Exercice 2 feuille 3

Les racines de $P(X) = X^4 - X - 1$.

a) Dans $\mathbb{F}_2[X]$, $P(X) = X^4 + X + 1$ est irréductible car n'a pas de racines et n'est pas divisible par $X^2 + X + 1$, seul polynôme irréductible de degré 2 sur $\mathbb{F}_2$.

b) Le polynôme P est premier avec sa dérivée P' (car le pgcd divise P est de degré $\leqslant 3$ donc c'est constant !). Donc P, P' n'ont pas de racine commune donc les racines x_1, x_2, x_3, x_4 de P sont simples (donc distinctes).

c) On a $P(X) = X^4 - X - 1 = (X - x_1)(X - x_2)(X - x_3)(X - x_4)$.

Donc $x_1 + x_2 + x_3 + x_4 = 0$ (=- le coefficient devant X^3) ;

$x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = 0$ (le coefficient devant X^2) ;

$x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = 1$ (=- le coefficient devant X) ;

$x_1x_2x_3x_4 = -1$ (le coefficient constant).

On a :

$$\begin{cases} x_1 + x_2 = z_1 \\ x_1 + x_3 = z_2 \\ x_1 + x_4 = z_3 \\ x_1 + x_2 + x_3 + x_4 = 0 \end{cases}$$

$$\Rightarrow \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1100 \\ 1010 \\ 1001 \\ 1111 \end{pmatrix}^{-1} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ 0 \end{pmatrix} \Rightarrow \begin{cases} x_1 = \frac{z_1 + z_2 + z_3}{2} \\ x_2 = \frac{z_1 - z_2 - z_3}{2} \\ x_3 = \frac{-z_1 + z_2 - z_3}{2} \\ x_4 = \frac{-z_1 - z_2 + z_3}{2} \end{cases}$$

En particulier, $\mathbb{Q}(z_1, z_2, z_3) = \mathbb{Q}(x_1, x_2, x_3, x_4)$.

d) Posons $Q(X) = (X - z_1^2)(X - z_2^2)(X - z_3^2) = X^3 - (z_1^2 + z_2^2 + z_3^2)X^2 + (z_1^2z_2^2 + z_1^2z_3^2 + z_2^2z_3^2)X + z_1^2z_2^2z_3^2$.

Or, on a :

$$z_1^2 + z_2^2 + z_3^2 = -(x_1 + x_2)\Big(\underbrace{x_3 + x_4}_{=-(x_1+x_2)}\Big) - (x_1 + x_3)(x_2 + x_4) - (x_1 + x_4)(x_2 + x_3)$$

$$= -(x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4) = 0.$$

$$z_1^2z_2^2 + z_1^2z_3^2 + z_2^2z_3^2 = (x_1 + x_2)^2(x_1 + x_3)^2 + (x_1 + x_2)^2(x_1 + x_4)^2 + (x_1 + x_3)^2(x_1 + x_4)^2$$

$$= (x_1^2 + x_1x_3 + x_1x_2 + x_2x_3)^2 + (x_1^2 + x_1x_4 + x_1x_2 + x_2x_4)^2 + (x_1^2 + x_1x_3 + x_1x_4 + x_3x_4)^2$$

$$= \Big(x_1\underbrace{(x_1 + x_2 + x_3)}_{-x_4} + x_2x_3\Big)^2 + (x_1(x_1 + x_2 + x_4) + x_2x_4)^2 + (x_1(x_1 + x_3 + x_4) + x_3x_4)^2$$

$$= (-x_1x_4 + x_2x_3)^2 + (-x_1x_3 + x_2x_4)^2 + (-x_1x_2 + x_3x_4)^2$$

$=(x_1x_2)^2+(x_1x_3)^2+(x_1x_4)^2+(x_2x_3)^2+(x_2x_4)^2+(x_3x_4)^2-6x_1x_2x_3x_4.$

Or, $x_1x_2x_3x_4=-1$ et :

