Contrôle final de 2020
correction

Exercice 1

Soit $A \in M_n(k)$. La matrice A est nilpotente $\Leftrightarrow A^n = 0 \Leftrightarrow \chi_A(X) = X^n$ où $\chi_A(X)$ est le polynôme caractéristique de A.

Notons $p_1(A), ..., p_n(A)$ les coefficients de $\chi_A(X) : \chi_A(X) = X^n + p_1(A)X^{n-1} + ... + p_n(A)$. Bien sûr, $p_1(A) = -\mathrm{Tr}(A)$ et $p_n(A) = (-1)^n \det A$.

Donc $N = V(p_1, ..., p_n) = \{A \in M_n(k) \ : \ p_1(A) = ... = p_n(A) = 0\}$. C'est donc un sous-esemble algébrique affine de $M_n(k)$.

On a donc $I(N) = \sqrt{(p_1, ..., p_n)}$.

On peut montrer par des méthodes sophistiquées (hors programme) d'algèbre commutative que $I(N) = (p_1, ..., p_n)$.

Exercice 2 Dans $\mathbb{R}^2$, on a :

$$\{(\cos x, \sin x \ : \ x \in \mathbb{R}\} = V(X^2 + Y^2 - 1)$$

c'est donc un sous-ensemble algébrique affine.

On a :

$$^\forall x \in \mathbb{R},\ \cos(2x) = 1 - 2\sin^2 x \ .$$

Donc $X - 2Y^2 \in I(B)$.

Réciproquement si $P \in \mathbb{R}[X, Y]$,

$$P = R(Y) mod X - 2Y^2$$

(en faisant une division euclidienne par $X - 2Y^2$ dans $\mathbb{R}[Y][X]$) où $R(Y) \in \mathbb{R}[Y]$. Donc $P \in I(B) \Rightarrow {}^\forall x \in \mathbb{R},\ P(\cos(2x), \sin x) = R(\sin x) = 0$. Donc $R = 0$ et $P \in (X - 2Y^2)$.

Donc $I(B) = (X - 2Y^2)$.

Si B était un sous-ensemble algébrique affine, on aurait $B = V(I(B)) = V(X - 2Y^2)$. C'est impossible car par exemple si on prend $y = 2$ et $x = 8$, on a $x = 2y^2 \Rightarrow (8, 2) \in V(X - 2Y^2)$ mais $(8, 2) \notin B$ car $|y| > 1$.

Donc B n'est pas un sous-ensemble algébrique affine de $\mathbb{R}^2$.

Remarque. En revanche, on a bien $B_{\mathbb{C}} = \{(\cos(2x), \sin x) \ : \ x \in \mathbb{C}\} = V_{\mathbb{C}}(X - 2Y^2)$ *qui est bien un sous-ensemble algébrique affine de* $\mathbb{C}^2$.

Exercice 3 a) Comme $\mathbb{Q}$ est de caractéristique nulle $E/\mathbb{Q}$ est séparable. Soit $\sigma : E \to \mathbb{C}$ un morphisme de corps. Alors ${}^\forall r \in \mathbb{Q}$, $\sigma(r) = r$ et $(\sigma(\sqrt{2})^2 = \sigma(\sqrt{2}^2) = \sigma(2) = 2 \Rightarrow \sigma(\sqrt{2}) = \pm\sqrt{2} \in E$. De même $\sigma(\sqrt{3}) \in E$. Donc $\sigma(E) \leq E$. C'est vrai pour tout morphisme de corps σ donc $E/\mathbb{Q}$ est normale.

L'extension $E/\mathbb{Q}$ est normale et séparable donc galoisienne.

