Géométrie et algèbre

Exercices et applications

D. Kohel

11/01/2022

Géométrie et algèbre

Nombres algébriques

Exercice

Soit $\alpha = \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{R}$.

a) Définir l'extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ par quotient de $\mathbb{Q}[x,y]$:

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) \cong \mathbb{Q}[x,y]/(x^2-2,\, y^2-3). \quad (*)$$

À noter que $V(x^2-2, y^2-3)$ est une variété de dimension zéro.

Les points sont $(\pm\sqrt{2}, \pm\sqrt{3}) \in V(\overline{\mathbb{Q}})$.

Le corps de nombres $(*)$ est l'algèbre de fonctions sur $V(x^2-2, y^2-3)$.

b) Ajouter une variable z avec relation linéaire $z = x+y$.

Alors on a $\cong \left(\mathbb{Q}[x,y]/(x^2-2, y^2-3)\right)[z]/(x+y-z)$

$$\mathbb{Q}(\sqrt{2},\sqrt{3},\alpha) \cong \mathbb{Q}[x,y,z]/(x^2-2,\, y^2-3,\, x+y-z).$$

À noter que

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

est une extension triviale.

Remarque. Si $V(I)$ est une variété, dans $\mathbb{A}^n$, avec anneau des coordonnés $k[x_1, \dots, x_n]$, alors l'algèbre $k[x_1,\dots,x_n]/I$ est l'algèbre de fonctions sur $V=V(I)$. Si $f\in k[x_1,\dots,x_n]/I$, et $(a_1,\dots,a_n)\in V$, alors l'élément

$$f(a_1,\dots,a_n)\in \bar{k} \quad (\text{N.B. } V=V(\bar{k}))$$

est bien-défini, car si $g=f+p$ est un autre représentant pour f, avec $p\in I$, l'évaluation

$$g(a_1,\dots,a_n)=f(a_1,\dots,a_n)+\underbrace{p(a_1,\dots,a_n)}_{=0}$$

est égal à $f(a_1,\dots,a_n)$.

Donc, pour $V=V(x^2-2,y^2-3)$, on l'algèbre de fonctions

$$\mathbb{Q}[x,y]/(x^2-2,y^2-3),$$

pour lequel les fonctions définissent des applications dans

$$\mathbb{Q}(\sqrt{2},\sqrt{3})\subseteq\overline{\mathbb{Q}}\subseteq\mathbb{C}$$

L'application est

$$V\xrightarrow{f}\mathbb{C}$$
$$(a,b)\longmapsto f(a,b)$$

Ici, $(a,b)\in\{(\pm\sqrt{2},\pm\sqrt{3})\}$.

Remarque. On obtient, sur $\mathbb{R}$,

$$\frac{\mathbb{Q}[x,y]}{(x^2-2,\, y^2-3)} \longrightarrow \prod_{P\in V} \mathbb{R}, \quad V = \{(\pm\sqrt{2}, \pm\sqrt{3})\}$$

$$f \longmapsto (f(P))$$

Par exemple

$$x+y \longmapsto (\sqrt{2}+\sqrt{3}, -\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{3}, -\sqrt{2}-\sqrt{3})$$

(c) Utiliser élimination (par le résultant) pour trouver le polynôme minimal de α.
En utilisant notre modèle algébrique

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \alpha) \cong \mathbb{Q}[x,y,z] / (x^2-2,\, y^2-3,\, x+y-z)$$

on peut calculer

- $\mathrm{Res}_y(y^2-3,\, x+y-z) = (x-z)^2-3$

et ensuite

- $\mathrm{Res}_x(x^2-2,\, (x-z)^2-3) = z^4-10z^2+1.$

Alors le polynôme minimal de α est z^4-10z^2+1 (variable z).

d) Construction algèbrique.
Définir la matrice de multiplication par α dans la base $(1, \sqrt{2}, \sqrt{3}, \sqrt{2}\cdot\sqrt{3})$ de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
On a :

