DM n°10

Pour le 1e février.

EXERCICE I —Entiers de Gauss —

Les élèves intéressés, compléteront par l'exercice 38.
Soient $\mathbf{Z}[i]$ l'ensemble des nombres complexes de la forme $u+iv$, avec $(u,v) \in \mathbf{Z}^2$ et l'$A_p$plication. $\varphi\,;\, \mathbf{Z}[i] \to \mathbf{N}\,;\; a \mapsto \bar{a}a$.

1. Montrer que $\mathbf{Z}[i]$ est un sous-anneau du corps $\mathbf{C}$.
2. Déterminer $\mathbf{Z}[i]^*$, ensemble des éléments inversibles de $\mathbf{Z}[i]$.
3. Montrer que pour tout élément a de $\mathbf{Z}[i]$ et tout élément b de $\mathbf{Z}[i] \setminus \{0\}$, il existe un couple (non nécessairement unique) (q,r) d'éléments de $\mathbf{Z}[i]$ tel que $a = bq + r$ et $\varphi(r) < \varphi(b)$. On dit que l'anneau $\mathbf{Z}[i]$ est euclidien pour φ.
4. Montrer que tout idéal de $\mathbf{Z}[i]$ est de la forme $a\mathbf{Z}[i]$, on dit que $\mathbf{Z}[i]$ est principal.
5. Soit a un élément de $\mathbf{Z}[i]$. Montrer que si $\varphi(a)$ est premier, alors a est un élément irréductible de $\mathbf{Z}[i]$.
   rappelons qu'un élément a d'un anneau intègre est dit irréductible si par définition il n'est pas inversible et si il admet la décomposition $a = bc$, alors a ou b est inversible.

PROBLÈME I —Extentions de corps —

Les élèves intéressés, compléteront par le DM supplémentaire des vacances de Noël.
Première partie : Un exemple d'extension du corps $\mathbf{Q}$

1. Soit P le polynôme $X^3 - X - 1$.
   Montrer que P n'a pas de racines rationnelles. En déduire que P est irréductible dans $\mathbf{Q}[X]$.
   Montrer que P a une racine réelle que l'on notera ω.
2. Soit $\mathbf{K}$ le $\mathbf{Q}$-espace vectoriel engendré par $(\omega^i)_{i\in\mathbf{N}}$.
   Montrer que $\mathbf{K}$ est de dimension finie, et donner une base simple de K.
3. Montrer que $\mathbf{K}$ est une $\mathbf{Q}$-sous-algèbre de $\mathbf{R}$, muni de sa structure naturelle de $\mathbf{Q}$-algèbre.
4. Montrer que $\mathbf{K}$ est un sous-corps de $\mathbf{R}$.

Deuxième partie : Cas général d'extension de $\mathbf{Q}$
Soit a un réel.

1. Montrer que tout sous-corps de $\mathbf{R}$ contient $\mathbf{Q}$.
2. Montrer que l'ensemble des sous-corps de $\mathbf{R}$ qui contiennent a admet un plus petit élément pour l'inclusion. On le notera dans la suite $\mathbf{Q}(a)$.
3. Montrer que $\phi\ :\ \mathbf{Q}[X] \to \mathbf{R}\,;\; P \mapsto P(a)$ est un morphisme de la $\mathbf{Q}$-algèbres $\mathbf{Q}[X]$ dans la $\mathbf{Q}$ algèbre $\mathbf{R}$. On note $\mathbf{Q}[a]$ son image.

4. Soit $I := \{P \in \mathbf{Q}[X], P(a) = 0\}$. Montrer que I est un idéal de $\mathbf{Q}[X]$.
5. Le réel a est dit algébrique (sur $\mathbf{Q}$), si, par définition, a est racine d'un polynôme non nul à coefficients entiers.
   Montrer que a est algèbrique si et seulement si I est non réduit à $\{0\}$.
   Dans cette partie on suppose dans la suite que que a est algèbrique, sauf à la dernière question.
6. Montrer qu'il existe un et un seul élément de $\mathbf{Q}[X]$ unitaire, μ_a, tel que $I = \mu_a\mathbf{Q}[X]$.
   Montrer que μ_a est irréductible dans $\mathbf{Q}[X]$. Montrer que si a est irrationnel, alors le degré de μ_a est supérieur ou égal à 2. Déterminer μ_a pour $a = \sqrt{2}$ et pour $a = \sqrt{\frac{1+\sqrt{5}}{2}}$.
7. Montrer que $\mathbf{Q}[a]$ est un corps. Montrer que $\mathbf{Q}(a) = \mathbf{Q}[a]$.
   Montrer que $\mathbf{Q}(a)$ est un $\mathbf{Q}$-espace vectoriel de dimension n, où n est le degré de μ_a, dont on donnera une base simple.
8. Si a est non algébrique, montrer qu'alors $\mathbf{Q}(a)$ est un $\mathbf{Q}$-espace vectoriel de dimension infinie [1].

PROBLÈME II

Dans tout le problème, p désigne un nombre premier strictement supérieur à 3, $\mathbf{Z}_p$ l'anneau quotient $\mathbf{Z}/p\mathbf{Z}$.

Si A est un anneau fini, d'élément unité e, on $A_p$pelle ordre d'un élément inversible a de A, le plus petit entier strictement positif ω tel que $a^\omega = e$.

Pour toute matrice carrée M à coefficients dans un corps, on note $\Delta(M)$ son déterminant et $T(M)$ sa trace.

Les 3/2 vérifieront que pour tout élément M de $\mathcal{M}_2(\mathbf{R})$, on a : $\chi_M(M) = 0_2$ (Théorème de Caylay-Hamilton).

