Extensions de corps et constructions géomètriques

Julia PHAM BA NIEN

30 décembre 2023

Table des matières

1 Extensions d'anneaux

1.1 Introduction aux extensions

Dans cette section une certaine familiarité mathématique sera attendu.
Dans tout cet article, $\mathbb{K}$ sera un anneau quelconque.

Définition 1 (Extension de $\mathbb{K}$)**.** *On a $\mathbb{L}$ extension de $\mathbb{K}$ si $\mathbb{L}$ est un $\mathbb{K}$-module.*

Dans tout cet article, $\mathbb{L}$ sera une extension de K.

Définition 2 (degré d'une extension $\mathbb{L}$ de $\mathbb{K}$)**.** *C'est* $\dim_{\mathbb{K}}(\mathbb{L})$ *et se note* $[\mathbb{L} : \mathbb{K}]$

Définition 3 (extension de $\mathbb{K}$ par éléments)**.** *Soit x_1, ..., x_n des éléments d'un anneau $\mathbb{H}$, on note $\mathbb{K}[x_1, \ldots, x_n]$ l'anneau étant l'intersection de tous les anneaux contenant $\mathbb{K}$ et $x_1, \ldots, x_n$ coincidant avec $\mathbb{K}$ sur $\mathbb{K}$ et avec $\mathbb{H}$ sur $x_1, \ldots, x_n$.*

Dans tout cet article, X sera une indéterminé.

Définition 4 (extension de $\mathbb{K}$ par un ensemble)**.** *Dans la même veine, soit S sous ensemble de $\mathbb{H}$ un corp, on note $\mathbb{K}[S \ldots]$ l'anneau étant l'intersection de tout les anneaux contenant $\mathbb{K}$ et S coincidant avec $\mathbb{K}$ sur $\mathbb{K}$ et avec $\mathbb{H}$ sur S.*

Définition 5 (Nombres $\mathbb{K}$-algèbriques)**.** *Soit x un élément d'une extension de $\mathbb{K}$, x est $\mathbb{K}$-algèbrique si et seulement si x est racine d'un élément de $\mathbb{K}[X]^*$*

Définition 6 (degré d'un nombre $\mathbb{K}$-algèbrique)**.** *Soit x $\mathbb{K}$-algèbrique, son degrè* $\deg(x) = \min\{\deg(P) | P \in \mathbb{K}[X]^* \wedge P(x) = 0\}$

Définition 7 (polynome minimal d'un nombre $\mathbb{K}$-algèbrique)**.** *Soit a un nombre $\mathbb{K}$-algèbrique, on dit que $P \in \mathbb{K}[X]$ est polynome minimal de a si* $\deg(P) = \deg(a)$ *et le coefficiant du plus haut degrè de P est* 1.

Définition 8 (Nombres $\mathbb{K}$-trancendants)**.** *Soit x un élément d'une extension de $\mathbb{K}$, x est $\mathbb{K}$-trancendants si et seulement si x n'est pas $\mathbb{K}$-algèbrique.*

Théorème 1 (produit de dimension d'extensions)**.** *Soit $(\mathbb{L}_i)_{0 \leq i \leq n}$ avec $\mathbb{L}_0 = \mathbb{K}$ et $\mathbb{L}_n = \mathbb{L}$ et $\forall i \in [0, n-1], \mathbb{L}_{i+1}$ est un $\mathbb{L}_i$-module,*

$$[\mathbb{L} : \mathbb{K}] = \prod_{i=0}^{n-1} [\mathbb{L}_{i+1} : \mathbb{L}_i]$$

Démonstration. récurrence sur la taille de n
Initialisation (n=0, n=1) trivial.
Hérédité :
Soit $n \in \mathbb{N}^*$, supposons que $[\mathbb{L}_n : \mathbb{L}_0] = \prod_{i=0}^{n-1} [\mathbb{L}_{i+1} : \mathbb{L}_i]$.
On va supposer que toutes les dimensions sont finis (c'est trivial quand une dimension est infini)

