Corrigé du contrôle 2

Exercice 1

a) Posons $\alpha = \sqrt{2+\sqrt{2}}$

Alors $\alpha^2 = 2+\sqrt{2}$

$\Rightarrow (\alpha^2-2)^2 = 2$

$\Rightarrow \alpha^4 - 4\alpha^2 + 2 = 0$

$\Rightarrow \alpha$ est racine de

$$P(X) = X^4 - 4X^2 + 2.$$

Or $P(X) \in \mathbb{Q}[X]$ est irréductible d'après le critère d'Eisenstein.

Donc c'est le polynôme minimal de $\alpha = \sqrt{2+\sqrt{2}}$.

Ces racines sont :

$$x^4 - 4x^2 + 2 = 0 \iff x^2 = 2 \pm \sqrt{2}$$
$$\iff x = \pm\sqrt{2 \pm \sqrt{2}}$$

b) Le corps de décomposition de P sur $\mathbb{Q}$ est donc

$$K = \mathbb{Q}\left(\pm\sqrt{2\pm\sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}, \sqrt{2-\sqrt{2}}\right)$$

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

donc $\sqrt{2-\sqrt{2}} = \dfrac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} = \dfrac{\alpha^2-2}{\alpha} \in \mathbb{Q}(\alpha)$

d'où $K = \mathbb{Q}(\alpha)$

Or $[\mathbb{Q}(\alpha):\mathbb{Q}] = \deg P = 4$ donc $\mathrm{Gal}_{\mathbb{Q}}(P)$ est d'ordre 4.

Soit $\sigma : K \to K$

$$\alpha \longmapsto \sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\alpha}$$

Un tel morphisme de corps σ est bien défini car $\sqrt{2-\sqrt{2}}$ est une racine de $P = P_\alpha$.

On a $\sigma^2(\alpha) = \sigma\left(\frac{\sqrt{2}}{\alpha}\right) = \frac{\sigma(\sqrt{2})}{\sigma(\alpha)}$

Or $\sigma(\alpha) = \sqrt{2-\sqrt{2}}$

$\Rightarrow \sigma(\sqrt{2}) = \sigma(\alpha^2 - 2) = \sigma(\alpha)^2 - 2$

$= 2 - \sqrt{2} - 2 = -\sqrt{2}$

$\Rightarrow \sigma^2(\alpha) = \frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}} = -\sqrt{2+\sqrt{2}} = -\alpha$

$\Rightarrow \sigma^4(\alpha) = (\sigma^2 \circ \sigma^2)(\alpha) = \sqrt{2+\sqrt{2}} = \alpha$

$\Rightarrow \sigma^4 = Id$

Donc σ est d'ordre 4 et $G = Gal_{\mathbb{Q}} P = \langle \sigma \rangle \cong \mathbb{Z}/4\mathbb{Z}$.

Exercice 2

a) $P(X) = \frac{X^4}{4!} + \frac{X^3}{3!} + \frac{X^2}{2!} + X + 1$

$\Rightarrow P'(X) = \frac{X^3}{3!} + \frac{X^2}{2!} + X + 1$

$P(X) - P'(X) = \frac{X^4}{4!}$ donc le pgcd de P et P' divise $\frac{X^4}{4!}$

donc c'est une puissance de X. Or X et $P(X)$ sont premiers

entre eux.

Donc $\text{pgcd}(P, P') = 1$.

Si α était une racine multiple de P (d'ordre ≥ 2), on aurait $X-\alpha \mid \text{pgcd}(P,P')$ absurde.

Donc les racines (complexes de P) sont simples (donc 2 à 2 distinctes). Comme $\deg P = 4$, il y en a 4.

b) $24P(X) = X^4 + 4X^3 + 12X^2 + 24X + 24$

$= (X-x_1)(X-x_2)(X-x_3)(X-x_4)$

donc $24P'(x_i) = \prod_{\substack{j=1 \\ j\neq i}}^{4} (x_i - x_j)$

donc $\Delta = \prod_{1\leq i<j\leq 4} (x_i - x_j)^2$

$= \prod_{1\leq i\neq j\leq 4} (x_i - x_j) \cdot (-1)^{\binom{4}{2}}$

$= \prod_{i=1}^{4} 24\, P'(x_i)$

$= (24)^4 P'(x_1)P'(x_2)P'(x_3)P'(x_4)$

Comme $P'(x_i) = \frac{x_i^4}{4!} + \frac{x_i^3}{3!} + \frac{x_i^2}{2!} + x_i + 1 - \frac{x_i^4}{4!}$