I

1. Soit A_p l'ensemble des matrices à coefficient dans $\mathbf{Z}_p$ de la forme

   $$R = \lambda M + \mu I,$$

   où

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

   et λ et μ sont des éléments de $\mathbf{Z}_p$.
   Montrer que A_p est un anneau commutatif pour l'addition et la multiplication des matrices usuelles.
   Donner le nombre d'éléments de A_p.
2. Calculer $T(R)$ et $\Delta(R)$ pour R dans A_p. Exprimer $T(R^2)$ et $\Delta(R^2)$ en fonction de $T(R)$ et $\Delta(R)$.
3. Montrer que deux quelconques des conditions suivantes impliquent la troisième :
   i. T(R)=0.
   ii. $\Delta(R) = 1$.
   iii. L'ordre de R est 4.

1. On pourrait montrer que $\mathbf{Q}(a)$ est isomorphe en tant que corps au corps $\mathbf{Q}(X)$.

4. On considère la suite d'entiers $(Y_k)_{k\in N}$, définie par

$$Y_0 = 2 \text{ et } Y_{k+1} = 2Y_k^2 - 1.$$

, Comparer Y_k et $T(M_k)$, pour tout entier naturel k.

5. Montrer que pourtout entier naturel k, l'ordre de M est 2^k si et seulement si p divise Y_{k-2}.

II

1. Montrer que A_p est un corps si et seulement si $\bar{3}$ n'est pas le carré d'un élément de $\mathbf{Z}_p$.
2. Dans cette question, on suppose que $\bar{3}$ est un carré dans $\mathbf{Z}_p$: $\bar{3} = a^2$, où $a \in \mathbf{Z}_p$). Montrer que M est semblable à une matrice diagonale. En déduire que A_p est isomorphe à l'anneau produit $\mathbf{Z}_p \times \mathbf{Z}_p$, puis donner le nombre des éléments de A_p de déterminant 1, ainsi que celui de ses éléments inversibles.
3. Dans cette question, on suppose que $\bar{3}$ n'est pas un carré dans $\mathbf{Z}_p$.
   (a) Montrer que Δ donne un homomorphisme du groupe multiplicatif des éléments non nuls de A_p dans celui des éléments non nuls de $\mathbf{Z}_p$. En déduire que le nombre des éléments de l'image de Δ est un diviseur de $p-1$ et que celui des éléments du noyau de Δ est un multiple de $p+1$.
   (b) Vérifier que, pour tout $\lambda \in \mathbf{Z}_p$, il y a au plus deux éléments μ de $\mathbf{Z}_p$ tels que $\Delta(\lambda M + \mu I) = 1$

   Donner alors de nombre des éléments de A_p de déterminant 1.
4. Montrer que l'ordre de M divise le nombre des éléments de A_p de déterminant 1.
   En déduire que, si p divise Y_{k-2} alors 2^k divise $p-1$ ou $p+1$.

indication pour le DM n°9

Pour le 1e février.

EXERCICE I —Entiers de Gauss —

1. Sans problème.
2. Supposons que z soit un inversible de l'anneau $\mathbf{Z}[i]$, alors
$$1 = \varphi(1) = \varphi(zz^{-1}) = \varphi(z)\varphi(z^{-1}).$$
Donc φ qui est à valeurs dans $\mathbf{N}$ est inversible, donc vaut 1. Donc z est élément de $\{1, -1, i, -i\}$ ensemble des entiersde Gauss de module 1.
Réciproquement tout élément de $\{1, -1, i, -i\}$ est inversible dans $\mathbf{Z}[i]$, 1 et -1 étant leur propre inverse et i et $-i$ inverses l'un de l'autre.
L'ensemble des inversibles de $\mathbf{Z}[i]$ est $\{1, -1, i, -i\}$.
3. Notons α et β les parties réelle et imaginaire de $\frac{a}{b}$ ($b \neq 0$). Arrondissons α et β à l'entier (ou l'un des entiers) le plus proche (donc distant de moins de $\frac{1}{2}$), respectivement q_1 et q_2 et posons $q = q_1 + iq_2$, élément de $\mathbf{Z}[i]$. Alors
$$\varphi\left(\frac{a}{b} - q\right) = (\alpha - q_1)^2 + (\beta - q_2)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2};$$
de plus $a = bq + b\left(\frac{a}{b} - q\right)$ et $\varphi\left(b\left(\frac{a}{b} - q\right)\right) \leq \varphi(b)\frac{1}{2} < \varphi(b)$.
D'où le résultat.
4. Soit I un idéal. Excluons le cas où I est trivial et donc de la forme $0\mathbf{Z}[i]$, alors l'ensemble $\{\varphi(z), z \in \backslash\{0\}\}$ est une parie non vide de $\mathbf{N}$ et donc admet un plus petit élément, ce qui autorise à considérer a un élément de $I \setminus \{0\}$ de module au carré minimum.
• L'idéal engendré par a est évidement inclus dans l'idéal I : $a\mathbf{Z}[i] \subset I$. • Soit $z \in$. Par division euclidienne z s'écrit $z = qa + r$ avec q et r des entiers de Gauss et $\varphi(r) < \varphi(a)$. par le premier point $qa \in I$ et comme I est un sous-groupe de $\mathbf{Z}[i]$, on a $z - qa \in I$, autant dire que r est un élément de I de module au carré STRICTEMENT inférieur à celui de a donc est nul. Donc $z \in a\mathbf{Z}[i]$, et donc $I \subset a\mathbf{Z}[i]$.
Concluons : $I = a\mathbf{Z}[i]$.
5. Supposons $\phi(a)$ premier.
• Donc $\phi(a) \neq 1$ et donc a n'est pas inversible, ni nul.
• Soit $a = bc$ une décomposition de a en produit de deux éléments de $\mathbf{Z}[i]$. On a $\phi(a) = \phi(b)\phi(c)$, donc par primalité de $\phi(a)$ et positivité de φ, $\phi(a)$ ou $\phi(b)$ égal à 1, donc a ou b est inversible par 1.
De ces deux points nous vient {it la primalité de a.

