SESSION DE 1988

MATHÉMATIQUES GÉNÉRALES

DURÉE : 6 heures

Calculatrice électronique de poche — y compris calculatrice programmable et alphanumérique — à fonctionnement autonome, non imprimante, autorisée conformément à la circulaire n° 86-228 du 28 juillet 1986.

La clarté et la précision de la rédaction seront prises en compte dans l'appréciation de la copie.

OBJET DU PROBLÈME

On étudie la périodicité (éventuelle) de la suite 1, a, a^2, ... des puissances successives d'un élément d'un anneau, notamment dans le cas d'anneaux de matrices finis. La partie I étudie le cas particulier des éléments a tels que a^2 est égal à a. La partie II établit quelle forme peut prendre la périodicité envisagée. La partie III étudie le cas des anneaux de matrices sur les corps $\mathbb{R}$ et $\mathbb{C}$, la partie IV celui des anneaux de matrices sur un corps fini. Enfin, la partie V aborde le cas des matrices sur un quotient de $\mathbb{Z}$ et celui des quotients d'anneaux de polynômes sur un corps fini.

Sauf en ce qui concerne leurs dernières questions, les parties II à V n'utilisent pas les résultats de I, et les parties III à V n'utilisent que les résultats de II.1.

NOTATIONS

Dans tout le problème, « entier » signifie « entier naturel ». Les anneaux considérés ici seront toujours supposés unitaires et non triviaux (c'est-à-dire ayant au moins deux éléments) ; l'addition en sera notée +, la multiplication $\cdot$ (ou omise), les éléments neutres de l'addition et de la multiplication seront notés respectivement 0 et 1 (sauf mention spéciale). Les anneaux ne seront pas supposés commutatifs, en général.

Si a est un élément d'un anneau R et m un entier non nul, on notera (comme d'habitude) a^m pour le produit de m facteurs égaux à a. On conviendra de plus que a^0 est 1 pour tout a dans R (même nul). De la sorte les formules suivantes sont valables pour tout a dans R et tous m, n dans $\mathbb{N}$:

$$(a^m)(a^n) = a^{m+n} \qquad (a^m)^n = a^{mn}.$$

L'ensemble des éléments inversibles d'un anneau R sera noté R^*.

Si R est un anneau commutatif et r un entier non nul, on notera $\mathfrak{M}_r(R)$ l'anneau des matrices carrées $r \times r$ à coefficients dans R (les opérations étant définies de la même manière dans le cas d'un anneau commutatif quelconque que dans celui d'un corps commutatif), on notera dans ce cas $\mathbf{0}_r$ et $\mathbf{I}_r$ la matrice nulle et la matrice identité correspondantes (pour éviter la confusion avec les éléments 0 et 1 de R). On notera $\mathbf{J}_r$ l'élément de $\mathfrak{M}_r(R)$ dont le coefficient situé sur la i-ième ligne et la j-ième colonne est 1 si j est égal à $i+1$ et 0 sinon (en particulier $\mathbf{J}_1$ est $\mathbf{0}_1$).

RAPPEL

On pourra utiliser (sans démonstration) le résultat suivant : si K est un corps algébriquement clos, tout élément de $\mathfrak{M}_r(K)$ est semblable à une matrice diagonale de blocs du type :

$$\begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_s \end{pmatrix}$$

où chacun des blocs A_i est du type $\lambda_i \mathbf{I}_{r_i} + \mathbf{J}_{r_i}$ (forme réduite de Jordan).

I

1. *Pour tout anneau* R, *on pose :* $\mathscr{I}(R) = \{x \in R ; x^2 = x\}$; *on notera que* 0 *et* 1 *sont des éléments de* $\mathscr{I}(R)$.

1.*a*. Montrer que, si R est un anneau intègre, alors $\mathscr{I}(R)$ est réduit à $\{0,1\}$.

1.*b*. Montrer que, si p est un entier premier et α un entier non nul, alors $\mathscr{I}(\mathbb{Z}/p^\alpha\mathbb{Z})$ est réduit à $\{0,1\}$.

Tournez la page S.V.P.

