Corrigé de l'examen final du 25 mai 2022

Exercice 1 Une forme quadratique

1. La forme quadratique associée à la matrice A est :

$$q(x,y,z) = 2xy + 4xz + 2yz \ .$$

Par la méthode de Gauss, on trouve :

$$q = 2(x+z)(y+2z) - 4z^2$$

$$= 2\frac{(x+z+y+2z)^2}{4} - 2\frac{(x+z-y-2z)^2}{4} - 4z^2$$

$$= \frac{1}{2}(x+y+3z)^2 - \frac{1}{2}(x-y-z)^2 - 4z^2$$

donc q a pour signature $(1,2)$.

2. On cherche la base anteduale des formes linéaires :

$$l_1 = x+y+3z,\ l_2 = x-y-z,\ l_3 = z \ .$$

Cela revient à calculer :

$$\begin{pmatrix} 1 & 1 & 3 \\ 1 & -1 & -1 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -1 \\ \frac{1}{2} & -\frac{1}{2} & -2 \\ 0 & 0 & 1 \end{pmatrix} \ .$$

Donc si on pose v_1, v_2, v_3 les vecteurs colonnes de la matrice trouvée, on a :

$$q(t_1v_1 + t_2v_2 + t_3v_3) = \frac{1}{2}t_1^2 - \frac{1}{2}t_2^2 - 4t_3^2 \ .$$

D'où

$${}^t\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -1 \\ \frac{1}{2} & -\frac{1}{2} & -2 \\ 0 & 0 & 1 \end{pmatrix} A \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -1 \\ \frac{1}{2} & -\frac{1}{2} & -2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ 0 & -\frac{1}{2} & 0 \\ 0 & 0 & -4 \end{pmatrix}$$

on en déduit : ${}^tPAP = D$ où :

$$P = \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} & -\frac{1}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} & -1 \\ 0 & 0 & \frac{1}{2} \end{pmatrix}, D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \ .$$

Exercice 2 Géométrie affine

(I) 1. Soit G le groupe affine de $\mathscr{E}$ *c-à-d* le groupe des appilcations affines bijectives. Soit f une application affine telle que $\overrightarrow{f} = \pm Id_E$, alors f est bijective et sa réciproque est affine avec

$$\overrightarrow{f^{-1}} = \overrightarrow{f}^{-1} = \pm Id_E \ .$$

L'application

$$G \to \mathrm{GL}(E),\ f \mapsto \overrightarrow{f}$$

est un morphisme de groupes. Comme $\{\pm Id_E\}$ est un sous-groupe de $\mathrm{GL}(E)$, Γ est un sous-groupe de G comme image réciproque d'un sous-groupe par un morphisme de groupes. Il est clair que les translations et les symétries sont dans Γ. Réciproquement, si $\overrightarrow{f} = Id_E$, alors f est une translation ou l'identité et si $\overrightarrow{f} = -Id_E$, on a pour tout $M \in \mathscr{E}$ (et un point quelconque O de $\mathscr{E}$) :

$$\begin{aligned} f(f(M)) &= f(O) + \overrightarrow{f}(\overrightarrow{Of(M)}) = f(O) - \overrightarrow{Of(M)} \\ &= f(O) - \overrightarrow{Of(O)} - \overrightarrow{f(O)f(M)} \\ &= O - \overrightarrow{f}(OM) = O + \overrightarrow{OM} = M \end{aligned}$$

donc $f \circ f = \mathrm{Id}_{\mathscr{E}}$.

2. On a $\overrightarrow{g \circ f} = -(-\mathrm{Id}_E)) = \mathrm{Id}_E$ donc $g \circ f$ est une translation.
De plus

$$\begin{aligned} {}^{\forall} M \in \mathscr{E},\ g \circ f(M) &= g(A - \overrightarrow{AM}) = g(A) + \overrightarrow{AM} \\ &= g(B + \overrightarrow{BA}) + \overrightarrow{AM} \\ &= B - \overrightarrow{BA} + \overrightarrow{AM} = M + \overrightarrow{MB} - \overrightarrow{BA} + \overrightarrow{AM} \\ &= M + \overrightarrow{AB} - \overrightarrow{BA} = M + 2\overrightarrow{AB} \ . \end{aligned}$$

Donc $g \circ f$ est la translation de vecteur $2\overrightarrow{AB}$.