PROBLÈME I —Extentions de corps —

Première partie

1. Soit P le polynôme $X^3 - X - 1$.
   Supposons que P ait une racinne rationnelle r. Elle s'écrit : $r = \frac{p}{q}$ avec $p \in \mathbf{Z}$, $q \in \mathbf{N}$ et p et q premiers entre eux. On a donc : $r^3 - r - 1 = 0$, Soit

   $$p^3 - pq^2 - q^3 = 0. \tag{1}$$

   On déduit de cette égalité que p divise q^3. Or p et q sont premiers entre eux donc le théorème de Gauss dit que p divise q^2. Une nouvelle application du thèorème de gauss donne que p divise q, enfin une dernière application de ce théorème donne que p divise 1. Donc :

   $$p = 1. \tag{2}$$

   On déduit aussi de (1) que q divise p^3. Un raisonnement analogue au précédent donne $q|1$. Donc

   $$q = \pm 1. \tag{3}$$

   Donc on déduit de (2–3), que les seules racines rationnelles possibles sont 1 et -1. Or $P(1) = -1$, $P(-1) = -1$. Donc P n'admet pas de racines rationnelles.

   Montrons que P est irréductible dans $\mathbf{Q}[X]$. En premier lieu P n'est pas inversible. Ensuite, supposons que P s'écrive $P = AB$, avec A et B éléments de $\mathbf{Q}[X]$. Alors $\mathrm{d}^\circ A + \mathrm{d}^\circ B = \mathrm{d}^\circ P$. Or ni A ni B ne sont de degré 1, car un élément de $\mathbf{Q}[X]$ de degré 1 admet une racine rationnelle et P n'en admet pas. Donc $\mathrm{d}^\circ A = 0$ et $\mathrm{d}^\circ B = 3$ où $\mathrm{d}^\circ B = 0$ et $\mathrm{d}^\circ A = 3$.
   En conclusion P est irréductible dans $\mathbf{Q}[X]$.

   Le polynôme P est de degré *impair* à coefficients *réels*, il admet donc une racine réelle ω, puisque un au moins de ses facteurs irréductibles dans $\mathbf{R}$ est de degré 1.

2. Soit c un élément de $\mathbf{K}$. Par définition de $\mathbf{K}$, il s'écrit $c = \sum_{i=0}^{n} a_i \omega^i$, avec $n \in \mathbf{N}$ et $a_0, a_1, \ldots, a_n$ des rationnels. Soit l'élément de $\mathbf{Q}[X]$, $C = \sum_{i=0}^{n} a_i X^i$. Par division euclidienne de C par P dans $\mathbf{Q}[X]$ on obtient :

   $$C = QP + rX^2 + sX + t, \tag{4}$$

   avec $Q \in \mathbf{Q}[X]$, r, s et t des rationnels. En substituant ω à l'indéterminée dans (4), il vient : $c = C(\omega) = Q(\omega)P(\omega) + r\omega^2 + s\omega + t = r\omega^2 + s\omega + t$. Donc c étant quelconque, on a : $\mathbf{K}$ est le Q-espace vectoriel engendré par la sous famille de $(\omega^i)_{i\in\mathbf{N}}$, $(\omega^0, \omega^1, \omega^2)$.

   Montrons que la famille $(\omega^0, \omega^1, \omega^2)$ est libre. Soit λ, μ et ν des rationnels tels que : $\lambda\omega^2 + \mu\omega + \nu = 0$. Soit l'élément de $\mathbf{Q}[X]$, $C = \lambda X^2 + \mu X + \nu$. Supposons C non nul. Alors par division euclidienne : $P = \tilde{Q}C + uX + v$ avec $\tilde{Q} \in \mathbf{Q}[X]$, u et v des rationnels. En substituant dans cette égalité ω à l'indéterminée, il vient $0 = u\omega + v$. Comme ω est irrationnel $u = 0$ et donc $v = 0$, et donc C divise P. Mais P étant irréductible C est constant non nul, ce qui contredit $C(\omega) = 0$. Donc C est nul, c'est-à-dire : $\lambda = \mu = \nu = 0$. D'où la liberté de $(\omega^0, \omega^1, \omega^2)$.

   Finalement $(\omega^0, \omega^1, \omega^2)$ est une base de K.

3. • K sous-espace vectoriel sur Q de $\mathbf{R}$ est *stable par combinaison linéaire.*
   • soient x et x' des éléments de K. On dispose de rationnels a, b, c, a', b', c' tels que $x = a\omega^2 + b\omega + c,\ x' = a'\omega^2 + b'\omega + c'$. Alors
   $$xx' = aa'\omega^4 + (ab' + a'b)\omega^3 + (ac' + a'c + bb')\omega^2 + (bc' + c'b)\omega + cc'.$$
   Donc $xx' \in \underset{\mathbf{Q}}{\text{vect}}(\omega^i)_{i\in\mathbf{N}} = K$. Donc K *est stable par produit.*
   • Enfin $1 = \omega^0 \in K$.
   De ces trois points on déduit : K est une $\mathbf{Q}$-sous-algèbre de $\mathbf{R}$.
4. D'après (c), K est un sous-anneau de $\mathbf{R}$, il est donc *commutatif* et *non trivial.*
   Soit, par ailleurs, x un élément non nul de K. Il existe, d'après (b), des rationnels a, b et c non tous nuls, tels que $x = a\omega^2 + b\omega + c$. Soit $D = aX^2 + bX + C$. P et D sont, dans $Q[X]$, premiers entre eux, en effet P est irréductible (cf. 1.) et ne divise pas D, puisque $\mathrm{d}^\circ P > \mathrm{d}^\circ D > -\infty$. Le lemme de Bezout assure donc l'existence de U et V éléments de $\mathbf{Q}[X]$ tels que : $UD + VP = 1$. En substituant ω à l'indéterminée X dans cette égalité, il vient :
   $$U(\omega)D(\omega) + V(\omega)P(\omega) = xD(\omega) = 1.$$
   Donc $D(\omega)$ est l'inverse de x. *L'inverse de x est donc élément de K.*
   Conclusion : K est un sous-corps de $\mathbf{R}$.