1.*c.* Soit R un anneau quelconque : montrer que, si a est un élément de $\mathscr{I}$(R), alors $1 - a$ en est un aussi, et en déduire que le cardinal de $\mathscr{I}$(R), s'il est fini, est un entier pair.

1.*d.* Montrer que, si R est commutatif, alors $\mathscr{I}$(R) est stable par multiplication.

À quelle condition a-t-on l'équivalence : $x \in \mathscr{I}(R) \Leftrightarrow -x \in \mathscr{I}(R)$?

2.*a.* On suppose que K est un corps commutatif ; montrer que la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est dans $\mathscr{I}(\mathfrak{M}_2(K))$ si, et seulement si, ou bien elle est égale à 0_2 ou à I_2 ou bien a, b, c, d vérifient le système :

$$\begin{cases} a + d = 1 \\ ad = bc \end{cases}$$

2.*b.* Calculer le cardinal de $\mathscr{I}(\mathfrak{M}_2(\mathbb{Z}/p\mathbb{Z}))$ lorsque p est un nombre premier.

3. *On suppose que* p *et* q *sont des nombres premiers distincts.*

3.*a.* Il existe un isomorphisme entre les anneaux $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$; rappeler, sans démonstration, comment il est défini.

3.*b.* En déduire les cardinaux de $\mathscr{I}(\mathbb{Z}/pq\mathbb{Z})$ et de $\mathscr{I}(\mathfrak{M}_2(\mathbb{Z}/pq\mathbb{Z}))$.

4. *Soit* R *un anneau quelconque ; on définit sur* $\mathscr{I}$(R) *une relation binaire* $\leqslant$ *par :*

$$x \leqslant y \quad \textit{si et seulement si} \quad xy = yx = x\,.$$

Par ailleurs, deux éléments a, b *de* R *sont dits orthogonaux si et seulement si on a :* $ab = ba = 0$.

4.*a.* Montrer que $\leqslant$ est une relation d'ordre, admettant 0 comme minimum et 1 comme maximum.

4.*b.* On pose : $\mathscr{A}(R) = \{ x \in \mathscr{I}(R)$; 0 est le seul minorant strict de x pour $\leqslant \}$;
montrer que 1 est dans $\mathscr{A}$(R) si et seulement si $\mathscr{I}$(R) est réduit à $\{0,1\}$.

4.*c.* Montrer que, pour tout a non nul dans $\mathscr{I}$(R), il y a équivalence entre :

(i) a n'est pas dans $\mathscr{A}$(R) ;

(ii) il existe deux éléments non nuls b, c dans $\mathscr{I}$(R) tels que a est égal à $b + c$ et b et c sont orthogonaux.

4.*d.* On dit que R vérifie la condition ($\#$) si, et seulement si, il n'existe pas de suite infinie dans $\mathscr{I}$(R) qui soit strictement décroissante pour $\leqslant$.

Montrer que, si R vérifie la condition ($\#$), alors tout élément non nul de $\mathscr{I}$(R) qui n'est pas dans $\mathscr{A}$(R) s'écrit comme somme finie d'éléments de $\mathscr{A}$(R) deux à deux orthogonaux.

5. *On garde les notations de la question précédente et on suppose en outre, dans cette question, que* R *a la propriété suivante :*

quels que soient a, b dans $\mathscr{A}$(R), ab et ba sont égaux.

5.*a.* Montrer que deux éléments distincts de $\mathscr{A}$(R) sont nécessairement orthogonaux. En déduire que toute somme d'éléments distincts de $\mathscr{A}$(R) est dans $\mathscr{I}$(R).

5.*b.* Montrer que, si $b_1, \ldots, b_n$ sont des éléments distincts de $\mathscr{A}$(R), alors $\{b_1, \ldots, b_n\}$ est exactement l'ensemble des éléments de $\mathscr{A}$(R) qui minorent $b_1 + \cdots + b_n$ (pour $\leqslant$).