Posons $A = \mathbb{L}_{i+1}$, $B = \mathbb{L}_i$ et $C = \mathbb{L}_0$
Posons $a = [A : B]$ et $b = [B : C]$.
Soit $\{a_1, \ldots, a_a\}$ un base A sur B et $\{b_1, \ldots, b_b\}$ un base de B sur C.
Montrons que $(a_i b_j)_{1 \leq i \leq a, 1 \leq j \leq b}$ forme une de A sur C.
Montrons que $(a_i b_j)_{1 \leq i \leq a, 1 \leq j \leq b}$ est un système libre, en effet, si :

$$\sum_{1 \leq i \leq a, 1 \leq j \leq b} x_{ij} a_i b_j = 0$$

alors :

$$\sum_{1 \leq i \leq a} a_i (\sum_{1 \leq j \leq b} x_{ij} b_j) = 0$$

donc pour tout $1 \leq i \leq j$,

$$\sum_{1 \leq j \leq b} x_{ij} b_j = 0$$

Donc tout les x_{ij} sont nuls, donc $(a_i b_j)_{1 \leq i \leq a, 1 \leq j \leq b}$ est libre.
Montrons que $(a_i b_j)_{1 \leq i \leq a, 1 \leq j \leq b}$ est générateur :
Soit $x \in A$,
comme $(a_i)_{1 \leq i \leq a}$ est générateur, il existe $(x_i)_{1 \leq i \leq a}$ tel que

$$x = \sum_{1 \leq i \leq a} a_i x_i$$

et comme $(b_j)_{1 \leq j \leq b}$ est générateur, les x_i peuvent s'écrire comme combinaison linéaire des b_j, donc il existe $(x_{ij})_{1 \leq i \leq a, 1 \leq j \leq b}$ tel que :

$$\begin{aligned} x &= \sum_{1 \leq i \leq a} a_i (\sum_{1 \leq j \leq b} x_{ij} b_j) \\ &(= \sum_{1 \leq i \leq a, 1 \leq j \leq b} a_i b_j x_{ij})) \end{aligned}$$

Donc $(a_i b_j)_{1 \leq i \leq a, 1 \leq j \leq b}$ est générateur.
Donc $(a_i b_j)_{1 \leq i \leq a, 1 \leq j \leq b}$ est une base.
Donc

$$\begin{aligned} [\mathbb{L}_{n+1} : \mathbb{L}_0] &= [A : C] \\ &= a \times b \\ &= [A : B][B : C] \\ &= [\mathbb{L}_{n+1} : \mathbb{L}_n][\mathbb{L}_n : \mathbb{L}_0] \\ &= [\mathbb{L}_{n+1} : \mathbb{L}_n] \prod_{i=0}^{n-1} [\mathbb{L}_{i+1} : \mathbb{L}_i] \\ &= \prod_{i=0}^{n} [\mathbb{L}_{i+1} : \mathbb{L}_i] \end{aligned}$$

On a l'initialisation et l'hérédité, donc la propriété.

1.2 Extensions algèbriques

On supposera maintenant que $\mathbb{K}$ est un corps.

Définition 9 (corps de rupture)**.** *Soit P polynome irréductible sur $\mathbb{K}$, et x une racine de P, alors on dit que $\mathbb{K}[x]$ est un corps de rupture.*

Théorème 2 (Corps d'extensions algèbriques)**.** *Si $\mathbb{K}$ est un corps et a est $\mathbb{K}$-algèbrique, alors $\mathbb{K}[a]$ est un corps.*