Deuxième partie Cas général :

Soit a un réel.

1. Soit K_0 un sous-corps de $\mathbf{R}$. Il contient 1, donc, étant stable par somme et différence il contient $\mathbf{Z}$. K_0 étant stable par passage à l'inverse et multiplication il contient $\mathbf{Q}$.
2. Soit $\mathcal{K}$ l'ensemble des sous-corps de $\mathbf{R}$ qui contiennent a. Soit $\mathbf{Q}(a)$, l'intersection de tous les éléments de $\mathcal{K}$:
   $$\mathbf{Q}(a) = \underset{K\in\mathcal{K}}{\cap} K.$$
   • $\mathbf{Q}(a)$ est un sous-corps de $\mathbf{R}$ comme intersection non vide ($\mathbf{R} \in \mathcal{K}$) de sous-corps.
   • Pour tout élément K de $\mathcal{K}$, $a \in K$, donc $a \in \mathbf{Q}(a)$.
   • Soit K_0 un sous-corps de $\mathbf{R}$ qui contient a, par définition de $\mathcal{K}$, $K_0 \in \mathcal{K}$ donc
   $$\mathbf{Q}(a) = \underset{K\in\mathcal{K}}{\cap} K \subset K_0.$$
   Donc l'ensemble $\mathcal{K}$ des sous-corps de $\mathbf{R}$ qui contiennent a,
   admet $\mathbf{Q}(a)$ comme plus petit élément pour l'inclusion.
3. Soient P et Q des éléments de $\mathbf{Q}[X]$, λ et μ des rationnels.
   • $\phi(\lambda P + \mu Q) = (\lambda P + \mu Q)(a) = \lambda P(a) + \mu Q(a) = \lambda\phi(P) + \mu\phi(Q)$.
   • $\phi(P \times Q) = (P \times Q)(a) = P(a) \times Q(a) = \phi(P) + \phi(Q)$.
   • $\phi(1) = 1$.
   Donc ϕ est un morphisme de la $\mathbf{Q}$-algèbre $\mathbf{Q}[X]$ dans la $\mathbf{Q}$-algèbre $\mathbf{R}$.
4. D'après la question précédente, ϕ induit notamment un morphisme de l'anneau $\mathbf{Q}[X]$ sur l'anneau $\mathbf{R}$. I en est le *noyau*, c'est donc un idéal de $\mathbf{Q}[X]$.
5. • Hypothèse : I non réduit à 0.
   Il existe donc un polynôme P élément de $\mathbf{Q}[X]$, non nul tel que $P(a) = 0$. Notons d le degré de P et pour $i = 0, 1, \ldots, d$, a_i sont coefficient de degré i. Pour tout $i \in \{0, 1, \ldots, n\}$, a_i s'écrit $\dfrac{p_i}{q_i}$, avec $p_i \in \mathbf{Z}$ et $q_i \in \mathbf{N}^*$. Posons $\delta = q_0 \times q_1 \times \cdots \times q_d$. δP est un polynôme non nul à coefficients entiers et $(\delta P)(a) = 0$. Donc a *est algébrique.*

- HYPOTHÈSE : a est algébrique.
  Donc a est racine d'un polynôme P non nul à coefficients entiers. Donc I admet P comme élément et I *est non réduit à* 0.
  Donc a est algèbrique si et seulement si I est non réduit à $\{0\}$.

6. I est un idéal de $\mathbf{Q}[X]$, donc, d'après le programme, il existe P élément de $\mathbf{Q}[X]$ (appelé générateur de I), tel que $I = P\mathbf{Q}[X]$, I étant non nul, il admet un et un seul générateur unitaire.

   $\mu_a(a) = 0$, donc μ_a ne saurait être un inversible de $\mathbf{Q}[X]$. Soient A et B des éléments de $\mathbf{Q}[X]$, tels que $\mu_a = AB$. $A(a)B(a) = \mu_a(a) = 0$. L'intégrité de $\mathbf{Q}$ assure donc que $A(a)$ ou $B(a)$ est nul. Prenons par exemple $A(a)$ nul. Alors $A \in I$ donc $\mu_a | A$, or $A | \mu_a$ donc A et μ_a sont associés et donc B est de degré 0. Donc μ_a est irréductible.

   Supposons que $\mathrm{d}^\mathrm{o}\mu_a \leq 1$. $\mathrm{d}^\mathrm{o}\mu_a \neq -\infty$ (I non nul) et $\mathrm{d}^\mathrm{o}\mu_a \neq 0$ car $\mu_a(a) = 0$, donc $\mathrm{d}^\mathrm{o}\mu_a = 1$. Il existe donc s et t rationels tels que $s \neq 0$ et $\mu_a = sX + t$. De $\mu_a(a) = 0$ on déduit $a = -\frac{t}{s}$, et donc $a \in \mathbf{Q}$. Par contaposition :
   si a est irrationnel, alors le degré de μ_a est supérieur ou égal à 2.