Soit $\phi : \mathrm{Gal}(E/\mathbb{Q}) \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\sigma \mapsto (\epsilon_1, \epsilon_2)$ où $\sigma(\sqrt{2}) = (-1)^{\epsilon_1}\sqrt{2}$ et $\sigma(\sqrt{3}) = (-1)^{\epsilon_2}\sqrt{3}$. L'application ϕ est un morphisme de groupes, injectif car $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Or $E/\mathbb{Q}$ est galoisienne donc $\mathrm{Gal}(E/\mathbb{Q})$ est d'ordre $[E : \mathbb{Q}] = 4$ car $\sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \Rightarrow \sqrt{3}$ est de degré 2 sur $\mathbb{Q}(\sqrt{2})$.

Donc ϕ est un isomorphisme de groupes. Notons s_1, s_2, s_3, s_4 les morphismes $\phi^{-1}(0, 0), \phi^{-1}(0, 1), \phi^{-1}(1, 0), \phi^{-1}(1, 1)$.

b) On a : $\alpha^2 = (2+\sqrt{2})(3+\sqrt{3}) \in E$; Donc $\mathbb{Q}(\alpha^2) \leq E$. Les éléments de $\mathrm{Gal}(E/\mathbb{Q})$ sont les morphismes :

$$s_1, s_2, s_3, s_4$$

où :

$$s_1(\alpha^2) = (2+\sqrt{2})(3+\sqrt{3}),\ s_2(\alpha^2) = (2+\sqrt{2})(3-\sqrt{3}),$$
$$s_3(\alpha^2) = (2-\sqrt{2})(3+\sqrt{3}),\ s_4(\alpha^2) = (2-\sqrt{2})(3-\sqrt{3})\ .$$

Comme $\mathbb{Q}(\alpha^2)/\mathbb{Q}$ est séparable, on a

$$[\mathbb{Q}(\alpha^2) : \mathbb{Q}] \geq |\{s_1(\alpha^2), s_2(\alpha^2), s_3(\alpha^2), s_4(\alpha^2)\} = 4$$

donc $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 4 = [E : \mathbb{Q}] \Rightarrow \mathbb{Q}(\alpha^2) = E$. En particulier, $E = \mathbb{Q}(\alpha^2) \leq \mathbb{Q}(\alpha$.

c) On a

$$(X-(2+\sqrt{2})(3+\sqrt{3}))(X-(2-\sqrt{2})(3+\sqrt{3}))(X-(2+\sqrt{2})(3-\sqrt{3}))(X-(2-\sqrt{2})(3-\sqrt{3}))$$
$$= (X^2 - 6(2+\sqrt{2})X + 6(6+4\sqrt{2}))(X^2 - 6(2-\sqrt{2})X + 6(6-4\sqrt{2}))$$
$$= X^4 - 24X^3 + 144X^2 - 288X + 144\ .$$

Donc :

$$(X^2-\alpha^2)(X^2-\beta^2)(X^2-\gamma^2)(X^2-\delta^2) = X^8-24X^6+144X^4-288X^2+144\,.$$

d) Il suffit de montrer que l'extension est normale. Soit $\sigma : \mathbb{Q}(\alpha) \to \mathbb{C}$ un morphisme de corps. Alors si on pose $P(X) = (X^2-\alpha^2)(X^2-\beta^2)(X^2-\gamma^2)(X^2-\delta^2)$, on a $P(\alpha^2) = 0$. comme P est à coefficients dans $\mathbb{Q}$, on a aussi

$$0 = \sigma(P(\alpha^2)) = P((\sigma(\alpha))^2) \Rightarrow \sigma(\alpha)^2 = \alpha^2, \beta^2, \gamma^2 \text{ ou } \delta^2$$

donc $\sigma(\alpha) = \pm\alpha, \pm\beta, \pm\gamma$ ou $\pm\delta$.

Or, $\alpha\beta = \sqrt{2}(3+\sqrt{3}) \in E \leq \mathbb{Q}(\alpha) \Rightarrow \beta = \frac{\sqrt{2}(3+\sqrt{3})}{\alpha} \in \mathbb{Q}(\alpha)$.

De même, $\gamma, \delta \in \mathbb{Q}(\alpha)$.