Démonstration. On a $\mathbb{K}[a]$ anneaux, il suffit donc de montrer que tout élément de $\mathbb{K}[a]^*$ est inversible.
Posons P le polynome minimal de a.
Posons $\phi : (\mathbb{K}[X])(\mathbb{K}[X] \setminus P\mathbb{K}[X])^{-1} \to \mathbb{K}(a)$ morphisme de corps définit par $\phi(X) = a$, $\forall x \in \mathbb{K}, \phi(x) = x$.
Il suffit donc de montrer que $\forall P \in \mathbb{K}(X), \phi(P) \in \mathbb{K}[a]$.
On a $\forall P \in (\mathbb{K}[X])(\mathbb{K}[X] \setminus P\mathbb{K}[X])^{-1}, \phi(P) \in \mathbb{K}[a]$.
Il suffit donc de montrer que $\forall P \in \mathbb{K}[X] \setminus P\mathbb{K}[X], \phi(\frac{1}{P}) \in \mathbb{K}[a]$.
Soit $Q \in \mathbb{K}[X] \setminus \mathbb{K}P$,
On a $Q(X) =: R(X)P(X) + W(X)$ avec $\deg(W) < \deg(P)$.
On a W et P copremier (on a $W \neq 0$ et ils ne peuvent pas avoir de racines en commun, cela contradirerait la minimalité de P pour ses racines).
Il existe donc $A, B \in \mathbb{K}[X]$ tel que $A(X)W(X) + B(X)P(X) = 1$.
Ainsi

$$\begin{aligned}
\phi(\frac{1}{Q(X)}) &= \phi(\frac{1}{R(X)P(X) + W(X)}) \\
&= \frac{1}{R(a)P(a) + W(a)} \\
&= \frac{1}{W(a)} \\
&= \frac{A(a)W(a) + B(a)P(a)}{W(a)} \\
&= \frac{A(a)W(a)}{W(a)} \\
&= A(a)(\in \mathbb{K}[a])
\end{aligned}$$

Lemme 1 (dimension d'extension par nombre algèbrique)**.** *Soit a $\mathbb{K}$-algèbrique, alors,*

$$\deg(a) = [\mathbb{K}[a] : \mathbb{K}]$$

Démonstration. Preuve directe
Posons n = $\deg(a)$.
On a $\mathbb{K}[a] = \mathrm{Im}(\phi)$ où $\phi : \mathbb{K}[X] \to \mathbb{K}[a]$ morphisme d'anneau avec $\phi(X) = a$ et ϕ coïcindant avec l'identité sur $\mathbb{K}$ (caractèrisation de $\mathbb{K}[a]$).

Montrons que $(a^k)_{0\leq k\leq n-1}$ est une famille libre.
Soit $(x_i)_{0\leq i\leq n-1}$ tel que

$$0 = \sum_{0\leq i\leq n-1} x_i a^i$$

Alors $Q(X) := \sum_{0\leq i\leq n-1} x_i X^i$ est annulé par a.
Or, $\deg(Q) < \deg(a) = n$, donc $Q = 0$.
Donc les x_i sont nuls, donc $(a^k)_{0\leq k\leq n-1}$ est libre.
Montrons que $(a^k)_{0\leq k\leq n-1}$ est générateur.
Posons P le polynome minimal de a.
Soit $x \in \mathbb{K}[a]$,
Alors il existe $W \in \mathbb{K}[X]$ tel que $W(a) = x$.
Alors il exist $Q, R \in \mathbb{K}[X]$ tel que $Q(a)P(a) + R(a) = x$ et $\dim(R) < \dim(P)$.
On a $Q(a)P(a) + R(a) = Q(a)0 + R(a) = R(a) = x$.
Comme $\dim(R) < \dim(P)$, $R(a)$ est combinaison linéaire des $(a^k)_{0\leq k\leq n-1}$, donc x est combinaison linéaire des $(a^k)_{0\leq k\leq n-1}$, donc $(a^k)_{0\leq k\leq n-1}$ est générateur.
Donc $(a^k)_{0\leq k\leq n-1}$ est libre et générateur, donc une base, et donc $\deg(a) = n = [\mathbb{K}[a] : \mathbb{K}]$ 

Supposons $n = [\mathbb{L} : \mathbb{K}] \in \mathbb{N}$
Si $n = 1$ il est trivial que $\mathbb{L} = \mathbb{K}$
Et si n est premier, les sous-anneaux de $\mathbb{L}$ contenants $\mathbb{K}$ sont $\mathbb{K}$ et $\mathbb{L}$ (conséquence directe du produit des dimensions d'extensions)

2 Théorie de la constuctibilité

2.1 Introductions aux constructions

Tout les termes viennent de moi, étant donné que je connais pas la littérature/le consensus.