   L'élément de $\mathbf{Q}[X]$, X^2-2 admet $\sqrt{2}$ comme racine. Donc $X^2-2 | \mu_{\sqrt{2}}$. Or $\sqrt{2}$ est notoirement irrationnel donc, comme on vient de le voir, $\mathrm{d}^\mathrm{o}\mu_{\sqrt{2}} \geq 2$. Donc $X^2 - 2$ qui est unitaire est égal à $\mu_{\sqrt{2}}$.

   $$\mu_{\sqrt{2}} = X^2 - 2.$$

   Maintenant $a = \sqrt{\frac{1+\sqrt{5}}{2}}$. L'élément de $\mathbf{Q}[X]$, $X^4 - X^2 - 1$ admet a comme racine. Donc $\mu_a | X^4 - X^2 - 1$. Montrons que $X^4 - X^2 - 1$ est irréductible dans $\mathbf{Q}[X]$. Supposons qu'il existe A et B éléments de $\mathbf{Q}[X]$ tels que :

   $$X^4 - X^2 - 1 = AB.$$

   En notant $a' = \sqrt{\frac{-1+\sqrt{5}}{2}}$. $X^4 - X^2 - 1$ admet quatre racines complexes, $a, -a, ia', -ia'$. $\sqrt{5}$ étant irrationnel, on montre qu'aucune de ses racines n'est rationnelle, donc ni A ni B n'est de degré 1. Supposons que $\mathrm{d}^\mathrm{o}A = 2$ et donc $\mathrm{d}^\mathrm{o}B = 2$. L'un des deux polynômes A et B, disons pour fixer les idées A, admet ia' comme racine, étant à coefficients rationnels donc réels, il admet aussi comme racine $\overline{ia'} = -ia'$. Donc il existe $c \in \mathbf{R}^*$, tel que $A = c(X^2 - \frac{1-\sqrt{5}}{2})$. A étant à coefficients rationnels, c est rationnel, mais alors $c\frac{1-\sqrt{5}}{2}$ est rationnel ce qui conduit à la rationnalité de $\sqrt{5}$, ce qui est faux. Donc finalement un des polynômes A et B est de degré 0, et donc $X^4 - X^2 - 1$ est *irréductible*.
   Donc μ_a, diviseur de $X^4 - X^2 - 1$ est associé à $X^4 - X^2 - 1$. Ces deux polynômes étant unitaires ils sont égaux :

   $$\mu_a = X^4 - X^2 - 1.$$

7. $\mathbf{Q}[a]$ est l'image par le morphisme d'anneaux ϕ de l'anneau $\mathbf{Q}[X]$ (cf. 3.), c'est donc un *sous-anneau* de $\mathbf{R}$. Comme $\mathbf{R}$ est un corps, l'anneau $\mathbf{Q}[a]$ est *commutatif et non trivial*. Soit x un élément non nul de $\mathbf{Q}[a]$. Il existe $P \in \mathbf{Q}[X]$ tel que $x = P(a)$. La division euclidienne de P par μ_a conduit à l'existence de Q et R éléments de $\mathbf{Q}[X]$ tels que : $P = Q\mu_a + R$

et $\mathrm{d}^\mathrm{o}R < \mathrm{d}^\mathrm{o}\mu_a$. D'où $x = P(a) = Q(a)\mu_a(a) + R(a) = R(a)$. x étant non nul, R est non nul, Donc μ_a ne saurait divisé R, polynôme dont le degré est inférieur au sien. Or μ_a est irréductible dans $\mathbf{Q}[X]$ (cf. 6.), donc R et μ_a sont premiers entres eux dans $\mathbf{Q}[X]$. Le lemme de Bezout affirme donc l'existence de deux éléments U et V de $\mathbf{Q}[X]$ tels que $UR+V\mu_a = 1$. En substituant a à l'indéterminé X, on obtient :

$$1 = U(a)R(a) + V(a)\mu_a(a) = U(a)x.$$

Donc $U(a) = x^{-1}$ et donc $x^{-1} \in \mathbf{Q}[a]$. Autrement dit $\mathbf{Q}[a]$ est *stable par passage à l'inverse.*

CONCLUSION : $\mathbf{Q}[a]$ est un corps.

$\mathbf{Q}[a]$ est un corps qui contient a. Donc $\mathbf{Q}(a) \subset \mathbf{Q}[a]$
Soit Soit x un élément de $\mathbf{Q}[a]$. Il sécrit

$$x = \sum_{i=0}^{n} c_i a^i,$$

avec n un naturel et $c_0, c_1, \ldots, c_n$ des rationnels. le corps $\mathbf{Q}(a)$ contenant 1 et a et étant stable par multiplication, il contient a^i, pour $i = 0, 1 \ldots, n$. Par ailleurs $c_i \in \mathbf{Q}(a)$ (cf. 1.). Donc le corps $\mathbf{Q}(a)$ étant stable par multiplication est addition, il contient $\sum_{i=0}^{n} c_i a^i = x$. Donc $\mathbf{Q}[a] \subset \mathbf{Q}(a)$.

CONCLUSION : $\mathbf{Q}(a) = \mathbf{Q}[a]$. $\mathbf{Q}[a]$ est l'image par ϕ, morphisme de $\mathbf{Q}$-espaces vectoriels, de l'espace vectoriel $\mathbf{Q}[X]$ (cf. 3.), c'est donc un *sous-espace vectoriel* du Q-espace vectoriel $\mathbf{R}$. En raisonnant comme dans le début de la question on montre que tout élément x de $\mathbf{Q}[a]$ est de la forme $x = R(a)$ où R est un élément de $\mathbf{Q}[X]$, de degré inférieur strictement à n, degré de μ_a. En notant c_i le coefficient d'ordre i de R, pour $i = 0, 1, 2 \ldots, n-1$, x s'écrit :

$$x = \sum_{i=0}^{n-1} c_i a^i.$$

Donc $\mathbf{Q}[a] \subset \underset{\mathbf{Q}}{\mathrm{vect}}(a^0, a^1, \ldots, a^{n-1})$. L'inclusion inverse étant évidente,

$$Q[a] = \underset{\mathbf{Q}}{\mathrm{vect}}(a^0, a^1, \ldots, a^{n-1}).$$

la famille *la famille* $(a^0, a^1, \ldots, a^{n-1})$ *engendre donc* $\mathbf{Q}[a]$.