5.*c.* En déduire que, si R vérifie de plus la condition ($\#$), on a les faits suivants :

(i) la décomposition obtenue en 4.*d.* est unique ;

(ii) $\mathscr{A}$(R) est fini ;

(iii) $\mathscr{I}$(R) est fini ;

(iv) $\mathscr{I}$(R) muni de la loi $\cdot$ est isomorphe à l'ensemble des parties de $\mathscr{A}$(R) muni de l'intersection ;

(v) $(\mathscr{I}(R), .)$ est isomorphe à un produit $(\mathbb{Z}/2\mathbb{Z}, .)^n$, où n est un entier qu'on précisera.

5.*d.* Que peut-on dire du cardinal de $\mathscr{I}$(R) lorsqu'on suppose que R est un anneau commutatif fini ? Ce résultat s'étend-il au cas non commutatif ?

5.*e.* Application : déterminer les entiers ≤ 60 dont les images dans $\mathbb{Z}/60\mathbb{Z}$ constituent les éléments de $\mathscr{I}(\mathbb{Z}/60\mathbb{Z})$ et ceux de $\mathscr{A}(\mathbb{Z}/60\mathbb{Z})$.

Tournez la page S.V.P.

II

Pour tout anneau R, *on pose :*

$$\mathscr{P}(\mathrm{R}) = \{x \in \mathrm{R} \, ; (\exists\, m \geq 0)\,(\exists\, n > 0)\,(x^{m+n} = x^m)\}.$$

On définit comme suit deux applications μ, π *de* $\mathscr{P}(\mathrm{R})$ *dans* $\mathbb{N}$ *: pour* a *dans* $\mathscr{P}(\mathrm{R})$, $\mu(\mathrm{a})$ *est le plus petit entier* m *tel qu'il existe* n *non nul avec* $\mathrm{a}^{\mathrm{m+n}} = \mathrm{a}^{\mathrm{m}}$, *et* $\pi(\mathrm{a})$ *est le plus petit entier* n *non nul tel que* $\mathrm{a}^{\mu(\mathrm{a})+\mathrm{n}}$ *est égal à* $\mathrm{a}^{\mu(\mathrm{a})}$. *On note* $\mathrm{x} \mid \mathrm{y}$ *la relation* « x divise y » *(dans* $\mathbb{N}$ *ou* $\mathbb{Z}$*).*

1.*a.* Montrer que, si a est dans $\mathscr{P}(\mathrm{R})$ et que $a^{\mu(a)+r}$ est égal à $a^{\mu(a)+r'}$ où r, r' sont deux entiers positifs ou nuls strictement inférieurs à $\pi(a)$, alors r et r' sont égaux.

1.*b.* Montrer que, pour a dans $\mathscr{P}(\mathrm{R})$ et m, n entiers avec n non nul, il y a équivalence entre :
(i) $a^{m+n} = a^m$.
(ii) $\mu(a) \leq m$ et $\pi(a) \mid n$.

1.*c.* Soit a dans R et k un entier non nul ; montrer que a^k est dans $\mathscr{P}(\mathrm{R})$ si, et seulement si, a est dans $\mathscr{P}(\mathrm{R})$ et montrer que, dans ce cas, on a les relations :

$$\mu(a^k) \leq \mu(a) \leq k\,\mu(a^k)$$
$$\pi(a^k) \mid \pi(a) \qquad \text{et} \qquad \pi(a) \mid k\,\pi(a^k).$$

1.*d.* Montrer que a est dans $\mathscr{P}(\mathrm{R})$ si, et seulement si, il existe k non nul tel que a^k est dans $\mathscr{I}(\mathrm{R})$; précisément, montrer que, si a est dans $\mathscr{P}(\mathrm{R})$ et k est un entier non nul, alors a^k est dans $\mathscr{I}(\mathrm{R})$ si, et seulement si, k vérifie :

$$\mu(a) \leq k \qquad \text{et} \qquad \pi(a) \mid k.$$

En déduire que, si a est dans $\mathscr{P}(\mathrm{R})$, le plus petit entier k non nul tel que a^k est dans $\mathscr{I}(\mathrm{R})$ vérifie :

$$\sup(\mu(a), \pi(a)) \leq k \leq \mu(a) + \pi(a).$$

1.*e.* Soit a un élément de $\mathscr{P}(\mathrm{R})$; montrer que a est inversible si, et seulement si, $\mu(a)$ est égal à 0. Montrer que, dans ce cas, a^{-1} est égal à $a^{\pi(a)-1}$, et que $\pi(a)$ est exactement l'ordre de a en tant qu'élément du groupe multiplicatif R^*.