Définition 10 (systèmes de constructions)**.** *L'ensemble des systèmes de constructions est noté C. Notons Q l'ensemble des points. Un système de constructions est une paire (P, R) où P est l'ensemble des points de base ($P \subset Q$) et R est un ensemble d'applications (nommé règles) de la forme $Q^n \to C$ partiellement définit où $n \in \mathbb{N}$ pouvant changer entre les règles.*

Cela ne fait pas forcément sens à cause de la définition récursive, mais l'idée est assez intuitive.
Tout au long de cet article l'ensemble de constructions sera noté C et Q l'ensemble des points.

Définition 11 (opérations de constructions)**.** *Soit (P, R) un système de construction, une opération de construction est une paire (p, r) avec $r : Q^n \to C \in R$, $p \in P^n$ et $r(p)$ défini.*
On dénote par $(P, R)(p, r)$ le système de construction $r(p)$.

Tout au long de cet article, l'associativité de l'application sera à gauche, ainsi $A(B)(C)$ désigne $(A(B))(C)$.

Définition 12 (points constructibles)**.** *Dans un système de constuction (P, R), on a x constructible s'il existe $n \in \mathbb{N}$ tel qu'il existe une famille d'opérations de constructions à n éléments $(O_i)_{1 \leq i \leq n}$ tel que pour $(A, B) := (P, R)(O_1)(O_2)\dots(O_n)$, on ait $x \in A$*

Définition 13 (système de construction dérivé)**.** *On a (P', R') dérivé de (P, R) s'il existe $n \in \mathbb{N}$ tel qu'il existe une famille d'opérations de constructions à n éléméntns $(O_i)_{1 \leq i \leq n}$ tel que $(P', R') = (P, R)(O_1)\dots(O_n)$.*

Définition 14 (systèmes de constructions stables)**.** *On a P, R système de construction qui est stable si $\forall r \in R, \forall p \in r^{-1}(\mathrm{Im}(r)), (A, B) := r(p) \wedge B = R \wedge P \subset A$.*
Par abus de language, on peut associé l'ensemble P et un autre ensemble R' d'applications de la forme $Q^n \to \mathfrak{P}(P)$ par un système de construction stable (P, R) où $R = \{p \mapsto (r(p) \cup P, R) | r \in R'\}$.

La définition récursive ne poses pas de problèmes dans les faits, il suffit de construire une suite R_i où $R_0 = \{\}$ et $R_{n+1} = \{p \mapsto (r(p) \cup P, R_n) | r \in R'\}$ et prendre un R_i où i sera plus grand que le nombre d'opération de constructions faites, et on nomme R un R_i convenable par abus de notation. (c'est plus simple à exprimer en lambda-calculusl $R := Y(f \mapsto \{p \mapsto (r(p) \cup P, f) | r \in R'\}))$

2.2 Constructions à la règle et au compas

Définition 15 (système à la règle et au compas)**.** *Un système à la règle et au compas est un système stable P, R où $P \subset \mathbb{R}^2$, $(0, 0) \in P$, $(0, 1) \in P$ et les éléments de R sont les points construits par intersection de deux droites non paralleles (passant par deux points construits), une droite (passant par deux points construits) et un cercle (de centre un point construit et passant par un point construit) et deux cercles (de centre un point construit et passant par un point construit).*

Lemme 2 (constructibilité à la règle et au compas)**.** *Un point (y, x) est constuctible si et seulement si $(0, |x|)$ et $(0, |y|)$ est constructible.*