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 1 \\ 0 & 3 & 2 & 0 \end{bmatrix} \qquad \begin{aligned} \alpha\cdot 1 &= \sqrt{2}+\sqrt{3} \\ \alpha\cdot\sqrt{2} &= 2+\sqrt{2}\sqrt{3} \\ \alpha\cdot\sqrt{3} &= 3+\sqrt{2}\sqrt{3} \\ \alpha\cdot\sqrt{6} &= 3\sqrt{2}+2\sqrt{3} \end{aligned}$$

On obtient également le polynôme caracteristique x^4-10x^2+1.
En conclusion : on peut utiliser des constructions géometriques ou algèbriques pour l'étude des propriétés des nombres algèbriques.

<u>Exercice</u> Soit $f(x) = x^4+x+1 \in \mathbb{Q}[x]$.
On a
$$p(x) = \prod_{i=1}^{4}(x-\alpha_i) \in \mathbb{C}[x].$$

On observe que
$$p(x) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4,$$
où
$$s_1 = \alpha_1 + \cdots + \alpha_4$$
$$s_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4$$
$$\vdots$$
$$s_4 = \alpha_1\alpha_2\alpha_3\alpha_4$$

où $s_1, \ldots, s_4$ sont les formes symétriques dans les racines $\alpha_1, \ldots, \alpha_4$. En particulier on a :

@ $$s_1 = s_2 = 0 \text{ et } -s_3 = s_4 = 1. \qquad \circledast$$

On peut étudier le système d'équations entre les racines et les polynômes symetriques. On introduit huit variables :

$$s_1, s_2, s_3, s_4 \text{ et } \underbrace{a_1, a_2, a_3, a_4}_{\text{pour les racines } \alpha_i}.$$

avec relations génériques pour les polynômes symétriques, données par :

$$x^4 + \sum_{i=1}^{4} (-1)^i s_i x^{4-i} = \prod_{i=1}^{4} (x - a_i)$$

et les relations spécifiques : $\circledast$.

Quelles sont les relations entre les variables $a_1, \ldots, a_4$?

Par exemple : $a_1 + \cdots + a_4 = 0$ et
$$a_1 a_2 a_3 a_4 = 1.$$

Comment étudier ce système en Sage / par les méthodes de calc. formels ?

(b) Les sommes de puissances des racines : on définit

$$P_n(\alpha_1,\dots,\alpha_4) = \sum_{i=1}^{4} \alpha_i^n .$$

On note que ces expressions sont stable sous l'action de permutation des racines (les α_i).
Par conséquent, on peut les exprimer en termes des formes symétriques (évaluation des polynômes symetriques) dans les racines.
On définit la derivée logarithmique de $f(x) \in k[x]$ par

$$\frac{d\log f(x)}{d\log x} = \frac{d\log f(x)}{dx} \Big/ \frac{d\log x}{dx}$$

(defn) $\updownarrow$

$$= \frac{x f'(x)}{f(x)} \overset{(*)}{=} \sum \frac{x}{x-\alpha_i} = \sum_{i=1}^{d} \frac{1}{1-\alpha_i z}$$

Si $f(x) = \prod_{i=1}^{d} (x-\alpha_i)$, on a

où $z = 1/x$.

