DM - Exercice 4

$P = X^3 - X - 1$

Q1) Montrer que P est irréductible sur $\mathbb{Q}$:

Par l'absurde : Supposons $\exists Q, R \in \mathbb{Q}[X]$, $P = QR$, et $\deg(Q), \deg(R) \geq 1$.

Alors $\deg(Q) = 1$ ou $\deg(R) = 1$.
Donc Q ou R possède une racine dans ~~$\mathbb{R}$~~ $\mathbb{Q}$:
donc P admet une racine dans $\mathbb{Q}$:

$\exists p \in \mathbb{Z}, q \in \mathbb{N}^*, p \wedge q = 1$, et $P(\frac{p}{q}) = 0$,

donc $(\frac{p}{q})^3 - \frac{p}{q} - 1 = 1$,

donc $p^3 = q(pq + q^2)$,

donc $q \mid p^3$ et $p \wedge q = 1$,

donc $q \mid p \times p^2$, où $p \wedge q = 1$,
donc d'après le lemme de Gauss, $q \mid p^2$.

Donc $q \mid p \times p$, où $p \wedge q = 1$,
donc d'après le lemme de Gauss, $q \mid p$.

Or $p \wedge q = 1$. Donc $q = 1$.

Donc $p^3 = p + 1$ et $p \times (p+1) = 1$.
De même, on obtient $(p+1) \mid p$.

Donc $p+1 = 1$ ou -1,
donc $p = -2$ ou 0.

Or, $P(-2) \neq 0$, et $P(0) \neq 0$.

Ainsi, P est irréductible sur $\mathbb{Q}$.

Q2) Soit $f \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^3 - x - 1 \end{array} \right.$

$\forall x \in \mathbb{R},\ f'(x) = (\sqrt{3}x - 1)(\sqrt{3}x + 1)$

x	$-\infty$		$\frac{-1}{\sqrt{3}}$		$\frac{1}{\sqrt{3}}$		$+\infty$
Signe de $f'(x)$		$+$	0	$-$	0	$+$	
f	$-\infty$	$\nearrow$	$f\left(\frac{-1}{\sqrt{3}}\right) < 0$ *	$\searrow$	$f\left(\frac{1}{\sqrt{3}}\right) < 0$	$\nearrow$	$+\infty$

* $f\left(\frac{-1}{\sqrt{3}}\right) = \frac{2}{3\sqrt{3}} - 1 < 0$ car $\frac{4}{27} < 1$ et

$x \mapsto x^2$ est croissante sur $\mathbb{R}^+$

$f(\frac{-1}{\sqrt{3}})$ majore f sur $]-\infty, \frac{1}{\sqrt{3}}]$.

Or, $f(\frac{-1}{\sqrt{3}}) < 0$ donc f ne s'annule pas sur cet intervalle.

Par théorème de la bijection, f induit une bijection de $[\frac{1}{\sqrt{3}}, +\infty[$ vers $[f(\frac{1}{\sqrt{3}}), \lim\limits_{x \to +\infty} f(x)[$.

On remarque que $\lim\limits_{x \to +\infty} f(x) = +\infty$, et que $0 > f(\frac{1}{\sqrt{3}})$. Donc $0 \in [f(\frac{1}{\sqrt{3}}), +\infty[$.

Ainsi, f s'annule une unique fois, sur $[\frac{1}{\sqrt{3}}; +\infty[$.

On note a, l'unique racine de P.

Q3) Donnons une $\mathbb{Q}$-base de F, où $F := \mathrm{Vect}_{\mathbb{Q}}(\{a^k : k \in \mathbb{N}\})$:

$a^3 = a + 1$, donc $a^3 \in \mathrm{Vect}_{\mathbb{Q}}(\{1; a\})$,

avec $\mathrm{Vect}_{\mathbb{Q}}(\{1; a\}) \subset \mathrm{Vect}_{\mathbb{Q}}(\{1; a; a^2\})$.