Donc pour tout $\sigma : \mathbb{Q}(\alpha) \to \mathbb{C}$ morphisme de corps, on a $\sigma(\alpha) \in \mathbb{Q}(\alpha)$. Donc $\mathbb{Q}(\alpha)/\mathbb{Q}$ est normale donc galoisienne.

e) Il existe $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ tel que $\sigma(\sqrt{2}) = \sqrt{2}$ et $\sigma(\sqrt{3}) = -\sqrt{3}$. On peut prolonger σ en un morphisme de corps $\mathbb{Q}(\alpha) \to \mathbb{C}$. Comme $\mathbb{Q}(\alpha)/\mathbb{Q}$ est normale, σ est un automorphisme de $\mathbb{Q}(\alpha)$.

On a

$$\left(\frac{\sigma(\alpha)}{\alpha}\right)^2 = \frac{\sigma(\alpha^2)}{\alpha^2} = \frac{(2+\sqrt{2})(3-\sqrt{3})}{(2+\sqrt{2})(3+\sqrt{3})}$$
$$= \frac{3-\sqrt{3}}{3+\sqrt{3}} = \frac{(3-\sqrt{3})^2}{6}$$

donc $\frac{\sigma(\alpha)}{\alpha} = \pm\sqrt{\frac{(3-\sqrt{3})^2}{6}} = \pm\frac{3-\sqrt{3}}{6}$.

f) Notons $\epsilon = \pm 1$ tel que

$$\frac{\sigma(\alpha)}{\alpha} = \epsilon \frac{3-\sqrt{3}}{6} \ .$$

On a $\sigma\left(\frac{\sigma(\alpha)}{\alpha}\right) = \frac{\sigma^2(\alpha)}{\sigma(\alpha)} = \epsilon\frac{3+\sqrt{3}}{-\sqrt{6}}$.
Donc :

$$\sigma^2(\alpha) = -\epsilon\sigma(\alpha)\frac{3+\sqrt{3}}{\sqrt{6}} = -\epsilon^2\alpha\frac{3-\sqrt{3}}{\sqrt{6}}\frac{3+\sqrt{3}}{\sqrt{6}} = -\alpha \ .$$

Comme $\alpha^2 \in E$, α est de degré au plus 2 sur E. Comme σ^2 est l'identité sur E, $\sigma^2(\alpha) = -\alpha \neq \alpha \Rightarrow \alpha \notin E$. Donc α est de degré 2 sur E.
Puisque $\mathbb{Q}(\sqrt{2}) \leq E \leq \mathbb{Q}(\alpha)$, on a alors $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\alpha) : E][E : \mathbb{Q}(\sqrt{2})] = 2.2 = 4$.
Comme $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne, $\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{2})$ aussi. Donc $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{2}))$ est d'ordre $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] = 4$. Or $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{2}))$ est d'ordre 4 (car $\sigma^2 \neq \sigma$ et $\sigma^4 = \mathrm{Id}$ (car $\sigma^4(\alpha) = \sigma^2(-\alpha) = \alpha$)).
Donc $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{2})) = \langle\sigma\rangle$. et $|G| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 8$.

g) De même, $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{3}))$ (respectivement $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{6}))$) est cyclique d'ordre 4 engendré par un $\tau \in G$ tel que $\tau(\sqrt{2}) = -\sqrt{2}$ (respectivement un $\upsilon \in G$ tel que $\upsilon(\sqrt{2}) = -\sqrt{2}$ et $\upsilon(\sqrt{3}) = -\sqrt{3}$).