8. Montrons que la famille $(a^0, a^1, \ldots, a^{n-1})$ est libre. Soient $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ des rationnels tels que : $\lambda_0 a^0 + \lambda_1 a^1 + \cdots + \lambda_{n-1} a^{n-1} = 0$. Soit l'élément de $\mathbf{Q}[X]$, $C = \lambda_0 X^0 + \lambda_1 X^1 + \cdots + \lambda_{n-1} X^{n-1}$. Supposons C non nul. Alors par division euclidienne : $\mu_a = \tilde{Q}C + R$ avec $\tilde{Q} \in \mathbf{Q}[X]$, $R \in \mathbf{Q}[X]$ et $\mathrm{d}^\mathrm{o}R \leq n-1$. En substituant dans cette égalité a à l'indéterminée, il vient $0 = R(a)$. Donc $R(a)$ est élément de I, il est donc divisible par μ_a, mais son degré étant inférieur strictement à celui de μ_a, c'est qu'il est nul. Donc C divise μ_a. Mais μ_a étant irréductible C est constant non nul, ce qui contredit $C(a) = 0$. Donc C est nul, c'est-à-dire : $\lambda_0 = \lambda_0 = \cdots = \lambda_{n-1} = 0$. D'où la liberté de $(a^0, a^1, \ldots, a^{n-1})$.

Finalement $(a^0, a^1, \ldots, a^{n-1})$ est une base de $\mathbf{Q}[a]$, qui est donc de dimension n.

9. Supposons que la famille $(a_i)_{i\in\mathbf{N}}$ soit liée. Montrons qu'alors a est algèbrique. Par hypothèse il existe $m \in \mathbf{N}$, $\lambda_0, \lambda_1, \ldots, \lambda_{m-1}$ des rationnels non tous nuls, tels que : $\lambda_0 a^0 + \lambda_1 a^1 + \cdots + \lambda_{m-1} a^{m-1} = 0$. Soit l'élément de $\mathbf{Q}[X]$,

$$D = \lambda_0 X^0 + \lambda_1 X^1 + \cdots + \lambda_{m-1} X^{m-1}.$$

D est non nul et $D \in I$, donc d'après 5., a est algébrique. Par contraposée, si a est non algébrique, alors la famille d'éléments de $\mathbf{Q}(a)$, $(a_i)_{i\in\mathbf{N}}$ est libre et donc $\mathbf{Q}(a)$ est de dimension infinie.

PROBLÈME II L'énoncé du problème confond les notations $\bar{n}$ classe de n dans $\mathbf{Z}_p$ et n lorsqu'aucune confusion n' est à craindre. Nous nuserons pas de cette liberté.

I

1. D'abord A_p est le sous espace vectoriel engendré par (I, M), cette famille étant manifestement libre le sous-espace vectoriel A_p de $\mathcal{M}_2(Z_p)$ est de dimension 2 et donc isomorphe à l'espace vectoriel $\mathbf{Z}^{p2}$ (par l'application coordonnées dans (I, M), par exemple). donc le cardinal de A_p est $|F_p|^2 = p^2$.
   Ensuite A_p jouit des propriétés suivantes :
   — il contient I ;
   — stabilité par addition (en tant que sous-espace vectoriel de $\mathcal{M}_2(\mathbf{Z}_p)$) ;
   — stabilité par multiplication en effet la famille génératrice (I, M) est stable par produit, puisque — et c'est la seule chose à vérifier — $M^2 \in \text{vect}(I, M)$ grâce au théorème de Cayley-Hamilton.
   Donc A_p est un sous-anneau de l'anneau $\mathcal{M}_2(\mathbf{Z}_p)$. Il est de plus commutatif, puisqu'inclus dans l'algèbre commutative $F_p[M]$.
2. Soit R élément de A_p de coordonnées (μ, λ) dans (I, M).
   • $T(R) = \bar{4}\lambda + \bar{2}\mu$ et $\Delta(R) = \lambda^2 + \bar{4}\lambda\mu + \mu^2$.
   • par propriété du déterminant, $\Delta(R^2) = [\Delta(R)]^2$.
   • Par le théorème de Cayley-Hamilton,

$$R^2 - T(R)R = (R)I = O_2, \tag{C-H}$$

   donc $T(R^2) = [T(R)]^2 - \bar{2}\Delta(R)$.
3. Montrer que deux quelconques des conditions suivantes impliquent la troisième :
   i. T(R)=0.
   ii. $\Delta(R) = 1$.
   iii. L'ordre de R est 4.
   Gardons les notations précédentes.
   • *Supposons i. et ii.*
   Par (C-H), $R^2 = -I$, et donc $R^4 = I$ donc l'ordre de R est un diviseur de 4 qui n'est pas 2 et qui n'est pas 1, car $T(R) = 0 \neq T(I)$. D'où iii.
   • *Supposons i. et iii.* Par (C-H) et i., on a $R^2 = -\Delta(R)I$ et donc par iii., $I = R^4 = \Delta(R)^2 I$. Donc $\Delta(R) \pm \bar{1}$ mais $\Delta(R) \neq -\bar{1}$ car sinon R^2 serait égal à I contredisant iii. Donc $\Delta(R) = 1$, soit ii.
   • Supposons ii. et iii. Le théorème de Cayley-Hamilton appliqué à R^2 puis à R donne :

$$\bar{2}I = T(R^2)R^2 \text{ et } R^2 = T(R)R - I$$

   Donc

$$\bar{2}I = T(R^2)(T(R)R - I) = (T(R^2)T(R))\ R + T(R^2)I.$$

   En admettant un instant la liberté de (R, I) on : $(T(R^2)T(R)) = \bar{0}$ et $T(R^2) = \bar{2}$. Donc $T(R) = 0$ puisque $\bar{2}$ nest pas nul car $p \geq 3$. D'ou i.
   La liberté de R et I vient de ce que si $R = \mu I$, alors par ii. $1 = D(R) = \mu^2$ et donc $R^2 = \mu^2 I = I$ ce qui contredit ii.

