Corrigé de l'examen final du mercredi 25 mai 2022

Exercice 1 1. Le polynôme P est irréductible par Eisenstein avec $p = 5$.

2. On a

$$(x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2 = -4 \times 5^3 - 27 \times 5^2 = -47 \times 5^2$$
$$\Rightarrow (x_1 - x_2)(x_2 - x_3)(x_1 - x_3) = \pm 5i\sqrt{47}$$
$$\Rightarrow i\sqrt{47} \in K = \mathbb{Q}(x_1, x_2, x_3)$$

et l'extension de $\mathbb{Q}$

$$\mathbb{F} = \mathbb{Q}(i\sqrt{47})$$

est quadratique.

3. Comme P est irréductible sur $\mathbb{Q}$, $3 \,|\, [K : \mathbb{Q}] = |\mathrm{Gal}(K/\mathbb{Q})|$.
Or, $[F : \mathbb{Q}] \,|\, [K : \mathbb{Q}] \Rightarrow 2 \,|\, |\mathrm{Gal}(K/\mathbb{Q})|$.
D'où $6 \,|\, |\mathrm{Gal}(K/\mathbb{Q})| \Rightarrow \mathrm{Gal}(K/\mathbb{Q}) = \mathfrak{S}_3$. Comme K est aussi galoisienne sur $\mathbb{F}$, on a $|\mathrm{Gal}(K/\mathbb{F}) = [K : \mathbb{F}] = 3$ et donc

$$\mathrm{Gal}(K/\mathbb{Q}) = \mathfrak{A}_3$$

seul sous-groupe d'ordre 3 de $\mathfrak{S}_3$.

Exercice 2 1.

$$P(0) = P(1) = 1 \neq 0$$

donc P n'a pas de racine dans $\mathbb{F}_2$. Dans $\mathbb{F}_4$, on a :

$$^\forall x \neq 0,\, x^3 = 1 \Rightarrow x^6 + x + 1 = 1 + x + 1 = x \neq 0$$

(on est en caractéristique 2). Donc P n'a pas de racine dans $\mathbb{F}_4$ non plus. Dans $\mathbb{F}_8$, on a

$$^\forall x \neq 0,\, x^7 = 1 \Rightarrow x^6 + x + 1 = \frac{x^7 + x^2 + x}{x} = \frac{x^2 + x + 1}{x} \neq 0$$

car si $x^2 + x + 1 = 0$, $x \in \mathbb{F}_4$ et comme $\mathbb{F}_4 \cap \mathbb{F}_8 = \mathbb{F}_2$, on aurait $x \in \mathbb{F}_2$, *absurde.* Donc pas de racine dans $\mathbb{F}_8$ non plus.

2. Soit Q un facteur irréductible unitaire de P de degré minimal dans $\mathbb{F}_2[X]$. Comme $\deg P = 6$, on a $d := \deg Q = 1, 2, 3$ ou 6.
Or P a une racine dans le corps $\mathbb{F}_2[X]/(Q) \simeq \mathbb{F}_{2^d}$. Comme il n'y a pas de racine dans $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8$, forcément, $d = 6$ donc $P = Q$ est irréductible.
Le corps $\mathbb{F}_2[X]/(P)$ est de cardinal $2^6 = 64$ car c'est un $\mathbb{F}_2-$espace vectoriel de dimension 6.

3. Comme $\overline{X} \in k^\times$, comme $k^\times$ est un groupe d'ordre 63, on a $\overline{X}^{63} = 1 \Rightarrow \overline{X}^{64} = \overline{X}$ dans k donc $P | X^{64} - X$.

4. Le groupe $k^\times$ est d'ordre 63 donc l'ordre de x divise $63 = 3^2 \times 7$ donc x est d'ordre $1, 3, 7, 3^2, 3 \times 7$ ou 63.
Or

$$x^1 = x \neq 1,\, x^3 \neq 1,\, x^7 = (x^6)x = (x + 1)x = x^2 + x \neq 1$$
$$x^9 = x^6x^3 = (x + 1)x^3 = x^4 + x \neq 1$$
$$x^{21} = (x^7)^3 = (x^2 + x)^3 = x^6 + x^5 + x^4 + x^3 = x^5 + x^4 + x^3 + x + 1 \neq 1$$

Donc x est d'ordre 63 et $\langle x \rangle = k^\times$.

5. Si $\alpha \in \mathbb{F}_{64}$, alors $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] \,|\, [\mathbb{F}_{64} : \mathbb{F}_2] = 6$ donc $\mathbb{F}_2(\alpha) = \mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8$ ou $\mathbb{F}_{64}$.
   Donc $\mathbb{F}_2(\alpha) = \mathbb{F}_{64} \Leftrightarrow \alpha \in \mathbb{F}_{64} \setminus \mathbb{F}_2 \cup \mathbb{F}_4 \cup \mathbb{F}_8$. Or

$$|\mathbb{F}_2 \cup \mathbb{F}_4 \cup \mathbb{F}_8| = |\mathbb{F}_4 \cup \mathbb{F}_8| = |\mathbb{F}_4| + |\mathbb{F}_8| - |\mathbb{F}_4 \cap \mathbb{F}_8| = 4 + 8 - |\mathbb{F}_2| = 10 \ .$$