(il est supposé de connaître ses constructions géométriques de base)

Démonstration. Supposons $P = (y, x)$ constructible.
Créons A la droite passant par $(0, 0)$ et $(0, 1)$.
Créons B le point $0, -1$ par intersection de A et du cercle de centre $(0, 0)$ passant par $(0, 1)$.
Créons C la médiatrice de $[(0, -1), (0, 1)]$.
Créons D la projection de P sur A qui est $(0, x)$
Si $x < 0$, on construit $E = (0, |x|)$ l'intersection $(0, -x)$ du cercle de centre $(0, 0)$ passant par $(0, x)$, sinon on pose $E = D$.

Posons $F = (y, 0)$ la projection de P sur C.
Posons $G = (0, |y|)$ l'intersection positive du cercle de centre $(0, 0)$ et passant par F et la droite A.

Supposons $(0, |x|)$ et $(0, |y|)$ constructible.
Créons A la droite passant par $(0, 0)$ et $(0, 1)$.
Créons B le point $0, -1$ par intersection de A et du cercle de centre $(0, 0)$ passant par $(0, 1)$.
Créons C la médiatrice de $[(0, -1), (0, 1)]$.
Alors $(0, x)$ et (resp $(y, 0)$) constructible par intersection du cercle de centre $0, |x|$ (resp $(0, |y|)$) et de A (resp C).
Si l'un a une partie en 0 c'est fini, on suppose donc ensuite que ce n'est pas le cas.
Créons E la médiatrice de $[(0, 0), (0, 2x)]$.
Créons F la médiatrice de $[(0, 0), (2y, 0)]$.
Alors $G = (y, x)$ est l'intersection entre E et F.

Lemme 3 (groupe additif de constructibilité)**.** *Si* $(0, a)$ *et* $(0, b)$ *constructibles, alors* $(0, a + b)$ *constructibles.*

Démonstration. Sans perdre en généralité, supposons $|a| \geq |b|$.
On pose D la droite $((0, 0)(0, 1))$ On créé le point $C = (0, \frac{b}{2})$ par intersection entre D et la médiatrice de $[(0, 0)(a, b)]$
On créé le point $-C = (0, -\frac{b}{2})$ par intersection entre D et le cercle de centre $(0, 0)$ et passant par C.
On créé le point $-E = (0, -b - a)$ par intersection entre D et le cercle de centre $-C$ passant par $(0, a)$.
Ainsi, $E = (0, a + b)$ intersection entre D et le cercle de centre $(0, 0)$ passant par $-E$ est constructible.

Corollaire 1 (Latice entière)**.** *Les points de la forme* (a, b) *avec* $a, b \in \mathbb{Z}$ *sont constructibles.*

Lemme 4 (monoid multiplicatif de constructibilité)**.** *Si* $(0, a)$ *et* $(0, b)$ *constructibles, alors* $(0, a \times b)$ *constructible.*

Démonstration. Sans perdre en généralité, supposons $a \geq b \geq 0$.
Si $b = 0$, $(0, a \times b) = (0, 0)$ qui est constructible.
Sinon $b \neq 0$.
Créons la droite des absices A.
Créons $B = (a, 0)$ constructible.
Créons $C = (b - 1, a)$ constructible.
Alors $D = (0, a \times b)$ est l'intersection de A et de (BC) donc constructible.

Lemme 5 (groupe multiplicatif de constructibilité)**.** *Si* $(0, a) \neq (0, 0)$ *constructibles, alors* $(0, \frac{1}{a})$ *constructible.*

Démonstration. Soit $P = (0, a) \neq (0, 0)$.
Supposons sans perdre de généralité que $a \geq 0$.
On crée A la droite des absices.
On crée B la droite passant par $(1, 0)$ et $(a - 1, 1)$.
Alors $C = (0, \frac{1}{a})$ est le point d'intersection entre A et B.