D'où l'équivalence de i., ii., et iii.

Remarque. Pour le dernier point on pouvait se vautrer dans la théorie.

Le polynôme caractéristique de M qui est annulateur est le polynôme minimal, car si ce dernier était de degré 1, On aurait $R = \mu I$ ou $\mu \in \mathbf{Z}_p$ et par ii. viendrait $\bar{1} = \Delta(R) = \mu^2$ puis $R^2 = \mu^2 I = I$, ce qui contredirait iii.

Comme par iii., $X^4 - \bar{1}$ est annulateur pour R, on a $X^2 - T(R)X + \bar{1}$ divise $X^4 - \bar{1}$. Donc $X^4 - 1$ s'écrit

$$X^4 - \bar{1} = (X^2 - T(R)X + \bar{1})(X^2 + aX - \bar{1}),$$

ou $a \in \mathbf{Z}_p$. En développant

$$X^4 - \bar{1} = (X^4 + (a - T(R))X^3 - T(R)aX^2 + (T(R) + a)X - \bar{1}.$$

Donc $T(R) = a\,; T(R)a = 0\,; T(R) = -a$ ce qui conduit à $T(R) = 0$ de plusieurs façons

4. Une récurrence sans malice montre que pour tout $k \in \mathbf{N}$,

$$\boxed{T(M^{2k}) = \bar{2}\bar{Y}_k.}$$

5. Le théorème de Cayley-Hamilton assure que $M^2 = \bar{4}M - I$, donc , puisque $p \neq 2$, $M^2 \neq I$ si l'ordre de M est 2^k, alors $k \in [\![2, +\infty[\![$

Soit un entier $k \geq 2$. Posons $R := M^{2^{k-2}}$. On a $R^4 = M^{2^k}$, $R^2 = M^{2^{k-1}}$.

Supposons M d'ordre 2^k alors $R^4 = I$ et donc l'ordre de R divise 4, mais n'est pas 2 ni 1, donc est 4.

Réciproquement supposons l'ordre de R égal à 4. Alors $M^{2^k} = I$, l'ordre de M est donc un diviseur de 2^k, qui ne divise pas 2^{k-1} (comme $R^2 \neq I$), autant dire 2^k.

Donc l'ordre de M est 2^k si et seulement si R est d'ordre 4, mais $\Delta(R) = \Delta(M)^{2^k} = 1^{2^k} = 1$, donc par 3., l'ordre de M est 2^k si et seulement si $T(R) = \bar{0}$.

Or par 4., $T(R) = \bar{2}\bar{Y}_k$ et comme $\bar{2}$ est inversible ($p \neq 2$) on a que M est d'ordre 2^k si et seulement si Y_k

Montrer que pourtout entier naturel k, l'ordre de M est 2^k si et seulement si p divise Y_{k-2}.

II

1. Soit R un élément de A_p NON NUL, on note toujours (μ, λ) ses coordonnées dans (I, M). Supposons R inversible dans A_p. *A fortiori* R est inversible dans $\mathcal{M}_2(\mathbf{Z}_p)$, donc son déterminant est non nul.

Réciproquement si $\Delta(R) \neq 0$ alors le théorème de Cayley-Hamilton donne

$$R^{-1} = -D(R)^{-1}(R - T(r)I) \in A_p.$$

Donc R est inversible dans A_p si et seulement si son déterminant est non nul. Or l'expression du polynôme caractéristique de R montre qu'il admet 0 comme racine si et seulement si $\Delta(R) = 0$, donc R est inversible dans A_p si et seulement si $0 \neq \mathrm{sp}(R)$.

• Cas 3 n'est pas un carré.

Pour commencer observons que

$$\chi_M(X) = X^2 - \bar{4}X + \bar{1} = (X - \bar{2})^2 - \bar{3}.$$

Donc le spectre de M est vide.

Si λ est nul alors μ ne l'est pas ($R \neq O_2$) et A est inversible dans A_p d'inverse $\frac{1}{\mu}I$.

Sinon, prenons α une éventuelle valeur propre de R et X un vecteur propre qui lui est associé. On a $\lambda MX + \mu X = \alpha X$, donc $MX = \left(\frac{\alpha-\mu}{\lambda}\right) X$, ce qui contredit la vacuité du spectre de M.

Donc le spectre de R est vide et ne contient *a fortiori* pas 0, donc R est inversible.

Conclusions A_p est un corps.

• Cas $\bar{3}$ est un carré.

On a $\bar{3} = a^2$ et χ_M se factorise en $((X - \bar{2}) - a)((X - \bar{2}) + a)$, donc par Le théorème de Cayley-Hamilton

$$((M - \bar{2}I) - aI)((M - \bar{2}) + aI) = O_2$$

Ainsi $((M - \bar{2}I) - aI)$, élément de A_p, non nul par liberté de (I, M), est-il non inversibe.

Conclusion : A_p est un corps si et seulement si $\bar{3}$ n'est pas un carré.