3. On a $\overrightarrow{st} = \overrightarrow{s}\,\overrightarrow{t} = -\mathrm{Id}_E$ donc $st \in \Gamma$ n'est pas une translation et c'est une symétrie centrale.
Cherchons le centre :

$$\begin{aligned} st(M) = M &\Leftrightarrow s(M + \vec{u}) = M \Leftrightarrow I - \overrightarrow{IM} - \vec{u} = M \\ &\Leftrightarrow I - \overrightarrow{IM} - \vec{u} = I + \overrightarrow{IM} \\ &\Leftrightarrow 2\overrightarrow{IM} = -\vec{u} \\ &\Leftrightarrow M = I - \frac{1}{2}\vec{u} \end{aligned}$$

c'est le centre de st.
De même ts est une symétrie de centre $I + \frac{1}{2}\vec{u}$.
Donc $st = ts \Leftrightarrow I - \frac{1}{2}\vec{u} = I + \frac{1}{2}\vec{u} \Leftrightarrow \vec{u} = 0 \Leftrightarrow t = \mathrm{Id}_E$.

(II) 1. Pour tout i, $s_i(M_i) = M_{i+1}$. Donc :

$$\begin{aligned} s_{i-1}s_{i-2}...s_1(M_1) &= s_{i-1}s_{i-2}...s_2(M_2) \\ &= ... = s_{i-1}(M_{i-1}) = M_i \ . \end{aligned}$$

2. Si le problème est résolu, alors

$$s_n...s_1(M_1) = s_n(M_n) = M_1$$

donc il y a un point fixe. Réciproquement, si M_1 est un point fixe de $s_n...s_1$, on pose

$$^\forall 1 \leq i \leq n-1,\ M_{i+1} = s_i(M_i)$$

ce qui définit par récurrence les points $M_1, ..., M_n$ qui conviennent.

3. Si n est impair, $\overrightarrow{s_n...s_1} = (-1)^n \mathrm{Id}_E = -\mathrm{Id}_E$ donc $s_n...s_1$ est une symétrie et a un seul point fixe.

4. Si n est pair, alors $\overrightarrow{s_n...s_1} = (-1)^n \mathrm{Id}_E = \mathrm{Id}_E$ donc $s_n...s_1$ est une translation. Donc il y a un point fixe si et seulement si $s_n...s_1 = \mathrm{Id}_{\mathscr{E}}$. Dans ce cas, tous les points de $\mathscr{E}$ sont des points fixes. Cela fait une infinité de solutions.