1.*f.* Montrer que, si R est fini, alors $\mathscr{P}(\mathrm{R})$ est égal à R tout entier ; obtenir, pour a dans R, un majorant de la valeur de $\mu(a) + \pi(a)$ en fonction du cardinal de R.

2.*a.* Montrer que, si b et c sont deux éléments orthogonaux de R (c'est-à-dire qu'on a : $bc = cb = 0$), alors, pour tout entier n non nul, on a : $(b+c)^n = b^n + c^n$.

En déduire que, si b et c sont dans $\mathscr{P}(\mathrm{R})$ et sont orthogonaux, alors $b + c$ est dans $\mathscr{P}(\mathrm{R})$ et on a :

$$\mu(b+c) \leq \sup(\mu(b), \mu(c))$$
$$\text{et} \qquad \pi(b+c) \mid \mathrm{ppcm}(\pi(b), \pi(c)).$$

2.*b.* Soit b un élément de $\mathscr{P}(\mathrm{R})$ tel que $\mu(b)$ est inférieur ou égal à 1 ; montrer que, pour tout entier k non nul, on a :.

$$\left(b + 1 - b^{\pi(b)}\right)^k = b^k + \left(1 - b^{\pi(b)}\right)^k = b^k + 1 - b^{\pi(b)}.$$

En déduire que $b + 1 - b^{\pi(b)}$ est dans R^* et que $\pi(b)$ est un diviseur du cardinal de R^* si celui-ci est fini.

2.*c.* On pose : $\mathscr{N}(\mathrm{R}) = \{x \in \mathrm{R} \, ; \ (\exists\, m \geq 1)(x^m = 0)\}.$

Montrer que, si c est dans $\mathscr{N}(\mathrm{R})$, alors $1 - c$ est dans R^* ; en déduire que, dans ce cas, $\mu(c)$ est inférieur ou égal au cardinal de R^* (si celui-ci est fini).

2.*d.* Soit a un élément quelconque de $\mathscr{P}(\mathrm{R})$ et k un entier non nul tel que a^k est dans $\mathscr{I}(\mathrm{R})$;
on pose : $b = a^{k+1}$ *et* $c = a(1 - a^k)$;
montrer que b et c sont orthogonaux et appartiennent à $\mathscr{P}(\mathrm{R})$, que $\mu(b)$ est inférieur ou égal à 1 et que c est dans $\mathscr{N}(\mathrm{R})$. En déduire que, si le cardinal de R^* est un entier fini N, on a :

$$\mu(a) \leqslant \mathrm{N} \qquad \text{et} \qquad \pi(a) \mid \mathrm{N}.$$

Que dire de la majoration ainsi obtenue de $\pi(a)$ par N dans le cas où R est un corps fini ?

Tournez la page S.V.P.

III

On s'intéresse dans cette partie aux anneaux de matrices à coefficients dans les corps $\mathbb{C}$ *et* $\mathbb{R}$.

1. Soit R un anneau commutatif ; montrer que si A est une matrice diagonale de blocs :

$$\begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_s \end{pmatrix}$$

avec $A_1, \ldots, A_s$ dans $\mathfrak{M}_{r_1}(R), \ldots, \mathfrak{M}_{r_s}(R)$ respectivement, alors A est dans $\mathscr{P}\left(\mathfrak{M}_{r_1+\cdots+r_s}(R)\right)$ si et seulement si $A_1, \ldots, A_s$ sont dans $\mathscr{P}\left(\mathfrak{M}_{r_1}(R)\right), \ldots, \mathscr{P}\left(\mathfrak{M}_{r_s}(R)\right)$ respectivement ; dans ce cas, calculer $\mu(A)$ et $\pi(A)$ en fonction de $\mu(A_1), \ldots, \mu(A_s)$, $\pi(A_1), \ldots, \pi(A_s)$.

