Nombres algébriques, nombres transcendants, constructions à la règle et au compas.

Corrigé

Partie I

1. a. $\sqrt{2}$ et $\sqrt{3}$ annulent respectivement les polynômes X^2-2 et X^3-3 de $\mathbb{Q}[X]$.

On sait déjà que $\mathbb{Q}[\sqrt{2}]$ est un anneau, il reste à montrer que tout élément non nul de $\mathbb{Q}[\sqrt{2}]$ est inversible. Le polynôme X^2-2 est irréductible sur $\mathbb{Q}$ puisqu'il est de degré 2 sans racine dans $\mathbb{Q}$. Donc tout polynôme $P \in \mathbb{Q}[X]$ est soit divisible par X^2-2, soit premier à X^2-2. S'il est divisible par X^2-2, alors $P(\sqrt{2})=0$. Sinon, il existe U et V dans $\mathbb{Q}[X]$ tels que $U(X)P(X)+V(X)(X^2-2)=1$. Alors $U(\sqrt{2}).P(\sqrt{2})=1$, ce qui signifie que $P(\sqrt{2})$ est inversible dans $\mathbb{Q}[\sqrt{2}]$, d'inverse $U(\sqrt{2})$. On a montré que $\mathbb{Q}[\sqrt{2}]$ est un corps.
Soit $P \in \mathbb{Q}[X]$. La division euclidienne de P par X^2-2 donne un reste R de degré au plus 1. On a alors $P(\sqrt{2})=R(\sqrt{2}$. Cela montre que tout élément de $\mathbb{Q}[\sqrt{2}]$ s'écrit sous la forme $a+b\sqrt{2}$, avec $a,b \in \mathbb{Q}$. Comme $\sqrt{2}$ n'est pas rationnel, $\mathbb{Q}[\sqrt{2}] \neq \mathbb{Q}$. Cela montre que $\mathbb{Q}[\sqrt{2}]$ est de dimension sur $\mathbb{Q}$ au moins 2, donc égale à 2, avec $(1,\sqrt{2})$ comme base.
Remarque : lorsqu'on sait que tout élément de $\mathbb{Q}[\sqrt{2}]$ est de la forme $x=a+b\sqrt{2}$, on peut trouver son inverse en multipliant par la quantité conjuguée, par une formule bien connue pour les complexes $x^{-1}=\frac{\overline{x}}{||x||^2}$ où ici $\overline{x}=a-b\sqrt{2}$ et $||x||^2=a^2+2b^2$.

b. On a $(\sqrt{2}+\sqrt{3})^2=5+2\sqrt{6}$, donc $\sqrt{6}=\frac{1}{2}\alpha^2-\frac{5}{2} \in \mathbb{Q}[\alpha]$.
On a alors $24=\alpha^4-10\alpha^2+25$, donc α annule le polynôme $M_\alpha(X)=X^4-10X^2+1$.

c. Soit $P \in \mathbb{Q}[X]$. La division de P par M_α donne un reste R de degré au plus 3. On a alors $P(\alpha)=R(\alpha)$, ce qui montre le résultat demandé.

d. Supposons que $r=\frac{p}{q}$ est racine de M_α, avec $p \wedge q=1$ et $q>0$. Cela donne $(\frac{p}{q})^4-10(\frac{p}{q})^2+1=0$, donc $p^4-10p^2q^2+q^4=0$. Donc q divise p^4, mais comme p et q sont premiers entre eux, alors $q=1$. D'où $p^4-10p^2=-1$, p est inversible dans $\mathbb{Z}$, donc $p=\pm 1$. Mais 1 et -1 ne sont pas racines de M_α, cela conclut.

e. Supposons que $\sqrt{3}=a+b\sqrt{2}$. Alors $3=(a^2+2b^2)+2\sqrt{2}ab$. Comme $\sqrt{2}$ est irrationnel, cela impose $ab=0$. Mais $\sqrt{3}$ n'est pas rationnel, donc $b \neq 0$, ce qui donne $3=2b^2$, ce qui est absurde. Donc $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.
On a $\sqrt{2}+\sqrt{3} \in \mathbb{Q}[\alpha]$ et $\sqrt{6}(\sqrt{2}+\sqrt{3})=2\sqrt{3}+3\sqrt{2} \in \mathbb{Q}[\alpha]$. Par combinaison linéaire, on obtient que $\sqrt{2}$ et $\sqrt{3}$ appartiennent à $\mathbb{Q}[\alpha]$.
Supposons que $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}=0$, avec $a,b,c,d \in \mathbb{Q}$. Cela donne $\sqrt{3}(c+d\sqrt{2})=a+b\sqrt{2}$. Si $c+d\sqrt{2}=0$, alors $c=d=0$ puis $a=b=0$ puisque $(1,\sqrt{2})$ est une base de $\mathbb{Q}[\sqrt{2}]$. Sinon $c+d\sqrt{2}$ est inversible dans $\mathbb{Q}[\sqrt{2}]$ (qui est un corps), donc $\sqrt{3} \in \mathbb{Q}[\sqrt{2}]$, ce qui contredit ce qu'on vient de montrer. Cela montre que $(1,\sqrt{2},\sqrt{3},\sqrt{6})$ forme une famille libre de $\mathbb{Q}[\alpha]$. On a vu à la question 1-c) que $\mathbb{Q}[\alpha]$ est de dimension au plus 4 sur $\mathbb{Q}$. Ceci montre que $\mathbb{Q}[\alpha]$ est de dimension 4, de base $(1,\sqrt{2},\sqrt{3},\sqrt{6})$.
Remarque : $(1,\alpha,\alpha^2,\alpha^3)$ est aussi une base de $\mathbb{Q}[\alpha]$.