Corollaire 2. *Les points constructibles forment un corps.*

Corollaire 3. *Les points de la forme (a, b) avec $a, b \in \mathbb{Q}$ sont constructibles.*

Par abus de langage je dirais "a est constructible" pour "$(0, a)$ est constructible".

Définition 16 (ASMD)**.** *Un nombre est ASMD (addition/soustraction et multiplication/division) si il est constructible à partir de l'addition/soustraction et multiplication/division de mesures dans le système (distances entre deux points).*

2.2.1 Intersection entre deux droites

Une droite constructible s'écrit $ax + by + c$ avec a, b, c ASMD.
Donc si (y, x) est intersection de deux droites non perpendiculaire construites à la règle et au compas, on a

$$\begin{aligned} ax + by + c &= 0 \\ \wedge a'x + b'y + c' &= 0 \\ \iff \begin{pmatrix} a & b \\ a' & b' \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} &= - \begin{pmatrix} c \\ c' \end{pmatrix} \end{aligned}$$

Et par les formules de Cramer, y, x sont ASMD de a, b, c, a', b', c', donc $0[P \dots] = 0[P \dots][(y, x)]$

2.2.2 Intersection entre une droite et un cercle

Un cercle constructible s'écrit $x^2 + y^2 + ax + by + c = 0$ avec a, b, c ASMD.
Don csi (y, x) est intersection d'une droite et un cercle, alors (y, x) satifait

$$\begin{aligned} ax + by + c &= 0 \\ \wedge x^2 + y^2 + a'x + b'y + c &= 0 \end{aligned}$$

Avec a, b, c, a', b', c' ASMD.
Posons nous dorénamment sur $\mathbb{C} \cong \mathbb{R}^2 \cong$ plan.
Si $z = x + yi$ intésection d'une droite et d'un cercle, alors z solution de

$$\begin{aligned} (z - c)\overline{(z - c)} - r^2 = 0 \\ (z - a)\overline{w} + \overline{(z - a)}w = 0 \end{aligned}$$

Avec $r \in \mathbb{R}_+$ ASMD, $c \in \mathbb{C}$ à composantes ASMD et $w \in \mathbb{C}^*$ à composantes ASMD.
La résolution des z solutions montre que ce sont les racine d'un polynome du second degré à coefficiants ASMD.
Si ce polynome est irréductible, $0[P\dots][(x,y)] = 0[P\dots][(x,y)]$.
Sinon, $2 = [0[P\dots][(x,y)] : 0[P\dots]]$.

2.2.3 Intersection entre une deux cercles

Si $z = x + yi$ intésection d'une droite et d'un cercle, alors z solution de

$$(z-a)\overline{w} + \overline{(z-a)}w = 0(z-a')\overline{w'} + \overline{(z-a')}w' \qquad = 0$$

Avec $a, a' \in \mathbb{C}$ à composantes ASMD et $w, w' \in \mathbb{C}^*$ à composantes ASMD.
La résolution des z solutions montre que ce sont les racine d'un polynome du second degré à coefficiants ASMD.
Si ce polynome est irréductible, $0[P\dots][(x,y)] = 0[P\dots][(x,y)]$.
Sinon, $2 = [0[P\dots][(x,y)] : 0[P\dots]]$.

2.2.4 Conditions nécessaire de la constructibilité d'un point en géométrie à la règle et au compas

Avec les trois sections précédentes, il est clair que les points construisibles sont des points algèbriques de $0[P\dots]$ à degré de la forme 2^n avec $n \in \mathbb{N}$. (je ne dis rien sur la réciproque)
Posons $P := \{(0,0),(0,1)\}$ et $\mathbb{K} := 0[P\dots]$.
Une très ancienne question de géométrie est : "est t'il possible de diminuer le côté d'un cube pour réduire de moitié son volume."
La réponse est non.