$= 0 - \frac{x_i^4}{4!} = \frac{-x_i^4}{4!}$

$\Rightarrow \Delta = \prod_{i=1}^{4} (-x_i^4) = (x_1 x_2 x_3 x_4)^4 = 24^4$.

c) Le groupe de Galois $G = \mathrm{Gal}_{\mathbb{Q}} P$ s'identifie à un sous-groupe de $\mathfrak{S}_4$:

$$G \longrightarrow \mathfrak{S}_4$$
$$\theta \longmapsto \sigma$$

où $\theta(x_i) = x_{\sigma(i)}$ $(\forall 1 \leq i \leq 4)$

Or $\Delta = \delta^2$ avec $\delta = \prod_{1 \leq i < j \leq 4} (x_i - x_j)$

$\Rightarrow \delta = \pm 24^2 \in \mathbb{Q}$

$\Rightarrow \forall \theta \in G, \quad \theta(\delta) = \delta$

Or $\theta(\delta) = \varepsilon(\sigma)\delta$ si σ est la permutation correspondant à θ.

Donc $\forall \sigma \in G, \varepsilon(\sigma) = 1$ et G s'identifie à un sous-groupe de $A_4 = \ker \varepsilon$.

d) $4! P(X) = +X^4 - X^3 + 2X^2 - X - 1 \mod 5$

$= (X-1)(X^3 + 2X + 1)$

Comme $X^3 + 2X + 1$ n'a pas de racine dans $\mathbb{F}_5$ ($0, \pm 1, \pm 2$ ne sont pas racines),

$4! P(X) = (X-1)(X^3 + 2X + 1)$ est la décomposition en facteurs irréductibles dans $\mathbb{F}_5[X]$.

Dans $\mathbb{F}_{17}[X]$:

$$4!P = X^4 + 4X^3 - 5X^2 + 7X + 7$$

$$= (X^2 + X - 1)(X^2 + 3X - 7) \mod 17$$

Calculons les discriminants des polynômes de degré 2 obtenus :

$X^2 + X - 1$: $\Delta = 1 + 4 = 5$

$X^2 + 3X - 7$: $\Delta = 9 + 28 = 37 = 3 \mod 17$

Or ni 5, ni 3 ne sont des carrés mod 17

(en effet : $\left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1$

et $\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = -1$)

Donc on a trouvé la factorisation en irréductibles mod 17.

e) Pour montrer que P est irréductible sur $\mathbb{Q}$, il suffit de montrer que $24P$ l'est $\Leftrightarrow$ $24P$ est irréductible sur $\mathbb{Z}$.

Or si $24P = QR$ avec $Q, R \in \mathbb{Z}[X]$ (unitaires) et $1 \leq \deg Q, \deg R < 4$, alors mod 5 on a :

$\overline{24P} = \overline{Q}\,\overline{R} \Rightarrow \deg \overline{Q}$ ou $\deg \overline{R} = 1$

et mod 17 : $\overline{24P} = \overline{Q}\,\overline{R} \Rightarrow \deg \overline{Q} = \deg \overline{R} = 2$

absurde !

Donc P est irréductible sur $\mathbb{Q}$

f)

Donc $G = Gal_{\mathbb{Q}}(P)$ est un sous-groupe de A_4 (d'après c))
qui agit transitivement sur $(1,2,3,4)$.
Donc l'ordre de G est un multiple de 4 qui divise $12 = 4 \times 3$

$\Rightarrow G = K = \{1, (12)(34), (13)(24), (14)(23)\}$ (d'ordre 4)

ou $G = A_4$, d'ordre 12.

g) $(X-\alpha)(X-\beta)(X-\gamma) = X^3 - (\alpha+\beta+\gamma)X^2 + (\alpha\beta+\beta\gamma+\alpha\gamma)X - \alpha\beta\gamma$

On a : $24P = (X-x_1)(X-x_2)(X-x_3)(X-x_4) = X^4 + 4X^3 + 12X^2 + 24X + 24$

$\Rightarrow$
$$\left.\begin{aligned} x_1+x_2+x_3+x_4 &= -4 \\ x_1x_2 + x_2x_3 + x_3x_4 + x_1x_3 + x_2x_4 + x_1x_4 &= 12 \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 &= -24 \\ x_1x_2x_3x_4 &= 24 \end{aligned}\right\} \text{ relations coefficients-racines}$$