5. On a :

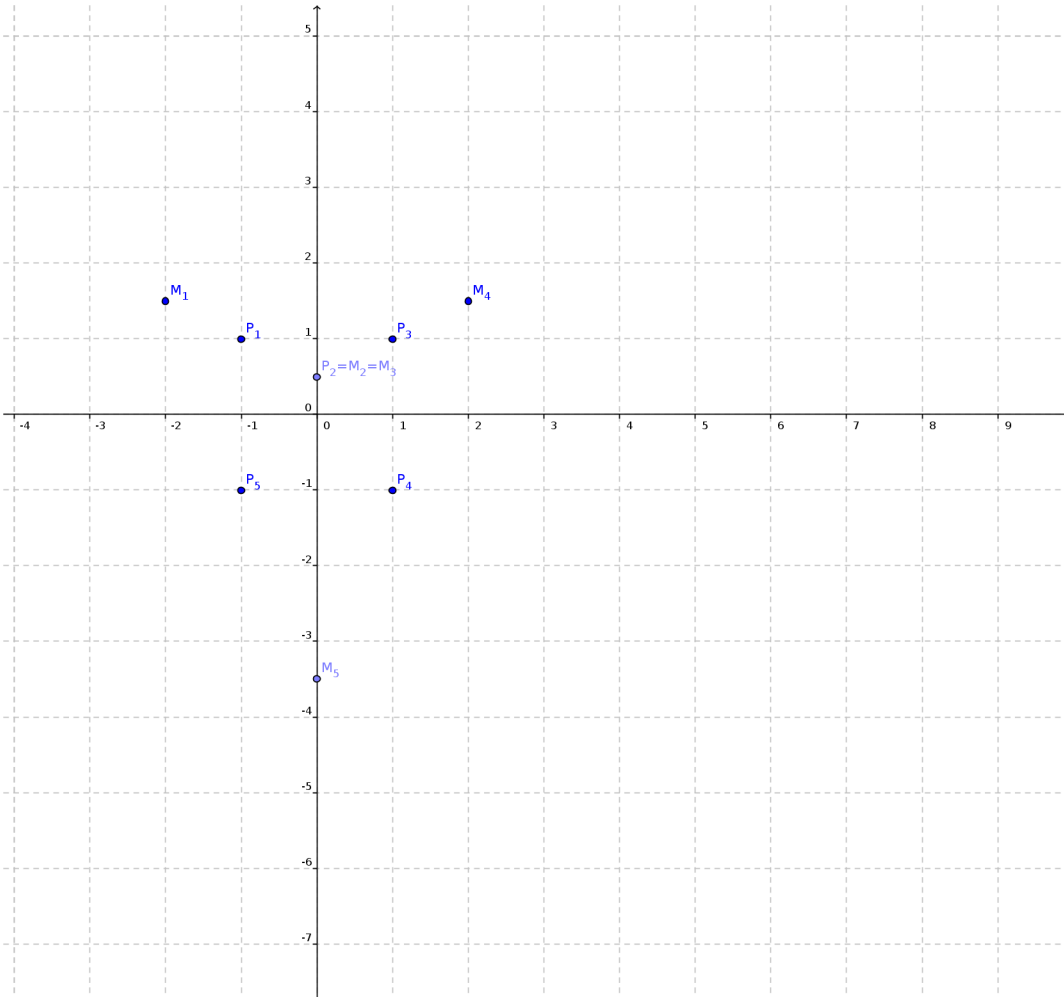
$$s_5 s_4 s_3 s_2 s_1 = t_{2\overrightarrow{P_4P_5}} t_{2\overrightarrow{P_2p_3}} s_1$$

d'après la question I.2. Donc

$$s_5 s_4 s_3 s_2 s_1 = t_u s_1$$

où $u = 2\overrightarrow{P_4P_5} + 2\overrightarrow{P_2P_3}$. Donc $s_5 s_4 s_3 s_2 s_1$ est la symétrie de centre $P_1 + \frac{1}{2}u = (-2, \frac{3}{2})$. On en déduit les points M_i par récurrence :

$$M_1 = (-2, \frac{3}{2}),\ ^\forall 1 \leq i \leq 4,\ M_{i+1} = s_{P_i}(M_i)\ .$$



6. Soient $P_1, P_2, P_3, P_4 \in \mathscr{E}$. D'après ce qui précède, si P_1, P_2, P_3, P_4 sont les milieux de $[M_1M_2], [M_2M_3], [M_3M_4], [M_4M_1]$, alors $s_4s_3s_2s_1 = \mathrm{Id}_{\mathscr{E}}$ où s_i est la symétrie de centre P_i et donc

$$s_4s_3 = (s_2s_1)^{-1} = s_1s_2$$
$$\Rightarrow t_{2\overrightarrow{P_3P_4}} = t_{2\overrightarrow{P_2P_1}}$$
$$\Rightarrow \overrightarrow{P_3P_4} = \overrightarrow{P_2P_1}$$
$$\Rightarrow P_1P_2P_3P_4 \text{ parallélogramme.}$$

Réciproquement si $N_1N_2N_3N_4$ est un parallélogramme, alors $\overrightarrow{N_1N_2} = \overrightarrow{N_4N_3}$ donc si on note s_i la symétrie de centre N_i on a :

$$s_4s_3s_2s_1 = t_{2\overrightarrow{N_3N_4}}t_{2\overrightarrow{N_1N_2}} = t_{2\overrightarrow{N_3N_4}+2\overrightarrow{N_1N_2}} = \mathrm{Id}_{\mathscr{E}}$$

donc d'après la question II.2. il existe M_1, M_2, M_3, M_4 tels que P_i est le milieu de $[M_iM_{i+1}]$ pour $1 \leq i \leq 4$ (avec $M_5 = M_4$).

