Matrices à coefficients dans un corps fini

Adrien REISNER[1]

Abstract. It is considered the set A_p of matrices of order 2 with their entries in $\mathbb{Z}_p$, defined by $A_p = \{a = \lambda M + \mu I; \lambda, \mu \in \mathbb{Z}_p\}$, and some properties of this set are presented (Theorems 1,3,6,7,9).
Keywords: unitary ring, the order of an element, the field $\mathbb{Z}_p$, isomorphism.
MSC 2000: 15A33.

A étant un anneau unitaire d'éléments neutre e on appelle *ordre d'un élément inversible* a de A le plus petit entier positif n del que $a^n = e$; dans ce cas l'ensemble $G_a = \{e, a, a^2, \ldots, a^{n-1}\}$ forme un sous-groupe du groupe G des éléments inversibles de l'anneau A: l'ordre n de l'élément $a \in G$ est le cardinal du ce sous-groupe G_a.

Pour toute matrice carrée M à coefficients dans un corps on désigne par T et Δ respectivement les deux applications suivantes: $T{:}M \to T(M)$=trace de la matrice M, $\Delta : M \to \Delta(M)$=déterminant de la matrice M.

p désignant un *nombre premier strictement supérieur à 3*, on considère le *corps fini* $\mathbb{Z}_p$ des classes résiduelles modulo p. M et I étant les deux matrices suivantes à coefficients dans $\mathbb{Z}_p$:

$$M = \begin{pmatrix} \widehat{4} & \widehat{1} \\ -\widehat{1} & \widehat{0} \end{pmatrix}, \quad I = \begin{pmatrix} \widehat{1} & \widehat{0} \\ \widehat{0} & \widehat{1} \end{pmatrix},$$

on considère l'ensemble A_p des matrices d'ordre 2 à coefficinets dans $\mathbb{Z}_p$ défini par:

$$A_p = \{a = \lambda M + \mu I; \lambda, \mu \in \mathbb{Z}_p\}.$$

Théorème 1. *L'ensemble A_p est un anneau commutatif unitaire pour les opérations usuelles. De plus: Card $A_p = p^2$.*

Démonstration. On a immédiatement $M^2 = \widehat{4}M - I$; on en déduit compte tenu de la structure de l'ensemble $\mathcal{M}_2(\mathbb{Z}_p)$ que A_p est un *algèbre* associative et unitaire. Enfin, la commutativité se vérifie directement. D'autre part, (I, M) étant une base de l'algèbre A_p, on a $A_p \simeq \mathbb{Z}_p^2$ et par suite: Card $A_p = (\text{Card } \mathbb{Z}_p)^2 = p^2$.

La proposition suivante se vérifie immédiatement par le calcul.

Proposition 2. *Pour toute matrice $A = \lambda M + \mu I \in A_p$, on a:*
a) $T(A) = \widehat{2}(\widehat{2}\lambda + \mu)$, $\Delta(A) = \lambda^2 + \mu^2 + \widehat{4}\lambda\mu$;
b) $T(A^2) = T^2(A) - 2\Delta(A)$.
En particulier, $T(A^2) = \widehat{2}(\widehat{7}\lambda^2 + \mu^2 + \widehat{4}\lambda\mu)$.

Théorème 3. *Pour $A \in A_p$, deux quelconques des conditions suivantes impliquent la troisième: a) $T(A) = \widehat{0}$, b) $\Delta(A) = \widehat{1}$, c) A est une matrice d'ordre 4.*

[1]Centre de Calcul E.N.S.T., Paris; e-mail: *adrien.reisner@enst.fr*

Démonstration. **a**) + **b**) ⇒ **c**) Le théorème de Cayley-Hamilton appliquée à la matrice A donne:

$$A^2 - T(A)A + \Delta(A)I = O.$$

Il vient alors avec les hypothèses a) et b): $A^2 = -I$ et $A^4 = I$. L'ordre de la matrice A devise donc 4 et comme $A^2 \neq I$ (p étant impair), 2 n'est pas multiple de cet ordre. Finalement, A est d'ordre 4.

a) + **c**) ⇒ **b**) Supposant les conditions a) et c) vérifiées, on a:

$$A^2 = -\Delta(A)I \text{ et } I = A^4 = \Delta^2(A)I.$$

On en déduit: $\Delta^2(A) = \widehat{1}$, $\Delta(A) \neq -\widehat{1}$ soit $\Delta(A) = \widehat{1}$.