Soit $n \in \mathbb{N}$, tel que $a^n \in \mathrm{Vect}_{\mathbb{Q}}(\{1; a; a^2\})$.

$\exists\, \alpha_n, \beta_n, \gamma_n \in \mathbb{Q}$, $a^n = \alpha_n + \beta_n a + \gamma_n a^2$.

Donc $a^{n+1} = \underbrace{\alpha_n a + \beta_n a^2}_{} + \underbrace{\gamma_n a^3}_{} \in \mathrm{Vect}_{\mathbb{Q}}(\{1; a; a^2\})$

Ainsi, $F \subset \mathrm{Vect}_{\mathbb{Q}}(\{1; a; a^2\})$.
L'inclusion réciproque est claire.

Liberté de la famille :

Soit $\varphi_a \left| \begin{array}{ccc} \mathbb{Q}[X] & \longrightarrow & F \\ Q & \longmapsto & Q(a) \end{array} \right.$

un morphisme de $\mathbb{Q}$-algèbres.

$\mathrm{Ker}(\varphi_a)$ est alors un idéal de $\mathbb{Q}[X]$ non nul
$(P \in \mathrm{Ker}(\varphi_a))$.

$\exists! \, \pi_a \in \mathbb{Q}[X]$, $\left| \begin{array}{l} \pi_a \text{ est unitaire} \\ \text{et } \mathrm{Ker}(\varphi_a) = \pi_a \mathbb{Q}[X] \end{array} \right.$

Donc $\pi_a \mid P$ (dans $\mathbb{Q}[X]$).

Or, P est irréductible sur $\mathbb{Q}$,
donc $\pi_a = P$.

Soit $\alpha, \beta, \gamma \in \mathbb{Q}$, $\alpha + \beta a + \gamma a^2 = 0$.

Donc $Q = \alpha + \beta X + \gamma X^2 \in \ker(\varphi_a)$,
donc $\exists R \in \mathbb{Q}[X]$, $Q = \pi_a \times R$,

où $\deg(Q) \leq 2$, et $\deg(\pi_a) = 3$.
Donc $\deg(R) = -\infty$: $R = 0$.
Donc $Q = 0$: $\alpha = 0$, $\beta = 0$, $\gamma = 0$.

Q4) Montrons que F est une sous-$\mathbb{Q}$-algèbre de $\mathbb{R}$, puis que F est un corps :

$F = \operatorname{Im}(\varphi_a)$, donc F est une sous-$\mathbb{Q}$-algèbre de $\mathbb{R}$ comme image de la $\mathbb{Q}$-algèbre $\mathbb{Q}[X]$ par φ_a, un morphisme de $\mathbb{Q}$-algèbre.

Soit $x \in F \setminus \{0\}$,

$$\mu_x \left| \begin{array}{ccc} F & \longrightarrow & F \\ y & \longmapsto & xy \end{array} \right. \quad \mathbb{Q}\text{-linéaire.}$$

F est intègre, donc μ_x est injective.
$\dim(F) = 3 < \infty$ donc μ_x est bijective.

$\exists y \in F$, $\mu_x(y) = xy = 1$.

Q5) Déterminer $\varphi : F \to F$, automorphisme de $\mathbb{Q}$-algèbre :

Analyse : Soit φ comme ci-dessus :

$$0 = \varphi(\underbrace{a^3 - a - 1}_{= 0}) = \varphi^3(a) - \varphi(a) - 1.$$

Donc $\varphi(a)$ est racine de $X^3 - X - 1$ dans $F \subset \mathbb{R}$, donc $\varphi(a) = a$.

Soit $x \in F$, $\exists\, \alpha, \beta, \gamma \in \mathbb{Q}$, $x = \alpha + \beta a + \gamma a^2$,

$$\varphi(x) = \alpha + \beta\varphi(a) + \gamma\varphi(a)^2$$
$$= x.$$

Donc $\varphi = id_F$.