Exercice 3 Polynômes irréductibles

1. Le polynôme $P = X^3 - 3X + 1$ est unitaire à coefficients entiers. S'il a une racine $x \in \mathbb{Q}$, alors $x \in \mathbb{Z}$ et alors $x|1 \Rightarrow x = \pm 1$; Or ± 1 ne sont pas racines de P.
   donc P n'a pas de racine dans $\mathbb{Q}$. Comme $\deg P = 3$, P est irréductible sur $\mathbb{Q}$.
2. Soit $x = \frac{2\pi}{9}$. On a :
$$\cos 3x = \cos\frac{2\pi}{3} = -\frac{1}{2} = 4\cos^3 x - 3\cos x$$
$$\Rightarrow 8\cos^3 x - 6\cos x + 1 = 0$$
$$\Rightarrow y^3 - 3y + 1 = 0$$
   où $y = 2\cos x$.
   Donc $2\cos\frac{2\pi}{9}$ est racine de P.
3. On a :
$$\mathbb{Q}(\cos\frac{2\pi}{9}) = \mathbb{Q}(2\cos\frac{2\pi}{9})$$
   or, P est le polynôme minimal de $2\cos\frac{2\pi}{9}$ sur $\mathbb{Q}$ car P est irréductible sur $\mathbb{Q}$ et l'annule. Donc
$$\dim_{\mathbb{Q}} \mathbb{Q}(\cos\frac{2\pi}{9}) = \deg P = 3 \ .$$

Exercice 4 Idéaux maximaux de $\mathbb{C}[X_1, ..., X_n]$

1. Soit $N \in \mathbb{N}$ et soient $z_i \in \mathbb{C}$, $1 \leq i \leq N$ des nombres complexes distincts. Si
$$\sum_{i=1}^{N} \lambda_i \frac{1}{X - z_i} = 0$$
   dans $\mathbb{C}(X)$, alors par unicité de la décomposition en éléments simples, on a $^\forall i$, $\lambda_i = 0$.
   Donc les éléements $\frac{1}{X-z}$, $z \in \mathbb{C}$ sont $\mathbb{C}-$linéairement indépendants.
2. Le morphisme $\mathbb{C}[X_1, ..., X_n] \to \mathbb{C}$, $P \mapsto P(a_1, ..., a_n)$ est surjectif de noyau $m = (X_1 - a_1, ..., X_n - a_n)$ (car si $P = P(a_1, ..., a_n) \bmod (X_1 - a_1, ..., X_n - a_n)$). Donc le quotient
$$\mathbb{C}[X_1, .., X_n]/m \simeq \mathbb{C}$$
   est un corps donc m est maximal.
3. Soit $\mathbb{C}[X_1, ..., X_n]_k$ le sous-espace des polynômes de degré total $\leq k$. C'est un sous-espace de dimension finie $(= \binom{n+k+1}{n})$. On a $\mathbb{C}[X_1, ..., X_n] = \cup_{k\in\mathbb{N}} \mathbb{C}[X_1, ..., X_n]_k$.
4. Soit $\pi : \mathbb{C}[X_1, ..., X_n] \to \mathbb{C}[X_1, ..., X_n]/I$ la surjection canonique. On a
$$\mathbb{C}[X_1, ..., X_n]/I = \cup_{k\in\mathbb{N}} \pi(\mathbb{C}[X_1, ..., X_n]_k)$$
   et chaque $\pi(\mathbb{C}[X_1, ..., X_n]_k)$ est de dimension finie sur $\mathbb{C}$.
5.

6. Le quotient $\mathbb{C}[X_1, ..., X_n]/M$ est un corps. donc le morphisme ϕ_i s'étend en posant

$$^\forall P \in \mathbb{C}[X_i], \, ^\forall 0 \neq Q \in \mathbb{C}[X_i], \, \widetilde{\phi_i}(\frac{P}{Q}) := \phi_i(P)\phi_i(Q)^{-1}$$

(ce qui est possible car $0 \neq Q \Rightarrow \phi_i(Q) \neq 0$). C'est bien défini car si $P, Q, R, S \in \mathbb{C}[X_i]$, si $Q, S \neq 0$, alors

$$\frac{P}{Q} = \frac{R}{S} \Leftrightarrow PS = QR \Rightarrow \phi_i(PS) = \phi_i(QR) \Rightarrow \phi_i(P)\phi_i(S) = \phi_i(Q)\phi_i(R)$$

$$\Rightarrow \phi_i(P)\phi_i(Q)^{-1} = \phi_i(R)\phi_i(S)^{-1} \ .$$

L'application $\widetilde{\phi_i} : \mathbb{C}(X_i) \to \mathbb{C}[X_1, ..., X_n]/M$ est un morphisme de corps donc injectif.