2.*a.* À quelle condition la matrice $\lambda I_r + J_r$ est-elle dans $\mathscr{P}\left(\mathfrak{M}_r(\mathbb{C})\right)$?

2.*b.* Caractériser les éléments de $\mathscr{P}\left(\mathfrak{M}_r(\mathbb{C})\right)$ en termes de leurs valeurs propres et des dimensions des sous-espaces propres associés.

2.*c.* Quels sont les couples d'entiers (m, n) tels qu'il existe dans $\mathscr{P}\left(\mathfrak{M}_r(\mathbb{C})\right)$ un élément A tel que $\mu(A)$ soit égal à m et $\pi(A)$ à n ?

2.*d.* Donner un exemple d'anneau R tel que, pour tout couple d'entiers (m, n) avec n non nul, il existe dans $\mathscr{P}(R)$ un élément A tel que $\mu(A)$ est égal à m et $\pi(A)$ est égal à n.

3.*a.* Montrer que tout élément de $\mathfrak{M}_2(\mathbb{R})$ qui n'est pas multiple de I_2 est semblable à une matrice du type : $\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$; en déduire que deux matrices de $\mathfrak{M}_2(\mathbb{R})$ non multiples de I_2 sont semblables si et seulement si elles ont même polynôme caractéristique.

3.*b.* Décrire les éléments de $\mathscr{P}\left(\mathfrak{M}_2(\mathbb{R})\right)$: on déterminera un élément pour chaque classe de similitude et on précisera le polynôme caractéristique de cet élément.

IV

On étudie ici les valeurs des fonctions μ *et* π *dans le cas des anneaux de matrices à coefficients dans un corps fini.*

Dans toute cette partie, F *désigne un corps commutatif fini. La caractéristique de* F *est notée* p, *et le cardinal de* F *est noté* q. *On sait que* p *est un nombre premier, et qu'il existe un entier* α *non nul tel que* q *est égal à* p^α. *On admettra l'existence d'un corps algébriquement clos* F' *dont* F *est un sous-corps.*

On notera θ *et* γ *les deux fonctions de* $\mathbb{N}^2$ *dans* $\mathbb{N}$ *définies pour* $x \geq 2$ *et* $s \geq 1$ *par :*

$$\theta(x, s) = \operatorname{ppcm}(x - 1,\ x^2 - 1, \ldots, x^s - 1)$$

et $\gamma(x, s) =$ le plus petit entier k tel que x^k est $\geq s$.

1.*a.* On suppose que P est un polynôme (à une variable) à coefficients dans F de degré d supérieur ou égal à 2 et que P est irréductible dans F.

Soit λ une racine de P dans F' ; on note K le F-sous-espace vectoriel de F' engendré par $1, \lambda, \ldots, \lambda^{d-1}$:

Tournez la page S. V. P.

(i) montrer que, si S est un polynôme non nul à coefficients dans **F** de degré $\leq d-1$, il existe U et V dans **F** [X] tels qu'on ait : $1 = UP + VS$;
(ii) en déduire que K est un corps ;
(iii) montrer que λ^{q^d-1} est égal à 1.

1.*b.* Soit Q un polynôme (à une variable) à coefficients dans **F** de degré s et soit λ une racine de Q dans **F**′ ; montrer que λ est dans $\mathscr{P}$ (**F**′) et qu'on a :

$$\mu(\lambda) = \begin{cases} 0 & \text{si } \lambda \neq 0 \\ 1 & \text{si } \lambda = 0 \end{cases} \qquad \text{et} \qquad \pi(\lambda) \mid \theta(q, s)\,.$$

2.*a.* Montrer que si, dans un anneau R, la somme de p termes $1+1+\cdots+1$ est nulle et que a et b sont deux éléments de R qui commutent (c'est-à-dire tels que ab et ba sont égaux), alors on a pour tout entier e :

$$(a+b)^{p^e} = a^{p^e} + b^{p^e}.$$

2.*b.* Montrer que, si λ est dans $\mathscr{P}$ (**F**′), alors $\lambda \mathbf{I}_r + \mathbf{J}_r$ est dans $\mathscr{P}\left(\mathfrak{M}_r(\mathbf{F}')\right)$ et on a :

$$\mu(\lambda \mathbf{I}_r + \mathbf{J}_r) \leq r$$
$$\text{et} \qquad \pi(\lambda \mathbf{I}_r + \mathbf{J}_r) \mid \pi(\lambda)\, p^{\gamma(p,r)}$$

(on séparera les deux cas $\lambda = 0$ et $\lambda \neq 0$).