b) + **c**) ⇒ **a**) Compte tenu de b) et c), $A^2 = T(A)A - I$ d'où

$$I = A^4 = T^2(A)A^2 - \widehat{2}T(A)A + I = T(A)[T^2(A) - \widehat{2}]A + [\widehat{1} - T^2(A)]I.$$

On peut distinguer deux cas: I *A et I sont liés*, i.e. $A = \mu I$. Dans ce cas, $A^2 = \mu^2 I$, $A^4 = \mu^4 I$, d'oú, A étant d'ordre 4: $\mu^2 \neq \widehat{1}$, $\mu^4 = \widehat{1}$, $\mu^2 = -\widehat{1}$ et $A^2 = -I$, $T(A)A = 0$. Si $T(A) \neq \widehat{0}$, alors $A = O$ d'où $T(A) = \widehat{0}$, impossible. Par suite $T(A) = \widehat{0}$. II *$\{A, I\}$ est une famille libre.* Dans ce cas l'égalité $I = T(A)[T^2(A) - \widehat{2}]A + [\widehat{1} - T^2(A)]I$ implique: $\widehat{1} = \widehat{1} - T^2(A)$ d'oú $T(A) = \widehat{0}$. Le théorème est ainsi démontré.

On considère la suite des entiers $\{Y_k\}_{k\geq 0}$ définie par $Y_0 = 2$ et $Y_{k+1} = 2Y_k^2 - 1$, $k \geq 0$, dont les premiers terms sont: $Y_0 = 2$, $Y_1 = 7$, $Y_2 = 97$, $Y_3 = 18817, \ldots$

Théorème 4. *Pour tout $k \geq 0$, on a $2Y_k \in T(M^{2^k})$.*

Démonstration. Par récurrence sur k. Pour $k = 0$ la propriété se vérifie trivialment puisque $2Y_0 = 4 \in \widehat{4} = T(M)$. Supposant la propriété vérifiée à l'ordre k, démontrons-là pour $k + 1$. On a immédiatment d'une part: $2Y_{k+1} = 4Y_k^2 - 2 = (2Y_k)^2 - 2$ et d'autre part $T(M^{2^{k+1}}) = T[(M^{2^k})^2] = T^2(M^{2^k}) - \widehat{2}$, compte tenu de l'assertion b) de la Proposition 2 et puisque $\Delta(M) = \widehat{1}$. Donc, compte tenu de l'hypothèse de récurrence: $2Y_{k+1} = (2Y_k)^2 - 2 \in T(M^{2^{k+1}})$.

Théorème 5. *La matrice M est d'ordre 2^k si et seulement si $p|Y_{k-2}$.*

Démonstration. Supposons la matrice M d'ordre 2^k, i.e. $M^{2^k} = I$. On a: $M^2 = \begin{pmatrix} \widehat{15} & \widehat{4} \\ -\widehat{4} & -\widehat{1} \end{pmatrix}$ et par suite l'ordre de M ne divise pas 2 soit $k \geq 2$. En posant alors $A = M^{2^{k-2}}$ on a, M étant d'ordre 2^k : $A^2 = M^{2^{k-1}} \neq I$, $A^4 = M^{2^k} = I$. $A \in A_p$ est donc une matrice d'ordre 4 vérifiant aussi $\Delta(A) = \widehat{1}$. Compte tenu du théorème 3, $b) + c) \Rightarrow a)$, il vient alors: $T(A) = \widehat{0}$ soit d'après le théorème précédent: $2Y_{k-2} \in T(A) = \widehat{0}$, i.e. p divise $2Y_{k-2}$ et finalement p étant impair $p|Y_{k-2}$.

Réciproquement, avec les mêmes notations si $p|Y_{k-2}$ i.e. $Y_{k-2} \equiv 0 \pmod{p}$, alors $T(A) = \widehat{0}$. Mais, comme $\Delta(A) = \widehat{1}$, le théorème 3, $a) + b) \Rightarrow c)$, montre que la matrice A est d'ordre 4 soit $M^{2^k} = I$ et $M^{2^{k-1}} = A^2 \neq I$. L'ordre de M divisant 2^k mais non 2^{k-1} est donc égal à 2^k.