2. La factorisation de χ_M vue dans la question précédente, $((X - \bar{2}) - a)((X - \bar{2}) + a)$, assure que M possède deux valeurs propres distinctes, $\bar{2} + a$ et $\bar{2} - a$ en effet la différence entre ces deux éléments de $\mathbf{Z}_p$ est $\bar{4}$,donc non nulle puisque p, distinct de 2, ne divise pas 4 . Donc M est diagonalisable dans $2\mathbf{Z}_p$, plus précisément, on dispose d'un élément P de $2\mathbf{Z}_p$ tel que : $PMP^{-1} = \mathrm{diag}(\bar{2} + a, \bar{2} - a)$

Pour tout λ et tout μ élément de $\mathbf{Z}_p$, on a

$$P(\lambda M + \mu I)P^{-1} = \mathrm{diag}(\lambda(\bar{2} + a) + \mu, \lambda(\bar{2} - a) + \mu)$$

On dispose donc de l'application de $\Phi \ : \ A_p \to D_2(\mathbf{Z}_p)\,;\ M \mapsto PMP^{-1}$, où $D_2(\mathbf{Z}_p)$ est l'ensemble des éléments de $\mathcal{M}_2(\mathbf{Z}_p)$ diagonaux. Cette application est linéaire et son noyau est trivialement... trivial ! donc, par égalité des dimensions de A_p et $D_2(\mathbf{Z}_p)$, c'est un isomorphisme d'espace vectoriels, mais aussi d'anneaux puisque en plus $\Phi(I) = I$ et pour tout $(M, M') \in A_p^2$, on a $\Phi(MM') = PMM'P^{-1} = PM'P^{-1}PM'P^{-1} = \Phi(M)\Phi(M')$. Comme par ailleurs $D_2(\mathbf{Z}_p)$ s'identifie à l'anneau $\mathbf{Z}_p \times \mathbf{Z}_p$, en identifiant une matrice daigonale et le couple de ses termes diagonaux, l'anneau A_p est isomorphe à l'anneau produit $\mathbf{Z}_p \times \mathbf{Z}_p$.

Un élément R de A_p est de déterminant 1 si et seulement son image par l'isomorphisme précédent est de la forme (a, b) avec a inversible et $b = a^{-1}$. Donc l'ensemble $S_2(\mathbf{Z}_p)$ des éléments de A_p de déterminant 1 à le même cardinal que $\{(a, a^{-1}), a \in \mathbf{Z}_p^*\}$. Donc comme $|\mathbf{Z}_p^*| = p - 1$, on a $\boxed{|S_2(\mathbf{Z}_p)| = p - 1}$.

D'autre part il y a autant d'inversible dans A_p que dans $\mathbf{Z}_p \times \mathbf{Z}_p$ c'est à dire $(p-1)^2$, puisque un élément de $\mathbf{Z}_p \times \mathbf{Z}_p$ est inversible si et seulement si ses deux composantes le sont.

3. Dans cette question, on suppose que $\bar{3}$ n'est pas un carré dans $\mathbf{Z}_p$.

   (a) On a vu en II.1. que tout élément non nul de A_p est inversible donc de déterminant non nul, par ailleurs par la propriété morphique du déterminant, Δ réalise un homomorphisme du groupe multiplicatif des éléments non nuls de A_p dans celui des éléments non nuls de $\mathbf{Z}_p$.

   • L'image de Δ (considéré comme une application de A_p^* dans $\mathbf{Z}_p^*$, le texte est maladroit) est un sous groupe du groupe $(\mathbf{Z}_p^*, \times)$ donc son cardinal divise $p - 1$, cardinal de $\mathbf{Z}_p^*$.

   • Nous avons pour la suite besoin de la formule :

$$|\ker(\Delta)|\,|\mathrm{im}(\Delta)| = |\mathrm{A}_\mathrm{p}^*|.$$

Preuve[2].

Deux éléments R et R' de A_p^* ont même image par Δ si et seulement si $R'R^{-1} \in \ker(\Delta)$. Donc la relation $\mathcal{R}$ sur A_p^* avoir même image par Δ est une relation d'équivalence, car $\ker(\Delta)$ est un groupe. De plus la classe d'équivalence d'un élément R_0 est $\ker(\Delta)R_0$, ensemble de cardinal $|\ker(\Delta)|$.

Le nombre de classes d'équivalence est le nombre d'images d'éléments de A_p^* par Δ, autant dire le cardinal de $\mathrm{im}(\Delta)$. Donc, comme les classes d'équivalence de la relation $\mathcal{R}$ forme une partition de A_p^*, on a :

$$|A_p^*| = |\mathrm{im}(\Delta)||\ker(\Delta)|$$

Donc par le premier point et la formule,

$|\ \mathrm{im}(\Delta)||\ker(\Delta)| = |A_p^*| = (p+1)(p-1) = q|(p+1)\mathrm{im}(\Delta)|o\mathrm{q}\in \mathbf{N}$.

Donc $\underline{|\ker(\Delta)| \text{ divise } (p+1).}$

(b) • Soient $\lambda \in \mathbf{Z}_p$

Pour tout élément μ de $\mathbf{Z}_p$, $\Delta(\lambda M + \mu I) = 1$ si et seulement si μ est solution de

$$x^2 + 4x\mu + \mu^2 = 1.$$

Cette équation polynomiale x, de degré 2 , admet au plus deux racines dans le l'anneau *intègre* Z_p.

• Comme λ est élément d'un ensemble à p éléments, il y a donc au plus $2p$ éléments de déterminant 1 dans A_p. Donc $|\mathrm{Ker}(\Delta)|$ est inférieur ou égal à $2p$ et est aussi — on l'a vu en a. — un multiple (non nul) de $p+1$, on peut conclure que A_p admet $\underline{(p+1) \text{ éléments}}$ de déterminant 1.

4. Le raisonnement du II.1. a montré que tout élément de déterminant 1 de A_p est inversible dans A_p . Il est alors immédiat que l'ensemble $S_2(\mathbf{Z}_p)$ des éléments de déterminant 1 de A_p est un sous-groupe de A_p^* et est donc un groupe multiplicatif. Comme $M \in S_2(\mathbf{Z}_p)$, son ordre divise celui de $S_2(\mathbf{Z}_p)$, c'est-à-dire $p-1$ ou $p+1$ selon que 3 est un carré dans $\mathbf{Z}_p$(question II2.) ou ne l'est pas (question II3.), mais si p divise Y_{k-2} alors l'ordre de M n'est autre que 2^k, par I.5. $\underline{\text{D'où le résultat.}}$

.

2. Cette preuve a été donnée dans la démonstration du théorème de Lagrange général