7. C'est une contradiction car $\mathbb{C}(X_i)$ est de dimension non dénombrable (la famille $\frac{1}{X_i - z}$, $z \in \mathbb{C}$ est une famille libre de même cardinal que $\mathbb{C}$) et $\mathbb{C}[X_1, ..., X_n]/M$ est de dimension au plus dénombrable comme réunion dénombrable de sous-espaces de dimensions finies.
8. On a $\mathbb{C}[X_i]/(P_i)$ qui est isomorphe à un sous-anneau du corps $\mathbb{C}[X_1, ..., X_n]/M$. Donc c'est intègre. Donc l'idéal (P_i) est premier donc P_i est irréductible sur $\mathbb{C}$. Donc $\deg P_i = 1$ car les polynômes irréductibles sur $\mathbb{C}$ sont de degré 1.
9. Si $P_i = X_i - z_i$, alors $^\forall i$, $X_i - z_i \in M$ donc :

$$(X_1 - z_1, ..., X_n - z_n) \leq M$$

or l'idéal

$$(X_1 - z_1, ..., X_n - z_n)$$

est maximal donc $(X_1 - z_1, ..., X_n - z_n) = M$.

Exercice 5 Un anneau

1. L'ensemble $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ est un sous-anneau de $\mathbb{R}$. En effet il suffit de vérifier que c'est stable par produit. C'est le cas car :

$$^\forall a, b, c, d \in \mathbb{Z}, \, (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \ .$$

2. On a $\frac{1}{1+\sqrt{2}} = \sqrt{2} - 1 \in A$ donc $1 + \sqrt{2}$ est inversible dans A.
3. Soient $a, b, c, d \in \mathbb{Z}$. On a

$$N(a + b\sqrt{2})N(c + d\sqrt{2}) = (a^2 - 2b^2)(c^2 - 2d^2)$$

$$a^2c^2 + 4b^2d^2 - 2b^2c^2 - 2a^2d^2 \ .$$

D'un autre côté :

$$N((a + b\sqrt{2})(c + d\sqrt{2})) = N((ac + 2bd) + (bc + ad)\sqrt{2})$$

$$= (ac + 2bd)^2 - 2(bc + ad)^2$$

$$= a^2c^2 + 4b^2d^2 + 4abcd - 2b^2c^2 - 2a^2d^2 - 4abcd$$

$$= a^2c^2 + 4b^2d^2 - 2b^2c^2 - 2a^2d^2$$

$$= N(a + b\sqrt{2})N(c + d\sqrt{2}) \ .$$

Si $a + b\sqrt{2} \in A^\times$, alors il existe $z \in A$ tel que $az = 1$. Mais alors $N(az) = N(1) = 1 \Rightarrow N(a)N(z) = 1$. Comme $N(a), N(z) \in \mathbb{Z}$ sont entiers, comme les seuls entiers inversibles (dans $\mathbb{Z}$) sont ± 1, on a $N(a) = \pm 1$.

Réciproquement, si $a^2 - 2b^2 = \pm 1$, alors :

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 = \pm 1$$

donc comme $a - b\sqrt{2} \in A$, $a + b\sqrt{2}$ est inversible d'inverse $\pm(a - b\sqrt{2})$.

4. Dans $\mathbb{F}_3$, si $a^2 - 2b^2 = 0$, alors $a^2 = 2b^2$.

   Si $b \neq 0$, alors $2 = (\frac{a}{b})^2$ absurde car les seuls carrés dans $\mathbb{F}_3$ sont 0 et 1.

   Donc $b = 0$. donc $a^2 = 0 \Rightarrow a = 0$. La réciproque est évidente.