$(x_1x_2)^2+(x_1x_3)^2+(x_1x_4)^2+(x_2x_3)^2+(x_2x_4)^2+(x_3x_4)^2$

$=\Big(\underbrace{x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4}_{0}\Big)^2-2x_1^2x_2x_3-2x_1^2x_2x_4-2x_1x_2^2x_3-2x_1x_2^2x_4-2x_1x_2x_3x_4-2x_1^2x_3x_4-2x_1x_2x_3^2-2x_1x_2x_3x_4-2x_1x_3^2x_4-2x_1x_2x_3x_4-2x_1x_2x_4^2-2x_1x_3x_4^2-2x_2^2x_3x_4-2x_2x_3^2x_4-2x_2x_3x_4^2$

$=-6x_1x_2x_3x_4-2x_1x_2x_3\Big(\underbrace{x_1+x_2+x_3}_{-x_4}\Big)-2x_1x_2x_4(x_1+x_2+x_4)-2x_1x_3x_4(x_1+x_3+x_4)-2x_2x_3x_4(x_2+x_3+x_4)$

$=6+8x_1x_2x_3x_4=-2.$

Donc $z_1^2z_2^2+z_1^2z_3^2+z_2^2z_3^2=-2+6=4.$

On a aussi :

$z_1z_2z_3=(x_{1+}x_2)(x_1+x_3)(x_1+x_4)=(x_1^3+x_1^2x_4+x_1^2x_3+x_1x_3x_4+x_1^2x_2+x_1x_2x_4+x_1x_2x_3+x_2x_3x_4)$

$=(x_1^3+x_1^2x_4+x_1^2x_3+x_1^2x_2+1)$

$=\Big(x_1^3+x_1\Big(\underbrace{x_1x_4+x_1x_3+x_1x_2}_{-x_2x_3-x_2x_4-x_3x_4}\Big)+1\Big)=(x_1^3+1-x_1x_2x_3-x_1x_2x_4-x_1x_3x_4-x_2x_3x_4+x_2x_3x_4)$

$=(x_1^3+x_2x_3x_4)=\Big(x_1^3-\frac{1}{x_1}\Big)=1$ car $x_1^4-x_1-1=0.$

Donc $Q(X)=X^3+4X-1.$

On a donc $(z_1^2-z_2^2)^2(z_1^2-z_3^2)^2(z_2^2-z_3^2)^2=\Delta_Q=-4.(4^3)-27.(1)^2=-283<0.$

Donc $\mathbb{Q}(z_1^2,z_2^2,z_3^2)$ contient une racine carrée de -283 donc un élément de degré 2 sur $\mathbb{Q}$.

Comme $Q(X)$ est irréductible sur $\mathbb{Q}$ (comme ±1 ne sont pas racines),

$[\mathbb{Q}(z_1^2,z_2^2,z_3^2):\mathbb{Q}]$ est divisible par 3.

Donc $6|[\mathbb{Q}(z_1^2,z_2^2,z_3^2):\mathbb{Q}]$. Comme forcément c'est $\leqslant 6$, $[\mathbb{Q}(z_1^2,z_2^2,z_3^2):\mathbb{Q}]=6.$

e) Comme x_1 est de degré 4 sur $\mathbb{Q}$ et comme $4\nmid 6$, $x_1\notin\mathbb{Q}(z_1^2,z_2^2,z_3^2)$.

Or, $\mathbb{Q}(x_1,x_2,x_3,x_4)\geqslant\mathbb{Q}(z_1^2,z_2^2,z_3^2)$ et $\mathbb{Q}(x_1,x_2,x_3,x_4)\geqslant\mathbb{Q}(x_1)$

donc 6 et 4 divisent $[\mathbb{Q}(x_1,x_2,x_3,x_4):\mathbb{Q}]\Rightarrow 12|[\mathbb{Q}(x_1,x_2,x_3,x_4):\mathbb{Q}]$.