h) Comme τ est d'ordre 4, on n'a pas $\tau \in \mathrm{Gal}(\mathbb{Q}(\alpha)/E))$ qui est un groupe d'ordre 2. Donc $\tau(\sqrt{2}) = -\sqrt{2}$.
On en déduit $\tau(\alpha) = \epsilon'(\sqrt{2}-1)\alpha$ où $\epsilon' = \pm 1$. Or $\sigma(\alpha) = \epsilon\frac{3-\sqrt{3}}{\sqrt{6}}\alpha$ où $\epsilon = \pm 1$.
On a alors $\sigma(\tau(\alpha)) = \epsilon'\epsilon(\sqrt{2}-1)\frac{3-\sqrt{3}}{\sqrt{6}}\alpha = \epsilon\epsilon'\frac{(\sqrt{2}-1)(\sqrt{3}-1)}{\sqrt{2}}\alpha$. D'un autre côté, $\tau(\sigma(\alpha)) = -\epsilon\epsilon'\frac{(\sqrt{2}-1)(\sqrt{3}-1)}{\sqrt{2}}\alpha = -\sigma(\tau(\alpha))$.
Donc $\sigma\tau \neq \tau\sigma$.

i) $\sigma^2(\alpha) = \tau^2(\alpha) = -\alpha$. Donc $\sigma^2 = \tau^2$. Soit $f \in G$ d'ordre 2. Comme $f \in G$, on a $f(\alpha^2) \in \{\alpha^2, \beta^2, \gamma^2, \delta^2\}$. Si $f(\alpha^2) = \beta^2$, alors $f(\alpha) = \epsilon\beta$ où $\epsilon = \pm 1$. Comme $f^2(\alpha) = \alpha$, on a $f(\epsilon\beta) = \epsilon f(\beta) = \alpha \Rightarrow f(\beta) = \epsilon\alpha$. Or $\alpha\beta = \sqrt{2}(3+\sqrt{3})$. On voit que $\mathbb{Q}(\alpha\beta) = E$ (car $\alpha\beta$ a 4 conjugués donc est de degré 4 sur $\mathbb{Q}$). On a $f(\alpha\beta) = \epsilon^2\beta\alpha = \alpha\beta \Rightarrow f|_E = \mathrm{Id}$. Mais alors, $f(\alpha^2) = \alpha^2$ *absurde !*
Donc $f(\alpha^2) \neq \beta^2$. De même, on montre que $f(\alpha^2) \neq \gamma^2$. Si $f(\alpha^2) = \delta^2$, alors $f(\alpha) = \epsilon\delta$ et $f(\delta) = \epsilon\alpha$. Pour un $\epsilon = \pm 1$. Mais alors $f(\alpha\delta) = \alpha\delta \Leftrightarrow f(2\sqrt{3}) = 2\sqrt{3} \Rightarrow f(\sqrt{3}) = \sqrt{3})$. Donc $f(\alpha^2) = (2 \pm \sqrt{2})(3+\sqrt{3}) \neq \delta^2$ *contradiction !*.
Donc $f(\alpha^2) \neq \delta^2$. Nécessairement, $f(\alpha^2) = \alpha^2$. D'où $f(\alpha) = -\alpha$ (car $f \neq \mathrm{Id}$). Donc $f = \sigma^2 = \tau^2$ est le seul élément d'ordre 2 de G.

j) D'après la correspondance de Galois, un sous-corps de $\mathbb{Q}(\alpha)$ de degré 4 sur Q est de la forme $\mathbb{Q}(\alpha)^H$ où H est un sous-groupe de G et où $|H| = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha)^H] = \frac{8}{[\mathbb{Q}(\alpha)^H:\mathbb{Q}]} = 2$. Donc forcément $H = \langle\sigma^2\rangle$, seul sous-groupe de G d'ordre 2 d'après la question précédente. En particulier il y a un seul sous-corps de $\mathbb{Q}(\alpha)$ de degré 4 sur $\mathbb{Q}$. Comme E en est un, ce seul sous-corps est E !

k) Comme $\sigma\tau \neq \tau\sigma$, G est non abélien. De plus dans le groupe diédral D_4, il y a 5 éléments d'ordre 2 (les 4 symétries et la rotation d'angle π) alors que G a un seul élément d'ordre 2. Donc $G \not\simeq D_4$.