f. Si α était racine d'un polynôme de degré au plus 3 de $\mathbb{Q}[X]$, la même preuve qu'à la question 1-c) montrerait que $\mathbb{Q}[\alpha]$ serait de dimension au plus 3, ce qui n'est pas le cas. Si le polynôme M_α était réductible, α serait racine d'un de ses diviseurs non triviaux, ce qui n'est pas le cas. Cela conclut.
Remarque : cela confirme que M_α n'a pas de racine rationnelle.

g. Pour tout $x, y \in \mathbb{Q}[\alpha]$ et tout $\lambda, \mu \in \mathbb{Q}$, on a $f_\alpha(\lambda x+\mu y) = \alpha(\lambda x+\mu y) = \lambda f_\alpha(x)+\mu f_\alpha(y)$. L'application f_α est bien $\mathbb{Q}$-linéaire. Un calcul immédiat donne :

$$\mathrm{mat}_{(1,\sqrt{2},\sqrt{3},\sqrt{6})} f_\alpha = \begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

puis le polynôme caractéristique de cette matrice vaut $X^4 - 10X^2 + 1$, c'est M_α.
On sait que le polynôme minimal de f_α divise le polynôme caractéristique, qui est irréductible. Donc le polynôme minimal de f_α est M_α.

2. a. On a vu que $\sqrt{2} + \sqrt{3}$ annule $X^4 - 10X^2 + 1$, donc c'est un entier algébrique.

Notons $\beta = \frac{\sqrt{3}+\sqrt{7}}{2}$. On a $(2\beta)^2 = 10 + 2\sqrt{21}$, donc $(4\beta^2 - 10)^2 = 84$. Cela donne $16\beta^4 - 80\beta^2 + 16 = 0$, donc $\beta^4 - 5\beta^2 + 1 = 0$. Cela montre que β est un entier algébrique.
On a $\frac{1+i\sqrt{3}}{2} = e^{i\frac{\pi}{3}}$, donc $\frac{1+i\sqrt{3}}{2}$ annule le polynôme $X^6 - 1$. C'est un entier algébrique.

b. Notons $\gamma = \frac{\sqrt{2}+\sqrt{3}}{2}$. On a vu que $\alpha = \sqrt{2} + \sqrt{3}$ annule le polynôme $X^4 - 10X^2 + 1$, donc γ annule le polynôme $16X^4 - 40X^2 + 1$. Supposons que γ annule un polynôme P unitaire à coefficients entiers. La division euclidienne de P par $16X^4-40X^2+1$ dans $\mathbb{Q}[X]$ s'écrit $P(X) = (16X^4 - 40X^2 + 1)Q(X) + R(X)$, avec $R(X)$ de degré au plus 3. Comme $\gamma = 2\alpha$ annule le reste $R(X)$, α annule le polynôme $R(2X)$ de degré au plus 3, donc nul. Ainsi $R = 0$ et $P(X) = (16X^4 - 40X^2 + 1)Q(X)$. Écrivons $Q(X) = a_n X^n + ... + a_0$. Le terme de degré 0 dans le produit donne que $a_0 \in \mathbb{Z}$. Le terme de degré 1 donne $a_1 \in \mathbb{Z}$, le terme de degré 2 donne $-40a_0 + a_2 \in \mathbb{Z}$, donc $a_2 \in \mathbb{Z}$. Une récurrence jusqu'au coefficient $a_n - 40a_{n-2} + 16a_{n-4}$ d'ordre n montre que tous les coefficients de Q sont entiers. Mais alors le coefficient dominant $16a_n$ de $(16X^4 - 40X^2 + 1)Q(X)$ est divisible par 16, ce qui contredit le fait que P est unitaire.
Remarque : le raisonnement usuel dans cette situation utilise le contenu $c(P)$ d'un polynôme P à coefficients entiers, qui est défini comme le pgcd des coefficients de P. Il a la propriété d'être multiplicatif : $c(QR) = c(Q)c(R)$ pour tous polynômes à coefficients entiers Q et R. On en déduit facilement que si on a $P = QR$ avec $P, Q \in \mathbb{Z}[X]$, $R \in \mathbb{Q}[X]$ et $c(P) = c(Q) = 1$, alors $R \in \mathbb{Z}[X]$ (multiplier par le plus petit dénominateur commun des coefficients de R).

Partie II

1. a. L'ensemble $\mathcal{I}(\alpha)$ contient le polynôme nul. Soient $P, Q \in \mathcal{I}(\alpha)$, $R, S \in K[X]$. On a $(RP + QS)(\alpha) = R(\alpha)P(\alpha) + S(\alpha)Q(\alpha) = 0$, ce qui montre que $\mathcal{I}(\alpha)$ est un idéal.
Remarque : pour aller vite, on peut aussi dire que $\mathcal{I}(\alpha)$ est le noyau du morphisme d'anneau $P \mapsto P(\alpha)$ (on peut admettre que c'est un morphisme).
Comme $K[X]$ est un anneau principal, l'idéal $\mathcal{I}(\alpha)$ est engendré par un polynôme P. Comme α est algébrique, $\mathcal{I}(\alpha)$ n'est pas réduit à $\{0\}$, donc $P \neq 0$. Les polynômes qui engendrent l'idéal $\mathcal{I}(\alpha)$ sont les multiples de P par les inversibles de $K[X]$, les polynômes constants, et comme il y a un unique polynôme unitaire M_α multiple de P par un réel, cela conclut.

b. Soit P unitaire, irréductible s'annulant en α. Par définition $P \in \mathcal{I}(\alpha)$, donc M_α divise P. Or P est irréductible et M_α est degré au moins 1, donc P et M_α sont multiples l'un de l'autre par un réel non nul. Comme ils sont tous les deux unitaires, ils sont égaux.
La réciproque est évidente.