Théorème 6. *Les deux assertions suivantes sont équivalentes:*

a) $\widehat{3}$ *n'est pas le carré d'un élément de* $\mathbb{Z}_p$*;*

b) A_p *est un corps.*

Démonstration. a) $\Rightarrow$ **b**) Si $\widehat{3}$ n'est pas le carré d'un élément de $\mathbb{Z}_p$, alors pour $A \in A_p$:

$$\Delta(A) = \widehat{0} \Rightarrow A = O.$$

En effet, supposons $\Delta(A) = \widehat{0}$. Pour $A \in A_p$ on a: $\Delta(A) = \widehat{0} = (\lambda + \widehat{2}\mu)^2 - \widehat{3}\mu^2$. $\mu \neq \widehat{0}$ impliquerait $\widehat{3} = (\lambda\mu^{-1} + \widehat{2})^2$ ce qui est exclut par hypothèse. Donc $\mu = \widehat{0}$ et $\Delta(A) = \widehat{0} = \lambda^2$ soit: $\lambda = \widehat{0}$ et finalement: $A = O$. Donc l'ensemble A_p est formé de la matrice nulle et de matrices *inversibles* dans $\mathcal{M}_2(\mathbb{Z}_p)$.

$A \neq O$ étant une matrice de A_p, l'application $A_p \to A_p$ définie par $X \to AX$ est linéaire et injective, donc *surjective* ($\dim A_p = 2$). Pour $A \neq O$ il existe $B \in A_p$ telle que: $AB = 1$ soit $A^{-1} = B \in A_p$: les inverse des matrices non nulles de A_p sont dans A_p.

b) $\Rightarrow$ **a**) Nous allons montrer que, *non* **a**) $\Rightarrow$ *non* **b**). Supposons qu'il existe $a \in \mathbb{Z}_p$ tel que $a^2 = \widehat{3}$. Dans ce cas: $\Delta(A) = [\lambda + (\widehat{2} - a)\mu][\lambda + (\widehat{2} + a)\mu]$. Pour la matrice $A = (a - \widehat{2})M + I(a \neq \widehat{2}$ puisque $\widehat{2}^2 - \widehat{3} = \widehat{1})$ on a $\Delta(A) = \widehat{0}$ et (Cayley-Hamilton) $A(A - T(A)I) = O$ avec $A \neq O$ et $A \neq T(A)I$. On en déduit que A_p *n'est pas intègre* et par suite que A_p n'est pas un corps.

Théorème 7. *En supposant que* $\widehat{3}$ *est un carré dans* $\mathbb{Z}_p$*:*

a) M est semblable à une matrice diagonale;

b) A_p *est isomorphe à l'anneau produit* $\mathbb{Z}_p \times \mathbb{Z}_p$*;*

c) dans A_p *il y a* $p-1$ *éléments de déterminant* $\widehat{1}$ *et* $(p-1)^2$ *éléments inversibles.*

Démonstration. a) L'équation caractéristique de la matrice M s'écrit $X^2 - \widehat{4}X + \widehat{1} = (x - \widehat{2})^2 - a^2 = 0$ où a est tel que $a^2 = \widehat{3}$. M ayant deux valeurs propre *distinctes* $\lambda_1 = \widehat{2} + a$ et $\lambda_2 = \widehat{2} - a$, on en déduit que la matrice M est *diagonalisable* i.e. il existe $P \in GL_2(\mathbb{Z}_p)$ telle que $M = \begin{pmatrix} \widehat{2} + a & \widehat{0} \\ \widehat{0} & \widehat{2} - a \end{pmatrix} P^{-1}$.

b) L'application $R \to P^{-1}RP$ qui est un *automorphisme* pour la structure d'anneau, transforme toute matrice $A = \lambda M + \mu I$ de A_p en une *matrice diagonale*. Or l'ensemble $\mathcal{D}_p$ des matrices diagonales de $\mathcal{M}_2(\mathbb{Z}_p)$ ayant comme cardinal p^2 (je rappelle que Card $A_p = p^2$), l'application $A_p \to \mathcal{D}_p$, $A \to P^{-1}AP$ est donc un isomorphisme.

D'autre part, l'application $\mathbb{Z}_p \times \mathbb{Z}_p \to \mathcal{D}_p$, $(\alpha, \beta) \to \begin{pmatrix} \alpha & \widehat{0} \\ \widehat{0} & \beta \end{pmatrix}$, étant de façon immédiate un isomorphism, on en déduit que: $A_p \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ (cet isomorphisme est même un isomorphisme d'algèbre).

c) Compte tenu de l'isomorphisme précédent, comme $\Delta(A) = \Delta(P^{-1}AP)$, le nombre de matrices $A \in A_p$ telles que $\Delta(A) = \widehat{1}$ est égal aux nombre de couple (α, β) vérifiant $\alpha\beta = \widehat{1}$. Il y en a $p - 1$ (choisir d'abord α).