l) Il y a une bijection entre les sous-corps de $\mathbb{Q}(\alpha)$ et les sous-groupes de G. Une étude rapide des relations dans $G : \sigma^2 = \tau^2 = (\sigma\tau)^2 \Rightarrow \sigma\tau = (\tau\sigma)^{-1}$ montrer que les sous-groupes de G d'ordre 4 sont $\langle\sigma\rangle, \langle\tau\rangle, \langle\sigma\tau\rangle$. En particulier il y a exactement 3 sous-corps de $\mathbb{Q}(\alpha)$ de degré 2 sur $\mathbb{Q}$. Les voici :

$$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$$

voici le sous-corps de $\mathbb{Q}(\alpha)$ de degré 4 sur $\mathbb{Q}$:

$$E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

et les autres sous-corps sont bien sûr $\mathbb{Q}$ et $\mathbb{Q}(\alpha)$ lui-même.

m) L'extension $\mathbb{Q}(i, \sqrt[4]{2})$ est galoisienne sur $\mathbb{Q}$ et son groupe de Galois est isomorphe au groupe diédral D_4 (c'est le corps de décomposition du polynôme $X^4 - 2$ sur $\mathbb{Q}$).

Exercice 4

1. Soit $f_1, ..., f_N$ un système de générateurs de I. Il existe un polynôme non nul $q(y_1, ..., y_m) \in k[y_1, ..., y_m]$ tel que $qf_i \in k[y_1, ..., y_m, x_1, ..., x_n]$ pour tout i. (Il suffit de prendre par exemple pour q le ppcm des dénominateurs en $y_1, ..., y_m$ qui apparaissent dans les coefficients (en nombre fini) des f_i).
   On a $\frac{1}{q} \in K$ donc $I = (f_1, ..., f_N) = (qf_1, ..., qf_N)$. Et $G_1 = \{qf_1, ..., qf_N\}$ convient.
2. Si $g \in G_2 \cap k[y_1, ..., y_m]$ alors par définition $g \neq 0$ et g est inversible dans K. Comme $g \in I$, on a $\langle g\rangle \leq I \Rightarrow I = K[x_1, ..., x_n]$ †.
   Réciproquement, si $I = K[x_1, ..., x_n]$ pn a $1 \in I$. Donc 1 est dans l'idéal engendré par les termes dominants des éléments de G_2, en particulier il y a des éléments dans G_2 dont le terme dominant est 1. Par définition de l'ordre choisi, un tel élément est forcément dans $k[y_1, ..., y_m]$!
3. Comme $\langle G_2\rangle_{k[y_1,...,y_m,x_1,...,x_n]} = I_1$, on a $\langle G_2\rangle_{K[x_1,...,x_n]} = \langle I_1\rangle_{K[x_1,...,x_n]} = I$.
   Il reste à montrer que $\langle TD(g) \,:\, g \in G_2\rangle = TD(I)$ (pour l'ordre $\preceq$). Or si $f \in I$, il existe un $0 \neq q \in k[y_1, ..., y_m]$ tel que $qf \in I_1$. On a alors :

$$TD_{\preceq_1}(qf) = \sum_i a_i TD_{\preceq_1}(g_i)$$

   où les $g_i \in G_2$ et les $a_i \in k[x_1, ..., x_n, y_1, ..., y_m]$.
   Mais $TD_{\preceq}(f) = rx^\alpha$ pour un certain $r \in K$. Alors $TD_{\preceq_1}(qf) = y^\beta x^\alpha$ pour un certain $\beta \in \mathbb{N}^m$. Donc :

$$TD_{\preceq}(f) = rx^\alpha = \sum_i a_i \frac{r}{y^\beta} TD_{\preceq_1}(g_i)$$

   Comme pour tout i, $TD_{\preceq}(g_i) \;\Big|\; TD_{\preceq_1}(g_i)$ dans $K[x_1, ..., x_n]$, on a bien

$$TD_{\preceq}(f) \in \sum_i K[x_1, ..., x_n] TD_{\preceq}(g_i) \ .$$

† *Corriger l'énoncé : il s'agit de montrer que* $G_2 \cap k[y_1, ..., y_m] \neq \emptyset \Leftrightarrow I = K[x_1, ..., x_n]$.