2. i) $\Rightarrow$ iii) est évident.
iii) $\Rightarrow$ i) : $\alpha \in K[\alpha] = K$.
i) $\Rightarrow$ ii) : $M_\alpha(X) = X - \alpha$ (polynôme irréductible).
ii) $\Rightarrow$ i) : si $M_\alpha(X) = X - a \in K[X]$, on a $\alpha = a \in K$.

3. **a.** Le même raisonnement qu'en première partie montre que $K[\alpha]$ est un corps (division euclidienne par M_α) et a pour base $(1, \alpha)$, donc $\dim_K(K[\alpha]) = 2$.

b. α est racine *réelle* d'une équation algébrique de degré 2 de la forme $\alpha^2 - s\alpha + p = 0$, s et p étant éléments de K, donc réels. Dans ces conditions, α s'exprime dans $\mathbb{R}$ par la formule $\alpha = \frac{s \pm \sqrt{k}}{2}$, avec $k = s^2 - 4p \in K_+$. Ceci nous pousse à examiner $\delta = 2\alpha - s \in K[\alpha]$; on a $\delta^2 = 4\alpha^2 - 4s\alpha + s^2 = s^2 - 4p = k$, soit bien $\delta = \sqrt{k}$. En conséquence, on a $\sqrt{k} \subset K[\alpha]$, donc, puisque $K[\alpha]$ est un anneau, $K[\sqrt{k}] \subset K[\alpha]$. On a évidemment $\alpha \in K[\sqrt{k}]$, d'où l'égalité par le même principe.

Remarque : dans le vocabulaire de la théorie de Galois, on dit que toute extension quadratique réelle est une extension radicale. La restriction de α à être réel n'est pas fondamentale, et a été placée tout au long du problème pour simplifier les raisonnements en évitant d'avoir à choisir des racines complexes.

4. **a.** La division euclidienne d'un polynôme $P \in K[X]$ par M_α montre que tout élément de $K[\alpha]$ s'écrit sous la forme $R(\alpha)$ avec $\deg R \leq n-1$, c'est-à-dire comme une combinaison linéaire à coefficient dans K de $(1, \alpha, \ldots, \alpha^{n-1})$. Si $R(\alpha) = S(\alpha)$ avec $\deg R, \deg S \leq n-1$, alors $R - S$ s'annule en α. Donc $R - S$ est multiple du polynôme M_α, et le degré fait que $R - S = 0$. Cela montre l'unicité de R.
Par définition, l'unicité de l'écriture d'un élément de $K[\alpha]$ comme une combinaison linéaire de $(1, \alpha, \ldots, \alpha^{n-1})$ montre que $(1, \alpha, \ldots, \alpha^{n-1})$ est une base de $K[\alpha]$. Ainsi $\dim_K K[\alpha] = n$.

b. On a $\deg R \leq n-1$ et M_α est irréductible, donc $\operatorname{pgcd}(R, M_\alpha) = 1$. L'identité de Bezout montre, comme dans la première partie, l'existence de U.

c. On sait déjà que $K[\alpha]$ est un anneau. L'inversibilité des éléments non nuls de $K[\alpha]$ résulte de la question précédente.

d. On a déjà montré que $K[\alpha]$ est un corps, il contient α, K et est contenu dans $\mathbb{R}$. De plus tout anneau contenant α doit contenir $K[\alpha]$ (propriété déjà utilisée ci-dessus). Cela montre la question.

5. [Polynômes de Tchebycheff modifiés]

a. On a :
$P_2(X) = 4X^2 + 2X - 1$, $P_3(X) = 8X^3 + 4X^2 - 4X - 1$, $P_4(X) = 16X^4 + 8X^3 - 12X^2 - 4X + 1$.
Les polynômes Q_n vérifient la relation de récurrence $Q_{n+1} = XQ_n - Q_{n-1}$, avec $Q_0 = 1$ et $Q_1 = X + 1$. Des récurrences immédiates montrent que $\deg Q_n = n$, $Q_n \in \mathbb{Z}[X]$, Q_n unitaire, $Q_n(0) = 1$ si $n \equiv 0$ ou $n \equiv 1 \bmod 4$, $Q_n(0) = -1$ sinon ; soit $Q_n(0) = (-1)^{\frac{n(n-1)}{2}}$. On en déduit que $\deg P_n = n$, P_n a pour coefficient dominant 2^n et $P_n(0) = (-1)^{\frac{n(n-1)}{2}}$.