   Le quotient $A/(3)$ est un corps car tous ses éléments non nuls sont inversibles. En effet, si $a + b\sqrt{2} \neq 0 \bmod 3$, alors $a \neq 0 \bmod 3$ ou $b \neq 0 \bmod 3$. Donc $a^2 - 2b^2 \neq 0 \bmod 3$. Donc $a^2 - 2b^2 = \pm 1 \bmod 3$. Donc $a^2 - 2b^2$ est inversible dans $A/3$. Comme

   $$a^2 - 2b^2 = (a + b\sqrt{2})(a - b\sqrt{2})$$

   $a + b\sqrt{2} \bmod 3$ est aussi inversible.

   Comme $A/3 = \{x + y\sqrt{2} \ : \ x, y \in \mathbb{F}_3\}$ cela fait $3^2 = 9$ éléments distincts.

5. Le groupe $K^\times$ est de cardinal 8. Il suffit donc de démontrer que $1 + \sqrt{2}$ est d'ordre 8.

   Or,

   $$(1 + \sqrt{2})^2 = 2\sqrt{2} \bmod 3 \neq 1 \bmod 3$$

   $$(1 + \sqrt{2})^4 = 8 = -1 \bmod 3 \neq 1 \bmod 3$$

   $$(1 + \sqrt{2})^8 = 1 \bmod 3 \ .$$

   Donc $1 + \sqrt{2}$ est bien d'ordre 8 dans $K^\times$.

6. On a :

   $$\mathbb{Z}[X]/(3, X^2 - 2) \simeq \mathbb{F}_3[X]/(X^2 - 2)$$

   c'est un corps car $X^2 - 2$ n'a pas de racine dans $\mathbb{F}_3$ donc est irréductible sur $\mathbb{F}_3$.

   Donc l'idéal $(3, X^2 - 2)$ est maximal dans $\mathbb{Z}[X]$.

   S'il était principal, on pourrait trouver $P \in \mathbb{Z}[X]$ tel que

   $$(P) = (3, X^2 - 2)$$

   mais alors on aurait $3 \in (P) \Rightarrow P|3 \Rightarrow P$ constant.

   Comme $P|X^2-2$ on a forcément $P = \pm 1$. On aurait donc $1 \in (3, X^2-2) \Rightarrow (3, X^2-2) = (1)$. Absurde car l'idéal $(3, X^2-2)$ est maximal (donc propre). Donc l'idéal n'est pas principal !

7. Les polynômes unitaires irréductibles de degré 2 sont ceux dont le discriminant n'st pas un carré dans $\mathbb{F}_3$ *c-à-d* dont le discriminant est -1.
   On trouve donc
   $$X^2+1,\ X^2+X-1,\ X^2-X-1\ .$$
   On a
   $$X^9-X=X(X-1)(X+1)(X^2+1)(X^2+X-1)(X^2-X-1)\ .$$
   (En effet, si Q est irréductible de degré 2 sur $\mathbb{F}_3$, alors le corps $\mathbb{F}_3[X]/(Q)$ est de cardinal 9 donc $X^9=X \bmod Q$ *c-à-d* $Q|X^9-X$ dans $\mathbb{F}_3[X]$).
8. Comme K est de cardinal 9, on a :
   $$^\forall x\in K^\times,\ x^8=1$$
   car $K^\times$ est un groupe d'ordre 8. On en déduit :
   $$^\forall x\in K,\ x^9=x\ .$$
   Donc le polynôme X^9-X vérifie :
   $$X^9-X=\prod_{x\in K}(X-x)\ .$$
   Comme $P|X^9-X$ sur $\mathbb{F}_3$, on a P qui est scindé aussi sur K. Soit $x\in K$ une racine de P.
   Le morphisme $\mathbb{F}_3[X]\to K$, $X\mapsto x$ est un morphisme d'anneaux dont le noyau contient (P). Comme P est irréductible, l'idéal (P) est maximal dans $\mathbb{F}_3[X]$ donc le noyau est soit (P) soit (1). Ce n'est pas (1). Donc c'est (P) et on obtient un morphisme injectif
   $$\psi\ :\ \mathbb{F}_3[X]/(P)\to K\ .$$
   Or $\mathbb{F}_3[X]/(P)$ est de cardinal 9 car c'est un $\mathbb{F}_3-$espace vectoriel de dimension 2. Donc le morphisme ψ est un isomorphisme d'anneaux (*i.e.* de corps).