La démonstration de l'implication *a*) $\Rightarrow$ *b*) du Théoreme 6 a montré que $\Delta(A) \neq \widehat{0} \Rightarrow A^{-1} \in A_p$. On en déduit que le nombre de matrices A inversibles de A_p (i.e. le

nombre des matrices $A \in A_p$ telles que $\Delta(A) \neq \widehat{0}$) est égal aux nombre des couples $(\alpha, \beta) \in \mathbb{Z}_p \times \mathbb{Z}_p$ vérifiant $\alpha\beta = \widehat{0}$ soit $(p-1)^2$.

Corollaire 8. *Dans le cas où $\widehat{3}$ est un carré dans $\mathbb{Z}_p$:*
a) l'ordre de la matrice M divise $p-1$;
b) si $p|Y_{k-2}$, alors $2^k|p-1$.

Démonstration. a) L'ensemble des matrices de A_p de déterminant $\widehat{1}$ forment un sous-groupe multiplicatif de A_p^*, groupe des matrices inversibles de A_p (si $A \in A_p$ et $\Delta(A) \neq \widehat{0}$, alors $A^{-1} \in A_p$–voir *a)* $\Rightarrow$ *b)* du théorème 6). Compte tenu de l'assertion c) du théorème précédent ce sous-groupe est fini de cardinal $p-1$. Or la matrice M appartient à ce sous-groupe. L'ordre de M divise par suite $p-1$ (ordre de ce sous-groupe).

b) Si p divise Y_{k-2}, alors la matrice M est d'ordre 2^k d'aprés le Théorème 5. L'assertion a) de ce corollaire permet alors de conclure.

Théorème 9. *En supposant que $\widehat{3}$ n'est pas un carré dans $\mathbb{Z}_p$:*
a) Δ est un homomorphisme du groupe multiplicatif des éléments non nuls de A_p dans celui des éléments non nuls de $\mathbb{Z}_p$;
b) il existe k tel que $p-1 =$ Card (Im Δ) *et Card Ker*$\Delta = \mathrm{k(p+1)}$*;*
c) il existent $p+1$ éléments de déterminant $\widehat{1}$ dans A_p.

Démonstration. a) A_p étant un corps d'après le Théorème 6, l'assertion a) est évidente.

b) On en déduit l'isomorphisme $\mathrm{Im}\,\Delta \simeq A_p^*/\mathrm{Ker}\Delta$ et par suite: Card $A_p^* = p^2-1 =$ (Card Im Δ)(Card Ker Δ). De plus, Im Δ est un sous-groupe de $\mathbb{Z}_p^*$: il existe k tel que $p-1 = k$ Card (Im Δ), d'où Card Ker $\Delta = k(p+1)$. Notons que $1 \leq k \leq p-1$.

c) Les matrices A de Ker Δ vérifient $\Delta(A) = \widehat{1}$. Il s'agit de montrer que Card Ker $\Delta = p+1$. L'égalité $\Delta(A) = \widehat{1}$ entraîne, compte tenu de l'assertion a) de la Proposition 2: $\lambda^2 + \mu^2 + \widehat{4}\lambda\mu - \widehat{1} = \widehat{0}$ (1). $\lambda \in \mathbb{Z}_p$ étant donné, il existe donc 0, 1 ou 2 éléments $\mu \in \mathbb{Z}_p$ tels que $\Delta(A) = \widehat{1}$ ($\mathbb{Z}_p$ étant un corps), donc il existe au plus 2p couples (λ, μ) vérifiant l'équation (1). D'autre part, le nombre de tels couples est égal à-voir b)-$k(p+1)$ = Card Ker Δ. On en déduit finalement que $k = 1$ et par suite Card Ker $\Delta = p+1$.

Corollaire 10. *Dans le cas où $\widehat{3}$ n'est pas un carré dans $\mathbb{Z}_p$:*
a) l'ordre de la matrice M divise $p+1$;
b) si $p|Y_{k-2}$, alors $2^k|p+1$.

Démonstration. a) La matrice M de déterminant $\widehat{1}$ appartient au sous-groupe Ker Δ. L'ordre de M divise par suite l'ordre $p+1$ de ce sous-groupe Ker Δ -voir l'assertion c) du Théorème 9.

b) De même qu'au Corollaire 8, si p divise Y_{k-2}, alors la matrice M est d'ordre 2^k d'aprés le Théorème 5. L'assertion a) de ce corollaire permet alors de conclure.

Remarque. Dans le cas où $\widehat{3}$ n'est pas un carré dans $\mathbb{Z}_p$, l'ordre de *toute matrice* A de A_p vérifiant $\Delta(A) = \widehat{1}$ divise $p+1$ - ordre de sous-groupe Ker Δ. Par suite $\forall A \in A_p : A^{p+1} = I$.