b. Le même raisonnement qu'en première partie montre que si $\frac{a}{b} \in \mathbb{Q}$, avec $a \wedge b = 1$, est racine d'un polynôme $P = \sum_{i=0}^{n} a_i X^i$ à coefficients entiers, alors son numérateur a qui divise le coefficient constant a_0 et son dénominateur b divise le coefficient dominant a_n. Les polynômes Q_n étant unitaires à coefficients constants égaux à ± 1, on a ici $a = \pm 1$ et $b = \pm 1$. Cela montre que les seules racines rationnelles possibles de Q_n sont ± 1.
La relation de récurrence qui définit les Q_n montre que

$$Q_{n+3} + XQ_n = XQ_{n+2} - Q_{n+1} + XQ_n = X^2 Q_{n+1} - XQ_n - Q_{n+1} + XQ_n = (X^2 - 1)Q_{n+1}\,.$$

Dès lors, Q_n et Q_{n+3} ont les mêmes racines parmi 1 et -1.
D'autre part, on a $Q_0 = 1, Q_1 = X + 1, Q_2 = X^2 + X - 1$. Seul Q_1 a une racine rationnelle qui est -1 ; donc seuls les Q_{3k+1} ont une racine rationnelle, qui vaut -1. Dès lors, seuls les P_{3k+1} ont une racine rationnelle, qui est $-\frac{1}{2}$.

6. a. L'équation caractéristique de la relation de récurrence est $r^2 - 2r\cos(\theta) + 1 = 0$, qui a pour racine $e^{i\theta}$ et $e^{-i\theta}$. Les suites réelles vérifiant la relation de récurrence sont donc de la forme $\lambda\cos(n\theta) + \mu\sin(n\theta)$. En appliquant à $n = 0$ et $n = 1$, on obtient

$$u_n = u_0\cos(n\theta) + \frac{u_1 - u_0\cos(\theta)}{\sin(\theta)}\sin(n\theta).$$

b. La suite $(P_n(\cos(\theta)))_{n\in\mathbb{N}}$ vérifie la relation de récurrence de la question précédente avec $u_0 = 1$ et $u_1 = 2\cos(\theta) + 1$. Cela donne (on peut simplifier le résultat avec un formule trigonométrique) :

$$P_n(\cos\theta) = \frac{\sin((n+1)\theta) + \sin(n\theta)}{\sin(\theta)} = \frac{\sin(2n+1)\frac{\theta}{2}}{\sin\frac{\theta}{2}}.$$

Ce polynôme s'annule pour $\theta \in]0, \pi[$ lorsque $\sin(2n+1)\frac{\theta}{2} = 0$, soit $\theta = \frac{2k\pi}{2n+1}$ (pour n valeurs de $k : 1 \leq k \leq n$) ce qui donne n racines réelles distinctes de P_n qui sont $x_{k,n} = \cos\frac{2k\pi}{2n+1}$ avec $1 \leq k \leq n$.

c. Le nombre $\cos\frac{2\pi}{5}$ est donc racine de $P_2 = 4X^2 + 2X - 1$ donc algébrique sur $\mathbb{Q}$ et de degré 2 car non rationnel (voir question 5b). Ainsi, $\frac{1}{4}P_2$ est polynôme minimal de $\cos\frac{2\pi}{5}$.
Le nombre $\cos\frac{2\pi}{7}$ est racine de $P_3 = 8X^3 + 4X^2 - 4X - 1$ donc algébrique sur $\mathbb{Q}$ et de degré 3 au plus. Enfin, P_3 n'a pas de racine rationnelle (question 5b), donc ne peut aucunement se factoriser sur $\mathbb{Q}$; il est irréductible donc $\frac{1}{8}P_3$ est le polynôme minimal de $\cos\frac{2\pi}{7}$, qui est finalement de degré 3.
Le nombre $\cos\frac{2\pi}{9}$ est racine de P_4 donc algébrique sur $\mathbb{Q}$ et de degré 4 au plus. Mais, P_4 a une racine rationnelle (question 5b), et va se factoriser en produit d'un polynôme de degré 3 et d'un polynôme de degré 1. On obtient $P_4 = (2X + 1)(8X^3 - 6X + 1)$. Le polynôme $8X^3 - 6X + 1$ n'a pas de racine rationnelle, sinon ce serait $\pm\frac{1}{2}$ mais ce n'est pas le cas, donc il est irréductible sur $\mathbb{Q}$; par conséquent, le polynôme minimal de $\cos\frac{2\pi}{9}$ est $\frac{1}{8}(8X^3 - 6X + 1)$, et le degré de ce nombre algébrique est bien 3.
Remarque : historiquement, les Grecs d'Alexandrie, dont Euclide, furent très préoccupés de la difficulté apparente de construire certains objets géométriques à la règle et au compas. Faute de trouver des solutions explicites et de pouvoir démontrer les impossibilités qu'on verra au II (deux millénaires plus tard !), ils imaginèrent de faire appel à des tracés nouveaux, comme la Cissoïde de Dioclès ou la Conchoïde de Nicomède. Ces courbes leur permirent de réaliser la "trissection" de l'angle, donc de "construire" l'ennéagone (9 côtés), ou de "dupliquer le cube". De telles idées furent incorporées bien plus tard, par Abel, dans le cadre de la Théorie des Groupes et de la Géométrie Algébrique.