Démonstration. En effet, pour réduite le volume de moitié il faut multiplier la taille du côté par $\frac{1}{\sqrt[3]{2}}$ et $\deg_{\mathbb{K}}(\frac{1}{\sqrt[3]{2}}) = 3$ qui n'est pas une puissance de deux.

Une autre question est "est t'il possible de construire un carré de la même aire qu'un cercle constructible".
La réponse est non.

Démonstration. En effet, posons r le rayon du cercle (qui est constructible), le côté du carré devrait être de longueur $\sqrt{\pi}r$, or π est $\mathbb{K}$-trancendants, donc $\sqrt{\pi}$ est $\mathbb{K}$-trancendants, donc $\sqrt{\pi}r$ $\mathbb{K}$-trancendants (r est $\mathbb{K}$-algèbrique.)

Une autre question est "est t'il possible de trisecter un angle quelconque constructible".
La réponse est encore non, mais la démonstration est plus longue.

Démonstration. Essayons avec l'angle $\theta = \frac{\pi}{6}$ rad.
Si la trisection est possible, un des point d'intersection $(\cos(\theta), \sin(\theta))$ entre le cercle unitaire et la droite passant par $(0,0)$ d'angle $\frac{\theta}{3}$.
Montrons donc que $\frac{\theta}{3}$ n'est pas constructible. On a

$$\begin{aligned}
\sin(\theta) &= \sin(\frac{\theta}{3})\cos(\frac{2\theta}{3}) + \sin(\frac{2\theta}{3})\cos(\frac{\theta}{3}) \\
&= \sin(\frac{\theta}{3})(\cos(\frac{\theta}{3})^2 - \sin(\frac{\theta}{3})^2) + 2\sin(\frac{\theta}{3})\cos(\frac{\theta}{3})^2 \\
&= \sin(\frac{\theta}{3})(1 - 2\sin(\frac{\theta}{3})^2) + 2\sin(\frac{\theta}{3})(1 - \sin(\frac{\theta}{3})^2) \\
&= 3\sin(\frac{\theta}{3}) - 4\sin(\frac{\theta}{3})^3
\end{aligned}$$

Ainsi, $\sin(\frac{\theta}{3})$ est racine du polynome $4X^3 - 3X + \sin(\theta)$.
Donc racine de $8X^3 - 6X + 1$, qui est irréductible sur $\mathbb{K}[\sin(\theta), \cos(\theta)]$
Donc $3 | \deg(\sin(\frac{\theta}{3}))$, donc $\deg(\sin(\frac{\theta}{3}))$ n'est pas une puissance de 2.
Donc $\sin(\frac{\theta}{3})$ n'est pas constructible.
Donc (contraposé) la trisection de θ n'est pas possible. 

2.3 Constructions origamiques d'un plis

Maintenant que vous êtes en jambes, (*petite béquille*) on perds les bases de la géométrie usuelle apprise à l'école.
Je vais assumer une certaine familiarité avec le pliage d'une feuille de papier, sinon essayer de faire un avion en papier (tutoriel : `https://www.youtube.com/watch?v=vSCOvatRuq0`)
Dans cette géométrie, les cercles ne sont pas constructibles, seules les points de base et l'intersection de deux droites constructibles le sonts.
Il y a 6 manières de faire une droite en géométrie origamique.

- droite passant par deux points construits différents.
- médiatrice de $[AB]$ où A et B points construits.
- droite D tel que le symmétrique de A (A étant une droite construite) par rapport à D soit B (une autre doite construite).
- droite D passant par A un point construit et sa projection sur B une droite construite.
- droite D passant par A un point construit tel que la symétrie de C un point par rapport à D soit un point de D' une droite construite.
- droite D tel que A un point construit à pour symmétrie par rapport à D un point de B une droite construite et A' un point construit à pour symmétrie par rapport à D un point de B' une droite construite.

Comme en géométrie classique, on va supposer qu'on ait $(0,0)$ et $(0,1)$ parmis les points de bases.