Or $[\mathbb{Q}(x_1,x_2,x_3,x_4):\mathbb{Q}]\leqslant|\mathfrak{S}_4|=24.$

Donc $[\mathbb{Q}(x_1,x_2,x_3,x_4):\mathbb{Q}]=24$ ou 12.

f) Soit $G=\mathrm{Aut}(\mathbb{Q}(x_1,x_2,x_3,x_4))$.

Le groupe G s'identifie à un sous-groupe de $\mathfrak{S}_4$ d'ordre $[\mathbb{Q}(x_1,x_2,x_3,x_4):\mathbb{Q}]=24$ ou 12.

Donc $G\cong\mathfrak{S}_4$ ou $\mathfrak{A}_4$ le groupe alterné.

Or $G\to\mathrm{Aut}(\mathbb{Q}(\sqrt{-283}))\cong\mathbb{Z}/2\mathbb{Z}$ est surjectif. Donc G contient un sous-groupe (le noyau) d'indice 2. Ce n'est pas le cas de $\mathfrak{A}_4$ donc $G\cong\mathfrak{S}_4$ et $[\mathbb{Q}(x_1,x_2,x_3,x_4):\mathbb{Q}]=24.$

g) On a $Q(X)=X^3+4X-1=(X-z_1^2)(X-z_2^2)(X-z_3^2).$

Donc z_1^2, z_2^2, z_3^2 sont les racines de X^3+4X-1.

On cherche les racines de X^3+4X-1.

$(u+v)^3+4(u+v)-1=0 \Leftrightarrow u^3+v^3-1+(3uv+4)(u+v)=0$

$\Leftarrow \begin{cases} u^3+v^3=1 \\ uv=-\frac{4}{3} \end{cases} \Leftarrow u^3, v^3 = \frac{1 \pm \sqrt{\frac{283}{27}}}{2}$

Donc $z_1^2, z_2^2, z_3^2 = \sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + \sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}},\ j\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j^2\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}},\ j^2\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}$.

Quitte à renuméroter les x_i, on peut supposer que :

$$z_1^2 = \sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + \sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}},$$

$$z_2^2 = j\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j^2\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}},$$

$$z_3^2 = j^2\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}.$$

Choisissons des racines carrées dont le produit vaut 1 :

$$a_1 = \sqrt{\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + \sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}}, \qquad a_2 = \sqrt{j\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j^2\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}},$$

$$a_3 = \sqrt{j^2\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}}.$$

Comme $z_1z_2z_3=1$, on a $(z_1, z_2, z_3) = (a_1, a_2, a_3), (-a_1, -a_2, a_3), (-a_1, a_2, -a_3)$ ou $(a_1, -a_2, -a_3)$.

Cela fait une seule possibilité pour l'ensemble $\{x_1, x_2, x_3, x_4\}$:

$\{\frac{a_1+a_2+a_3}{2}, \frac{a_1-a_2-a_3}{2}, \frac{-a_1+a_2-a_3}{2}, \frac{-a_1-a_2+a_3}{2}\}$.

Donc voici les 4 racines de X^4-X-1 (à renumérotation près):

$$x_1 = \frac{\sqrt{\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + \sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}} + \sqrt{j\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j^2\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}} + \sqrt{j^2\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}}}{2}$$

$$x_2 = \frac{\sqrt{\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + \sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}} - \sqrt{j\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j^2\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}} - \sqrt{j^2\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}}}{2}$$

$$x_3 = \frac{-\sqrt{\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + \sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}} + \sqrt{j\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j^2\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}} - \sqrt{j^2\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}}}{2}$$

$$x_4 = \frac{-\sqrt{\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + \sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}} - \sqrt{j\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j^2\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}} + \sqrt{j^2\sqrt[3]{\frac{1+\sqrt{\frac{283}{27}}}{2}} + j\sqrt[3]{\frac{1-\sqrt{\frac{283}{27}}}{2}}}}{2}$$