7. a. On vient de voir que le degré de $\alpha = \cos\frac{2\pi}{9}$ sur $\mathbb{Q}$ est 3 ; le théorème du cours montre qu'alors $(1, \alpha, \alpha^2)$ est base de $\mathbb{Q}[\alpha]$ sur $\mathbb{Q}$. On calcule aisément les trois racines non rationnelles de P_4, donc de $8X^3 - 6X + 1$, ce sont $\alpha = \cos\frac{2\pi}{9}$, $\beta = 2\alpha^2 - 1 = \cos\frac{4\pi}{9}$ et $\gamma = -\alpha - 2\alpha^2 + 1 = \cos\frac{8\pi}{9}$, car la somme des racines de $N = 8X^3 - 6X + 1$ est nulle.

b. La multiplicativité de f montre que $f(1) = f(1)^2$; si $f(1) = 0$, alors $f(x) = f(x.1) = f(x)f(1) = 0$; l'auteur du sujet a oublié l'application nulle ! Sinon, on a $f(1) = 1$ et f est un endomorphisme de corps ; il est donc injectif et même bijectif par $\mathbb{Q}$-linéarité.

Le caractère morphique de f fait que la relation $8\alpha^3 - 6\alpha + 1 = 0$ se transfère à $f(\alpha)$; en somme, f permute les racines de $8X^3 - 6X + 1$. Il y a a priori six permutations possibles, mais on va voir que seules les permutations paires conviennent. En effet, si on avait (par exemple) $f(\alpha) = \alpha$, alors $f(\alpha^2) = f(\alpha)^2 = \alpha^2$ donc par linéarité f est l'application identité sur $\mathbb{Q}[\alpha]$. Pareillement, si $f(\alpha^2) = \alpha^2$ alors $f(\alpha^4) = \alpha^4$; or, $8\alpha^4 = 6\alpha^2 - \alpha$, donc $f(\alpha) = \alpha$. Ainsi, f fixe les trois racines du polynôme minimal, ou n'en fixe aucune. Il ne reste que deux possibilités non triviales (et mutuellement réciproques) : $\alpha \to \beta \to \gamma$ et $\alpha \to \gamma \to \beta$.
L'étude précédente laisse de côté le problème de l'existence de ces endomorphismes. Définissons d'abord f tel que $f(\alpha) = \beta$. Il est nécessaire que $f(\alpha^2) = \beta^2$. Réciproquement, la formule $f(x + y\alpha + z\alpha^2) = x + y\beta + z\beta^2$ définit-elle un morphisme d'anneaux ? Pour ce vérifier, il suffit de le tester sur les éléments de la base (à cause de la linéarité). Le calcul revient à vérifier que $f(\alpha^p) = f(\beta^p)$. On divise X^p par $N : X^p = NQ + R$, le reste étant de degré 2 au plus : $R = uX^2 + vX + w$. On a donc $\alpha^p = N(\alpha)Q(\alpha) + u\alpha^2 + v\alpha + w = u\alpha^2 + v\alpha + w$ et aussi $\beta^p = N(\beta)Q(\beta) + u\beta^2 + v\beta + w = u\beta^2 + v\beta + w$. Dès lors, on a $f(\alpha^p) = uf(\alpha^2) + vf(\alpha) + w = u\beta^2 + v\beta + w = \beta^p$.
En conclusion, il y a trois automorphismes du corps $\mathbb{Q}[\alpha]$, définis par les trois permutations paires des racines du polynôme minimal de α.
Les matrices se calculent aisément ; par exemple, f telle que $f(\alpha) = \beta = 2\alpha^2 - 1$ vérifie $f(\alpha^2) = (2\alpha^2 - 1)^2 = 4\alpha^4 - 4\alpha^2 + 1 = (8\alpha^3 - 6\alpha + 1)\frac{\alpha}{2} - \alpha^2 - \frac{\alpha}{2} + 1$ (à vérifier) et a pour matrice $\begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & -\frac{1}{2} \\ 0 & 2 & -1 \end{pmatrix}$. L'autre automorphisme non identique a une matrice inverse de celle-ci.

8. [Approximations rationnelles d'un nombre algébrique réel selon Liouville]

a. Soit $S(x) = s_n x^n + \cdots + s_0$ avec $s_n \neq 0$ et les s_k dans $\mathbb{Q}$, irréductible sur $\mathbb{Q}$. Quitte à multiplier S par le ppcm des dénominateurs des s_i, que nous noterons C_S, on peut remplacer S par une polynôme S_0 proportionnel et à coefficients entiers. Comme S_0 est irréductible, il n'a pas de racine rationnelle. On a donc $S_0(\frac{p}{q}) = \frac{N}{q^n} \neq 0$, N étant un certain entier non nul. Par conséquent, $|S_0(\frac{p}{q})| \geq \frac{1}{q^n}$ et donc $|S(\frac{p}{q})| \geq \frac{1}{C_S q^n}$.

b. Soit α algébrique de degré $n \geq 2$, zéro de S.
Considérons à présent la restriction de S à l'intervalle $[\alpha - 1, \alpha + 1]$; sa dérivée y reste bornée, donc on grâce au théorème des Accroissements Finis une condition de Lipschitz pour S qui s'écrit $|S(x) - S(y)| \leq M|x - y|$. Considérons ensuite une approximation $\frac{p}{q}$ de α, telle que $\frac{p}{q} \in [\alpha - 1, \alpha + 1]$ (pour q assez grand c'est possible). On a $|S(\frac{p}{q})| \geq \frac{1}{C_S q^n}$ et donc $M|\alpha - \frac{p}{q}| \geq |S(\frac{p}{q}) - S(\alpha)| \geq \frac{1}{C_S q^n}$, soit $|\alpha - \frac{p}{q}| \geq \frac{K}{q^n}$, avec $K = \frac{1}{MC_S}$.

c. Une inégalité $\frac{C}{q^{n+1}} \geq \frac{K}{q^n}$ ne peut avoir lieu pour une infinité d'entiers q. On a alors la conséquence suivante : Pour prouver qu'un réel non rationnel t est transcendant, il suffit de vérifier que, pour tout $n \geq 1$, il existe une infinité de rationnels $\frac{p}{q}$ avec $q > 0$ et (p, q) premiers entre eux, tels que l'on ait $|t - \frac{p}{q}| \leq \frac{1}{q^{n+1}}$.