$\alpha+\beta+\gamma = x_1x_2 + \dots + x_1x_4 = 12$

$\alpha\beta+\beta\gamma+\alpha\gamma = x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2 + x_1^2x_2x_4 + x_1x_2^2x_4 + x_1x_2x_4^2$
$+ x_1^2x_3x_4 + x_1x_3^2x_4 + x_1x_3x_4^2 + x_2^2x_3x_4 + x_2x_3^2x_4 + x_2x_3x_4^2$

$= x_1x_2x_3(-4-x_4) + x_1x_2x_4(-4-x_3) + x_1x_3x_4(-4-x_2) + x_2x_3x_4(-4-x_1)$

$= -4 \times (-24) - 4 \times 24 = 0$

$\alpha\beta\gamma = x_1^3x_2x_3x_4 + x_1x_2^3x_3x_4 + x_1x_2x_3^3x_4 + x_1x_2x_3x_4^3$
$+ x_1^2x_2^2x_3^2 + x_1^2x_2^2x_4^2 + x_1^2x_3^2x_4^2 + x_2^2x_3^2x_4^2$

$= x_1x_2x_3x_4(x_1^2+x_2^2+x_3^2+x_4^2) + (-24)^2 - 2[x_1^2x_2^2x_3x_4 + x_1^2x_2x_3^2x_4 + x_1^2x_2x_3x_4^2$
$+ x_1x_2^2x_3^2x_4 + x_1x_2^2x_3x_4^2 + x_1x_2x_3^2x_4^2]$

$= 24[(-4)^2 - 2x_1x_2 - 2x_1x_3 - \dots] + 24^2 - 2x_1x_2x_3x_4 \times [x_1x_2 + \dots]$

$= 24[16 - 2 \times 12] + 24^2 - 2 \times 24 \times [12] = -8 \times 24 = -192 = -3 \times 2^6$

d'où $(X-\alpha)(X-\beta)(X-\gamma) = X^3 - 12X^2 + 192$.

h) Le polynôme $R(X) = (X-\alpha)(X-\beta)(X-\gamma)$ est irréductible sur $\mathbb{Q}$ (par Eisenstein avec $p=3$)

donc $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$

or $\mathbb{Q}(\alpha) \subset \mathbb{Q}(x_1, x_2, x_3, x_4)$

donc $[\mathbb{Q}(x_1, x_2, x_3, x_4) : \mathbb{Q}]$ est un multiple de 3

Comme $|G| = [\mathbb{Q}(x_1, x_2, x_3, x_4) : \mathbb{Q}]$; on a :

$|G| = 12$ et $G = A_4$.

Exercice 3

a) On note $A_1, \dots, A_N$ les points de $\mathbb{A}$.

Soit $0 \neq v \in K^2 \setminus \{\overrightarrow{A_iA_j} \mid 1 \leq i \neq j \leq N\}$ $K^2 \setminus \bigcup_{i \neq j} K \overrightarrow{A_iA_j}$

où $\overrightarrow{A_iA_j} = A_j - A_i$. (c'est possible car K infini $\Rightarrow K^2$ n'est pas une réunion finie de sous-espaces propres)

On complète en une base (u, v) de K^2.

si $A_i, A_j \in D_a$ avec $i \neq j$, alors

$A_i = au + xv$ et $A_j = au + x'v$

où $x, x' \in K$

$\Rightarrow \overrightarrow{A_iA_j} = (x'-x)v \Rightarrow v \in K \overrightarrow{A_iA_j}$ absurde !

---

b) Notons $A_1, \dots, A_N$ les points de A

et $A_i = (x_i, y_j)$ leurs coordonnées.

Alors $\forall i \neq j$, $x_i \neq x_j$ car $A \cap (x = x_i)$

a au plus un élément.

Soit $P \in K[X]$ tel que $\forall i$, $P(x_i) = y_i$.

Il suffit de poser par exemple :

$$P(X) = \sum_{j=1}^{n} y_j \frac{\prod_{\substack{k=1 \\ k \neq j}}^{N} (X - x_k)}{\prod_{\substack{k=1 \\ k \neq j}}^{N} (x_j - x_k)}$$

on a alors :

$$A = \{ (x_i, P(x_i)) \mid i = 1 \text{ à } N \}$$

on pose ensuite $G(X) = \prod_{k=1}^{N} (X - x_k) \in K[X] \leq K[X,Y]$

et $F(X,Y) = Y - P(X) \in K[X,Y]$.

Alors $V(\langle F, G \rangle) = \{ (x,y) \in K^2 \mid F(x,y) = G(x,y) = 0 \}$

$$= \bigcup_k \{ (x,y) \in K^2 \mid x = x_k, y = P(x_k) \}$$

$$= A.$$