Si $1 \leqslant m \leqslant n,\ S_m - \sigma_1 s_{m-1} + \cdots + (-1)^{n-1} \sigma_{m-1} S_1 + (-1)^n \sigma_m m = 0,$
- Si $m \geqslant n,\ S_m - \sigma_1 s_{m-1} + \cdots + (-1)^m \sigma_n S_{m-n} = 0.$

2. Soient $n + 1$ nombres complexes $z_0, z_1, \cdots, z_n$ tels que tout polynôme $P \in \mathbb{C}[X]$ satisfasse la relation

$$P(z_0) = \frac{1}{n} \sum_{i=1}^{n} P(z_i).$$

Montrer que les $z_1, \cdots, z_n$ sont les affixes des sommets d'un n-gone régulier dont le centre est d'affixe z_0.

Symbole de Legendre

Soit p un nombre premier impair fixé une fois pour toutes. Afin d'alléger les notations, on appelle $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, et on pose $p' = (p-1)/2$. On note aussi $(\mathbb{F}_p^*)^2$ l'ensemble des carrés de $\mathbb{F}_p^*$. Enfin, si x est réel, on note $\lfloor x \rfloor$ sa partie entière.

1. Quel est le cardinal de $(\mathbb{F}_p^*)^2$?
2. Si $x \in \mathbb{Z}$ n'est pas divisible par p, on définit le *symbole de Legendre*
$$\left(\frac{x}{p}\right) = 1 \text{ si } x \in (\mathbb{F}_p^*)^2, \ -1 \text{ sinon.}$$
Montrer que $\left(\frac{x}{p}\right) \equiv x^{p'} \mod p$. En déduire la valeur de $\left(\frac{-1}{p}\right)$, puis montrer que $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.
3. On souhaite montrer que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Pour cela, on considère α une racine huitième primitive de l'unité de $\mathbb{F}_p$ dans la clôture algébrique de celui-ci. Que vaut α^4 ? On pose $\beta = \alpha + \alpha^{-1}$. Montrer que $2 \in (\mathbb{F}_p^*)^2$ si et seulement si $\beta \in \mathbb{F}_p$, et conclure.
4. Notre objectif est à présent de démontrer la *loi de réciprocité quadratique*, qui affire que si p et q sont premiers impairs distincts, alors
$$\left(\frac{p}{q}\right) = (-1)^{p'q'}\left(\frac{q}{p}\right).$$
Ceci nous permettrait de calculer le sybole de Legendre efficacement. Pour s'en convaincre, *en admettant teporarement la loi de réciprocité quadratique*, déterminer si 19 est un carré modulo 283.
5. On pose $S = \{1, 2, \cdots, p'\} \subset \mathbb{F}_p^*$, et on fixe $a \in \mathbb{Z}$ non-divisible par p. Vérifier que pour tout $s \in S$, on peut écrire $as = \epsilon_a(s)s_a$ avec $s_a \in S$ et $\epsilon_a(s) = \pm 1$, et montrer que l'application ainsi définie $S \to S$, $s \mapsto s_a$ est bijective.
6. Soit $\mu_a = Card\ \{s \in S | \epsilon_a(s) = -1\}$. Montrer que $\left(\frac{a}{p}\right) = (-1)^{\mu_a}$.
7. On pose $S_{p,q} = \sum_{s=1}^{p'} \left\lfloor \frac{sq}{p} \right\rfloor$ et $S_{q,p} = \sum_{s=1}^{q'} \left\lfloor \frac{sp}{q} \right\rfloor$. En considérant un rectangle de côtés p et q, montrer que $S_{p,q} + S_{q,p} = p'q'$.
8. Montrer que $S_{p,q} \equiv \mu_q \mod 2$, et conclure.