Étant donné un entier $p \geq 2$, on appelle nombre de Liouville tout réel somme d'une série de terme général $\frac{a_n}{p^{n!}}$ avec les a_n entiers compris entre 0 et $p - 1$, non tous nuls à partir d'un certain rang. Une telle série converge aisément (majorer par une série géométrique). On va prouver que tout nombre de Liouville est transcendant.

Soit un nombre de Liouville $t = \sum_{n=0}^{\infty} \frac{a_n}{p^{n!}}$. En posant $s_n = \sum_{k=0}^{n} \frac{a_k}{p^{k!}}$, on a

$$|t - s_n| = \sum_{k=n+1}^{\infty} \frac{a_k}{p^{k!}} \leq (p-1) \sum_{k=n+1}^{\infty} \frac{1}{p^{k!}} = \frac{p-1}{p^{(n+1)!}} \sum_{k=n+1}^{\infty} \frac{1}{p^{k!-(n+1)!}} \leq \frac{p-1}{p^{(n+1)!}} \sum_{k=n+1}^{\infty} \frac{1}{p^{k-n-1}} = \frac{1}{p^{(n+1)!-1}}$$

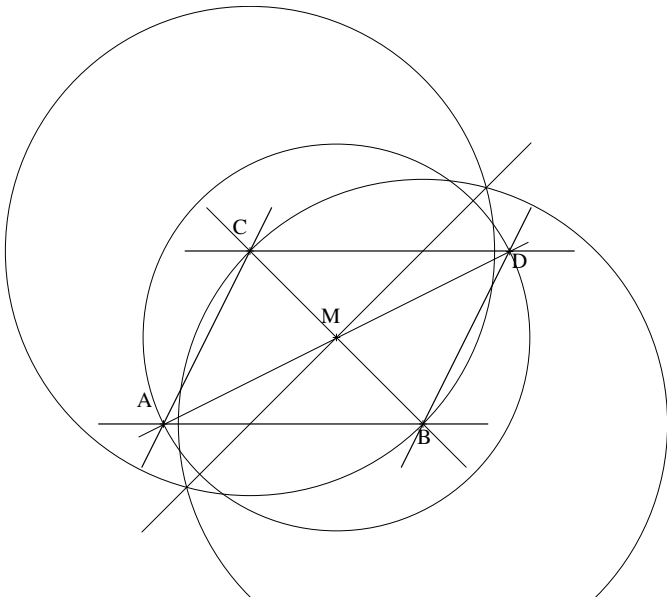
et par suite t est transcendant.

Partie III

1. *Droite de $\mathcal{D}$:* on a l'équation $(x - x_1)(y_2 - y_1) = (y - y_1)(x_2 - x_1)$ qui a ses coefficients dans K.
Cercle de $\mathcal{C}$: on a l'équation $(x-x_0)^2+(y-y_0)^2 = (x_1-x_2)^2+(y_1-y_2)^2$ qui a ses coefficients dans K.
Intersection de droites de $\mathcal{D}$: un système linéaire a ses solutions qui répondent aux formules de Cramer, qui sont rationnelles par rapport aux coefficients, donc restent dans K.
Intersection de droite et de cercle : on confronte $x^2+y^2-2ax-2by+c = 0$ $(a, b, c \in K)$ avec $y = mx+p$ $(m, p \in K)$. On en tire une équation du second degré $x^2+(mx+p)^2-2ax-2b(mx+p)+c = 0$, dont les deux solutions appartiennent à une extension quadratique de K, selon la question I3. Il se peut qu'il n'y ait qu'une racine (double : cercle et droite tangents) ; alors le discriminant est nul et la racine reste dans K. L'abscisse ayant été "calculée", l'ordonnée s'en déduit par $y = mx + p$, ce qui reste dans K ou dans l'extension quadratique dont on vient de parler.
Intersection de cercles : on confronte $x^2 + y^2 - 2ax - 2by + c = 0$ $(a, b, c \in K)$ avec $x^2 + y^2 - 2a'x - 2b'y + c' = 0$ $(a', b', c' \in K)$. Cela revient à $x^2 + y^2 - 2ax - 2by + c = 0 = 2(a - a')x + 2(b - b')y - (c - c')$, et on est ramenés au cas précédent (en fait, on trace l'axe radical des deux cercles). Donc les deux points d'intersection ont des coordonnées dans une extension quadratique de K ou dans K si les deux cercles sont tangents.

2. a. On construit le quatrième sommet du parallélogramme de la manière suivante (ce n'est pas la seule, mais elle a l'avantage de rester valide lorsque les points sont alignés) : on trace le cercle de centre C et de rayon BC ; puis le cercle de centre B et de même rayon ; ils se coupent en deux points M, P ; on trace la droite (MP) et la droite (BC) qui se coupent au milieu Q du segment $[B, C]$ (et centre du parallélogramme). On trace la droite (AQ) et le cercle de centre Q, rayon AQ. Cette droite et ce cercle se coupent en A et en D que l'on cherche.