$$= \sum_{i=1}^{d} \sum_{n=0}^{\infty} \alpha_i^n z^n$$

$$= \sum_{n=0}^{\infty} P_n z^n .$$

N.B. $\ln z^d f(1/z) \in k[[z]]$

$= \ln\left(\prod (1-\alpha_i z)\right) \Rightarrow$

L'égalité ⊛ $\dfrac{x f'(x)}{f(x)} = \sum_i \dfrac{x}{x-\alpha_i}$

peut être démontrée en utilisant

$$f'(x) = \sum_{i=1}^{d} \prod_{j\neq i} (x-\alpha_j),$$

alors

$$\frac{f'(x)}{f(x)} = \sum_{i=1}^{d} \frac{1}{x-\alpha_i} \quad (**)$$

ou en passant par $\dfrac{d \log f(x)}{dx}$, ln

$$\frac{d}{dx}\left(\ln \prod (x-\alpha_i)\right)$$

$$= \frac{d}{dx}\left(\sum_{i=1}^{d} \ln(x-\alpha_i)\right)$$

$$= \sum_{i=1}^{d} \frac{d \ln(x-\alpha_i)}{dx} = \sum_{i=1}^{d} \frac{1}{x-\alpha_i}. \quad (**)$$

On obtient la même expression (**) qui donne ⊛ après mult par $x = 1 \Big/ \left(\dfrac{d}{dx} \ln x\right)$.

$\Rightarrow$ et $\ln(1-t) = -\sum_{n=1}^{\infty} \dfrac{t^n}{n} \in k[[t]]$ (car $k = 0$)

En conclusion, on obtient ⑧

$$x f'(x) = f(x) \sum_{n=0}^{\infty} p_n z^n,$$

d'où $(x = 1/z)$:

$$\underbrace{f'(1/z)\, z^{d-1}}_{\text{polynôme en } z} = \underbrace{f(1/z)\, z^d}_{} \sum_{n=0}^{\infty} p_n z^n,$$

ce qui permet d'établir des expressions (recurrences) pour p_n en fonction des coeffients $(s_1, \dots, s_d)$ de $f(x)$:

$$f(x) = \sum_{i=1}^{d} (-1)^i s_i x^i.$$

ⓑ

Comment déterminer les sommes de puissances

$$\alpha_1^n + \dots + \alpha_4^n = p_n$$

des racines de $f(x) = x^4 + x + 1$?

— Étudier les récurrences pour p_n en termes des sommes symétriques (combinatoire),

— Géométrique (pour $p_1, \dots, p_n$, en nombre fixé): élimination des $s_1, \dots, s_n$.

- Algébrique : algèbre des polynômes : on observe que

$$p_n = \mathrm{Tr}(x^n \bmod f(x)) \qquad (***)$$

dans $\mathbb{Q}[x]/f(x)$. Dans une base $(1, x, x^2, x^3)$ pour $\mathbb{Q}[x]$, on a

$$\mathrm{Tr}(1) = 4 = p_0,$$

$$\mathrm{Tr}(x) = p_1 = s_1, \text{ etc}$$

N.B. Trace de l'identité sur un espace de dimension 4 $= p_0 = \alpha_1^0 + \alpha_2^0 + \alpha_3^0 + \alpha_4^0$.

Il suffit de déterminer le polynôme caractéristique de x^2 et x^3, et extraire le coefficient "trace" (la somme symétrique "s_1" $= -$ coefficient de x^3 dans son polynôme caractéristique).

- Algébrique #2 : déterminer la matrice de multiplication par x, $= A$, et alors

$$p_n = \mathrm{Tr}(A^n). \qquad (***)$$

On peut calculer $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -1 & 0 & 0 \end{pmatrix}$.

(Rappel : $x^4 = -x - 1$)

En Sage on peut vérifier que ces deux contruction s'accordent avec

$$(p_0, p_1, \ldots, p_7) = (4,0,0,-3,-4,0,3,7).$$

(c) En utilisant

$$x f'(x) = f(x) \sum_{n=0}^{\infty} p_n z^n \quad (\text{où } x = \tfrac{1}{z}),$$

trouver une récurrence pour la suite (p_n).

N.B. $z^4 \cdot x f'(x)$ est un polynôme de degré 4 en z, alors tous les termes de degré superieur s'annulent (dans l'expression

$$\underbrace{z^4 f(x)}_{\text{poly in } z} \sum_{n=0}^{\infty} p_n z^n).$$