3.*a.* Montrer que toute matrice A dans $\mathfrak{M}_r(\mathbf{F})$ est dans $\mathscr{P}\left(\mathfrak{M}_r(\mathbf{F})\right)$ et établir les relations suivantes :

$$\mu(A) \leq r \qquad \text{et} \qquad \pi(A) \mid \theta(q, r)\, p^{\gamma(p,r)}.$$

3.*b.* En déduire une majoration de $\pi(A)$ dans le cas $q = 4$, $r = 2$; comparer le résultat obtenu avec celui qu'on peut déduire de II.1.*f*.

3.*c.* Dénombrer les bases (ordonnées) d'un espace vectoriel de dimension r sur **F** et en déduire le cardinal de $\left(\mathfrak{M}_r(\mathbf{F})\right)^*$; établir alors, à l'aide de II.2.*d*, une nouvelle majoration de π, que l'on comparera, toujours dans le cas $q = 4$, $r = 2$, avec celle obtenue en 3.*a*.

V

On étudie ici les valeurs des fonctions μ et π dans le cas d'anneaux de matrices sur un quotient de **Z** *et celui de quotients d'anneaux de polynômes sur un corps fini.*

1. *Dans cette question,* p *est un entier premier fixé.*

1.*a.* Soit A dans $\mathfrak{M}_r(\mathbf{Z})$ et i, j deux entiers ; on suppose qu'il existe B dans $\mathfrak{M}_r(\mathbf{Z})$ telle que A^j soit égale à $A^i + pB$; montrer que, pour tout entier e, il existe B_e dans $\mathfrak{M}_r(\mathbf{Z})$ telle qu'on ait :

$$A^{jp^e} = A^{ip^e} + p^{e+1} B_e.$$

1.*b.* En déduire que, pour tout entier α non nul et pour toute matrice A dans $\mathfrak{M}_r(\mathbf{Z}/p^\alpha\mathbf{Z})$, on a les relations suivantes :

$$\mu(A) \leq rp^{\alpha-1} \qquad \text{et} \qquad \pi(A) \mid \theta(p, r)\, p^{\gamma(p,r)+\alpha-1}$$

(on appliquera le résultat de IV.3. à une matrice convenable).

2.*a.* Soit q un entier ≥ 2 ; on suppose que la décomposition de q en facteurs premiers est $p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Montrer que, pour toute matrice A dans $\mathfrak{M}_r(\mathbf{Z}/q\mathbf{Z})$, on a :

$$\mu(A) \leq r \sup\left(p_1^{\alpha_1-1}, \ldots, p_s^{\alpha_s-1}\right)$$
$$\text{et} \qquad \pi(A) \mid \operatorname*{ppcm}_{1 \leq i \leq s} \left(\theta(p_i, r)\, p_i^{\gamma(p_i,r)+\alpha_i-1}\right).$$

2.*b.* Calculer explicitement les majorants ainsi obtenus dans le cas de $\mathfrak{M}_2(\mathbf{Z}/24\mathbf{Z})$.

3. *Dans cette question,* **F** *désigne à nouveau un corps fini ; on note* p *sa caractéristique et* q *son cardinal.*

3.*a.* On suppose que P est un polynôme irréductible de degré d à coefficients dans **F** ; montrer que, pour tout entier β non nul et tout élément a de l'anneau quotient $\mathbf{F}[X]/(P^\beta)$ — en désignant par (P^β) l'idéal engendré par P^β —, on a :

$$\mu(a) \leq p^{\gamma(p,\beta)} \qquad \text{et} \qquad \pi(a) \mid p^{\gamma(p,\beta)}(q^d - 1).$$

3.*b.* Obtenir un résultat analogue dans le cas d'un quotient quelconque de l'anneau **F** [X].

• • •
•