Si A et Δ sont tracés, c'est que sur Δ il y a deux points B et C déjà tracés. On construit le parallélogramme $ABCD$, de sorte que la droite (AD) est la parallèle cherchée.



b. On obtient J par l'intersection de (OI) et du cercle de centre O passant par I. Les cercles de centres I et J et de même rayon IJ se coupent en deux point F, G ; la droite (FG) est l'axe des ordonnées et coupe le tout premier cercle en K et L.

Pour construire la somme de deux nombres réels constructibles, il suffit d'appliquer la méthode vue ci-dessus au parallélogramme (aplati) formé par les points d'abscisses $0, \alpha, \beta$ et $\alpha+\beta$, et ordonnées nulles. Pour construire produits, inverses, racines, on va placer des cercles passant par trois points déjà tracés (on sait construire : le centre provient de l'intersection de deux médiatrices), et intersecter ces cercles avec l'un des axes. A cet effet, nous servira le résultat suivant :

lemme : *Si un cercle du plan complexe coupe l'axe réel en des points d'affixes a, b et l'axe imaginaire pur en des points d'affixes ic, id, alors on a $ab = cd$.*

Le cercle a une équation qu'on peut écrire $x^2 + y^2 - 2ux - 2vy + w = 0$. L'intersection avec l'axe Ox amène l'équation $x^2 - 2ux + w = 0$, donc $w = ab$. L'intersection avec l'axe Oy amène l'équation $y^2 - 2vy + w = 0$, donc $w = cd$, ce qu'il fallait !

Produits : considérer le cercle passant par les points $A = (\alpha, 0); B = (\beta, 0); K = (0, 1)$. Il recoupe l'axe des ordonnées en un point de coordonnées $(0, c)$; d'après le Lemme on a $\alpha\beta = 1 \times c$. Il suffit de ramener ce point sur l'axe des abscisses par un cercle de centre O et le tour est joué.

Inverses : considérer le cercle passant par les points de coordonnées $A = (\alpha, 0); K = (0, 1); L = (0, -1)$. Il recoupe l'axe des abscisses en un point de coordonnées $(c, 0)$; d'après le Lemme on a $\alpha c = 1 \times (-1) = -1$. Il suffit de faire subir au point $(c, 0)$ un demi-tour de centre O pour obtenir $(\frac{1}{a}, 0)$.

Quotients : combinaison des deux méthodes précédentes.

Racines : considérer le cercle de diamètre AJ, passant par les points de coordonnées $A = (\alpha, 0); J = (-1, 0); M = (0, c); N = (0, -c)$; d'après le Lemme on a $\alpha \times (-1) = c \times (-c)$ soit $c = \sqrt{\alpha}$. Il suffit de ramener le point $(0, c)$ sur l'axe des abscisses par un cercle de centre O et la construction est achevée.

3. a. Si M est un point constructible, il est atteint à la suite de la construction de points intermédiaires M_i.

On passe de M_0 et M_1 à M_2 en appliquant l'une des règles prescrites, c'est-à-dire en traçant la droite qui les joint, et un ou deux cercles de centre M_0 ou M_1, puis en intersectant la droite et un cercle, ou les deux cercles. Il résulte par la question 1 que les coordonnées de M_2 sont dans K_2, extension quadratique de $K_1 = \mathbb{Q}$.
Supposons que les points $M_2, \ldots, M_i$ aient leurs coordonnées dans un corps K_i. Le prochain point peut réclamer le tracé de droites joignant certains des M_j déjà trouvés, et les coefficients de leurs équations restent dans K_i ; il peut aussi réclamer le tracé de cercles centrés sur certains des M_j et ayant un rayon égal à la distance de deux des M_i. Les coefficients des équations de ces cercles restent encore dans K_i (question 1 toujours). Donc tous les éléments "intermédiaires" de la construction restent dans K_i. Le passage final est une intersection, qui peut se faire "dans K_i", ou sinon réclamer le passage à une extension quadratique K_{i+1} de K_i. Dans le premier cas, on pose tout simplement $K_{i+1} = K_i$.
La récurrence fonctionne donc et prouve que tout point constructible a ses coordonnées dans le "sommet" d'une "pile d'extensions quadratiques" de $\mathbb{Q}$.

b. Soit une pile (K_i) d'extensions quadratiques. Les éléments du premier sont constructibles : il s'agit des nombres rationnels, constructibles comme quotients d'entiers selon II2b. Supposons que les éléments de K_i soient tous constructibles. Ceux de $K_{i+1} = K_i[\sqrt{k_i}]$ peuvent s'écrire sous la forme $x + y\sqrt{k_i}$, x, y, k_i étant dans K_i. On construit $\sqrt{k_i}$ comme indiqué au II2b, puis le produit $y\sqrt{k_i}$ de même, enfin la somme suivant le procédé prévu. En conséquence, tout élément de K_{i+1} est constructible.