Avec des constructions très similaire de la géométrie classique, on peut montrer que (y, x) est construtible si et seulement si $(0, |x|)$ et $(0, |y|)$ sont constructibles (exercice).
Par le même abus de langage, on dira que $x \in \mathbb{R}$ est constructible si $(0, x)$ est constructible.
Avec des constructions très similaire de la géométrie classique, on peut montrer que l'ensemble des points constructible $\subset \mathbb{R}$ forments un corps. (exercice)

Lemme 6 (points constructibles en origami)**.** *Si x est constructible avec pour points initial P en géométrie usuelle, alors x est constructible avec pour points initial P en géométrie origamique.*

Démonstration. On va prouver que les trois règles de constructions de la géométrie usuelle peuvent se faire en origamique.
Intersection entre deux droites et intersection d'une droite à un cercle sont triviales.
Montrons que l'intersection entre deux cercles est faisable.
Supposons A, B points constructibles et créons les intersections entre le cercle de rayon r (mesure) de centre A et le cercle de rayon R (mesure) de centre B.
Sans perdre en généralité, supposons $r \geq R$.
Posons O le milieu de $[AB]$.
Posons $d = \frac{r+R}{2}$.
Posons C l'intersection entre (AB) et le cercle de rayon $\frac{r^2-R^2}{4d}$ de centre O la plus proche de B.
Posons D la perpendiculaire passant pas C de (AB).
Alors, les points d'intersection entre le cercle de rayon R centré en B et la droite D sont les intersections des cercles de centre A de rayon r et de centre B de rayon R.

On a toutes les règles sauf la dernière qui est faisable à la règle et au compas, donc la combinaison de toutes sauf la dernière donne des racines de polynome de degré 1 ou 2.
Étudions alors quels points deviennent construisibles avec l'utilisation de la sixième règle.
(bon ok là je galère)
La règle 6 à A, B points et D, D' droites, dont maintent j'abbréverait en R6 est la droite tangeante à deux parabolles P_1 et P_2 ayant pour focale respectives A et B à coefficiants ASMD, ce qui a pour coefficiant directoire soit $+\infty$ soit une racine d'un polynome de degrè ≤ 3.
Donc l'intersection avec les droites des autres règles donnent des point $0[P \dots]$-algèbrique de degrè 2 ou 3.
Donc les points constructibles en origami simple sont tous de la forme $2^n 3^k$.
Je vous laisse en exercice comment construire $\sqrt{a}$ (possible à la règle et compas), $\sqrt[3]{a}$.
Comme on peut construire $\sqrt{a}$ on peut résoudre toute équation du second degré à coefficiant ASMD. (formules de lycées)

Comme on peut construire $\sqrt[3]{a}$ on peut résoudre toute équation du troisième degré à coefficiant ASMD. (formules de Cardan)
Ainsi, on a $x \in \mathbb{R}$ origami constructible si et seulement si il existe $P_0, \dots, P_n$ tel que $P_0 = P$, $[P_{i+1} : P_i] \in \{2, 3\}$ et $x \in P_n$.
Ainsi il est possible de trisecter un angle, multiplier le volume d'un cube par $\frac{1}{2}$, mais pas possible de construire la quadrature d'un cercle (en règle général).

2.4 Constructions origamiques à plusieurs plis

La même chose mais on peut faire plusieurs plis successifs comme un vrai origami.
Tout ce qui est faisable avec un plis à la fois est trivialement possible avec plusieurs, donc les points construtibles forment encore un corps.
D'après `https://www.researchgate.net/publication/255578688_One_Two_and_Multi-Fold_Origami_Axioms` toutes équations de degrès $n \geq 3$ est résolvable en autorisant $n - 2$ plis à la fois. (les preuves sont trop longues pour que je les explicites ici.)
Ainsi en s'autorisant autant de plis qu'on veut à la fois, tout nombres $0[P \dots]$-algèbriques sont constructibles et réciproquement, tout nombres constructibles sont $0[P \dots]$-algèbriques.