   Il y a donc $64 - 10 = 54$ éléments $\alpha \in \mathbb{F}_{64}$ tels que $\mathbb{F}_2(\alpha) = \mathbb{F}_{64}$. Pour chacun de ces éléments, le polynôme minimal est de degré 6 et irréductible sur $\mathbb{F}_2$. Réciproquement, chaque polynôme irréductible unitaire Q de degré 6 sur $\mathbb{F}_2$ a exactement 6 racines dans $\mathbb{F}_{64}$. En effet, comme on l'a montré pour P, on a $Q|X^{64}-X$ et $\mathbb{F}_{64}$ est le corps de décomposition de $X^{64}-X$ sur $\mathbb{F}_2$. Chaque racine α d'un tel polynôme vérifie $\mathbb{F}_2(\alpha) = \mathbb{F}_{64}$. Conclusion le nombre de polynômes unitaires irréducibles de degré 6 sur $\mathbb{F}_2$ est n_6 qui vérifie :

$$6n_6 = 54 \Rightarrow n_6 = 9 \ .$$

Exercice 3 1.

$$Y - \alpha \,|\, P(Y) - P(\alpha) = P(Y)$$

dans $\mathbb{F}(\alpha)[X]$. Si on remplace Y par un polynôme $Q \in \mathbb{F}[X]$, on trouve :

$$Q(X) - \alpha \,|\, P(Q(X)) = R(X)$$

dans $\mathbb{F}(\alpha)[X]$.

2. Si $P(Y) = A(Y)B(Y)$ avec $A, B \in \mathbb{F}[X]$, alors $R(X) = P(Q(X)) = A(Q(X))B(Q(X))$ dans $\mathbb{F}[X]$. Donc comme R est irréductible sur $\mathbb{F}$, on a $A(Q(X))$ ou $B(Q(X))$ constant donc A ou B constant dans $\mathbb{F}[X]$. Ainsi P est irréductible sur $\mathbb{F}$.
   Soit x_0 une racine de R (dans une extension quelconque de $\mathbb{F}$). Alors $R(x_0) = P(Q(x_0)) = 0$ donc il existe $\sigma \in \mathrm{Gal}(L/\mathbb{F})$ tel que $\sigma(\alpha) = Q(x_0)$. On a :

$$\mathbb{F} \leq \mathbb{F}(\sigma(\alpha)) \leq \mathbb{F}(x_0)$$

$$\Rightarrow \deg R = [\mathbb{F}(x_0) : \mathbb{F}] = [\mathbb{F}(x_0) : \mathbb{F}(\sigma(\alpha))][\mathbb{F}(\sigma(\alpha)) : \mathbb{F}]$$

   (la première égalité vient de l'irréductibilité de R). Or $\mathbb{F}(\sigma(\alpha)) \simeq \mathbb{F}(\alpha)$ donc

$$[\mathbb{F}(\sigma(\alpha)) : \mathbb{F}] = [\mathbb{F}(\alpha) : \mathbb{F}] = \deg P$$

   car P est irréductible sur $\mathbb{F}$.
   Donc

$$[\mathbb{F}(x_0) : \mathbb{F}(\sigma(\alpha))] = \frac{\deg R}{\deg P} = \deg Q$$

   car $R = P(Q(X))$.
   Donc le polynôme $Q(X) - \sigma(\alpha) \in \mathbb{F}(\sigma(\alpha))[X]$ est le polynôme minimal de x_0 sur $\mathbb{F}(\sigma(\alpha))$ donc $Q(X) - \sigma(\alpha)$ est irréductible sur $\mathbb{F}(\sigma(\alpha))$.
   En appliquant σ^{-1}, on trouve que $Q(X) - \alpha$ est irréductible sur $\mathbb{F}(\alpha)$.

3. Soit x_0 une racine de $Q(X)-\alpha$ dans une extension de $\mathbb{F}(\alpha)$. Alors $R(x_0) = P(\alpha) = 0$. Donc :

$$[\mathbb{F}(x_0) : \mathbb{F}] = [\mathbb{F}(x_0) : \mathbb{F}(\alpha)][\mathbb{F}(\alpha) : \mathbb{F}]$$

$$= [\mathbb{F}(\alpha, x_0) : \mathbb{F}(\alpha)][\mathbb{F}(\alpha) : \mathbb{F}]$$
$$= \deg Q \deg P$$

car $Q(X) - \alpha$ est irréductible sur $\mathbb{F}(\alpha)$ et P est irréductible sur $\mathbb{F}$.
Or,

$$\deg Q \deg P = \deg R$$

donc R est forcément le polynôme minimal (à multiplication par un scalaire non nul près) de x_0 sur $\mathbb{F}$ et R est irréductible sur $\mathbb{F}$.

Exercice 4 1. Si $^\forall x \in \mathbb{C}$, $P(x, \phi(x)) = 0$ alors pour tout $x_0 \in \mathbb{C}$, on a :

$$^\forall n \in \mathbb{Z},\ P(x_0 + na, \phi(x_0)) = 0$$

donc le polynôme en une variable $P(X, \phi(x_0))$ est nul (car il a une infinté de racines !).
Soit $P(X, Y) = a_d(Y)X^d + ... + a_0(Y)$ où les a_i sont des polynômes dans $\mathbb{C}[Y]$ et $d = \deg_Y P$. On a forcément $a_d(\phi(x_0)) = 0$ pour tout $x_0 \in \mathbb{C}$. Comme ϕ est continue sur $\mathbb{C}$, $\phi(\mathbb{C})$ est infini dans $\mathbb{C}$. Donc $a_d = 0$. Donc $P = 0$.
On a montré que $I(A) = 0$.

2. Raisonnons par l'absurde, si $A = V(I)$ pour un idéal $I \leq \mathbb{C}[X, Y]$, alors

$$I \leq I(A) = 0 \Rightarrow I = 0 \Rightarrow A = V(0) = \mathbb{C}^2\ .$$

Or, $(0, y) \in \mathbb{C}^2 \setminus A$ si $y \neq \phi(0)$. D'où la contradiction. Donc A n'est pas de la forme $V(I)$ pour un idéal $I \leq \mathbb{C}[X, Y]$.