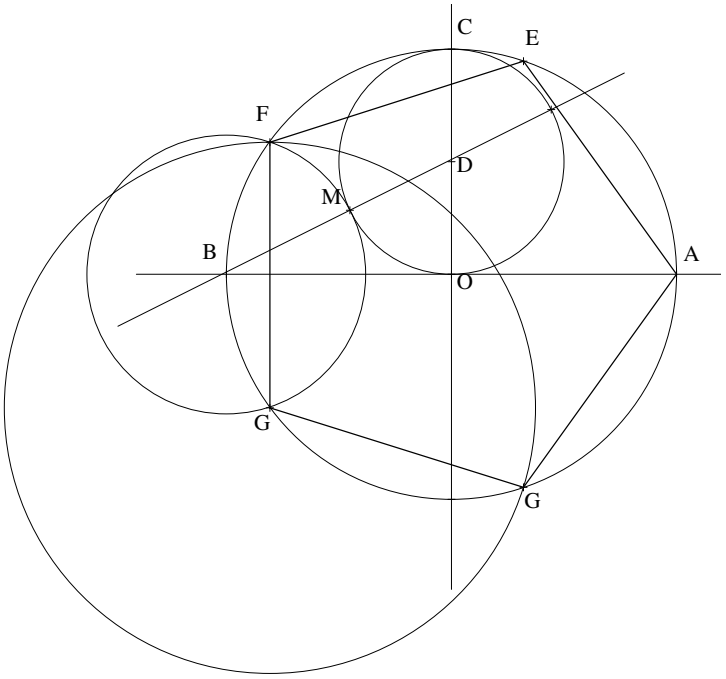
4. a. On suppose que G est une extension de dimension finie sur F et que H est une extension de dimension finie sur G. Montrons que H est une extension de dimension finie sur F.
On considère une base (x_i) de G sur F et une base (y_j) de H sur G, avec $\dim_F G = q$ et $\dim_G H = r$. Soit un élément x de G ; on peut écrire : $x = \sum_{j=1}^{r} \lambda_j y_j$ et l'on peut développer chaque λ_j (qui est dans G sur F, soit : $\lambda_j = \sum_{i=1}^{q} \gamma_{ij} x_i$ avec $\gamma_{ij} \in F$ et donc $x = \sum_{j=1}^{r} \sum_{i=1}^{q} \gamma_{ij} x_i y_j$; donc la famille $(x_i y_j)$ est génératrice de H sur le corps de base F et elle possède bien qr éléments ; elle est libre car si $\sum_{j=1}^{r} \sum_{i=1}^{q} \gamma_{ij} x_i y_j = 0$ alors chaque $\sum_{i=1}^{q} \gamma_{ij} x_i$ est nul par indépendance des y_j et ceci entraîne la nullité des γ_{ij} par l'indépendance des x_i. C'est une base et l'on a $\dim_F H = qr = \dim_F G . \dim_G H$.
Remarque : : en théorie des corps, cette dimension s'appelle le *degré* de l'extension.

b. Lorsque l'on passe d'un corps K_i à une extension quadratique, la dimension sur $\mathbb{Q}$ double d'après la question précédente. Si on a plutôt $K_i = K_{i+1}$ alors la dimension ne change pas. Ainsi, la dimension de K_n, "sommet" d'une pile d'extension quadratiques (strict) vaut 2^n, et s'il y a des corps identiques dans la pile, la dimension du sommet est une puissance de 2, inférieure ou égale à 2^n.

c. Il résulte des études précédentes que si α est constructible, le point de coordonnées $(\alpha, 0)$ l'est, et donc α appartient à un sommet K_n d'une pile d'extensions quadratiques de $\mathbb{Q}$. On peut donc considérer la chaîne de corps : $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset K_n$; la formule de multiplicativité des dimensions va donner $\deg_{\mathbb{Q}} \alpha \times \dim_{\mathbb{Q}[\alpha]} K_n = 2^p$; ainsi, $\deg_{\mathbb{Q}} \alpha$ divise une puissance de 2, donc est une puissance de 2.

5. Il s'agit de voir quels sont les nombres de la forme $\cos \frac{2\pi}{n}$ qui sont algébriques sur $\mathbb{Q}$ (tous, on l'a vu au I), et quels sont ceux dont le degré est une puissance de 2. Il est à noter que la condition sur le degré n'est pas a priori suffisante, elle est seulement nécessaire.
De fait, seul $\cos \frac{2\pi}{5}$ convient à ce point de vue. On sait donc construire les polygones à $3, 4, 6$ côtés (élémentaire), à 5 côtés (on vient de le voir au plan théorique), à 8 et 10 côtés (par

bissectrices). les polygones à 7 et 9 côtés ne sont sûrement pas constructibles puisque 3 n'est pas une puissance de 2.
Remarque : : Gauss a démontré que pour qu'un polygone régulier à n côtés soit constructible, il suffit que les facteurs primaires de n, de la forme p^r, avec p premier supérieur à 2, soient tels que p soit un nombre de Fermat $(2^{2^n}+1)$ et que r soit égal à 1 (à vérifier). Il existe une construction (compliquée, due à Erchinger) du polygone à 17 côtés, car on a



$$\cos\frac{\pi}{17}=\frac{1}{16}\left[1-\sqrt{17}+\sqrt{34-2\sqrt{17}}+\sqrt{68+12\sqrt{17}}+16\sqrt{34+2\sqrt{17}}-2(\sqrt{17}-1)\sqrt{34-2\sqrt{17}}\right]$$

Il y a de même une construction du polygone à $2^8+1=257$ *côtés, et de même pour* $2^{16}+1=65537$. *En revanche,* $2^{32}+1=4294967297$ *n'est pas premier, il est divisible par 641 (selon Euler).*
En fin de compte, une liste plus étendue des polygones constructibles serait :

$$3,4,5,6,8,10,12,15,16,17,20,24,25,30,32,34,40,48,51,60,64,68,80\ldots$$