

Corps de modules VS Corps de définition

Dans cet exposé j'ai présenté la notion de **corps de modules** bien souvent moins connue que celle de **corps de définition**. L'objectif ayant été de :

- montrer le lien entre les deux notions,
- interpréter géométriquement la notion de corps de modules à travers l'exemple d'espaces de modules de courbes,
- donner des critères permettant de savoir si les deux notions coïncident,
- traiter un exemple explicite où les deux notions ne coïncident pas mais dont l'origine incite plutôt à considérer le corps de modules.

1 Introduction.

Soient k un corps et \bar{k} une clôture algébrique de k . Je note $\Gamma := \text{Gal}(\bar{k}|k)$ et considère $\Gamma \curvearrowright A$ une action à orbites finies.

Définition 1. *Un sous-corps $k \subset K \subset \bar{k}$ est dit corps de modules pour $a \in A$ si pour tout $\gamma \in \Gamma$ fixant K , $a^\gamma = a$. On appelle corps de modules universel de a l'intersection de tous ses corps de modules, noté $\mathcal{M}(a)$.*

La correspondance de Galois assure que le corps de modules universel est déterminé par l'égalité

$$\text{Gal}(\bar{k}|\mathcal{M}(a)) = \text{Stab}_\Gamma(a)$$

qui est donc d'indice fini, en particulier $\mathcal{M}(a)|k$ est de degré fini.

Si $\mathcal{M}(a)|k$ est galoisienne alors l'image de l'action $\Gamma \curvearrowright \text{Orb}_\Gamma(a)$ est $\text{Gal}(\mathcal{M}(a)|k)$, et en général si $\mathcal{M}(a) = k(\alpha)$ alors

$$\Gamma \curvearrowright \{\text{conjugués de } \alpha\} \simeq \Gamma \curvearrowright \text{Orb}_\Gamma(a)$$

En général pour disposer d'une action de Γ , faut que les éléments de A soient « définis » sur \bar{k} et pour avoir des orbites finies faut qu'ils soient en fait « définis » chacun sur une extension finie de k . C'est ce que nous allons avoir dans la section suivante. Dans la suite on dit **corps de modules** pour dire **corps de modules universel**.

2 Géométrie algébrique.

Soit S un schéma sur k . Je note \bar{S} le schéma obtenu après extensions des scalaires à \bar{k} . Nous allons considérer C une sous-catégorie de $\text{Sch}_{/\bar{S}}$. En effet on dispose d'une action de Γ sur C donnée par les changements de base $\gamma : \text{Spec}(\bar{k}) \rightarrow \text{Spec}(\bar{k})$. C'est une action sur une catégorie au sens où on dispose d'équivalences de catégories $X \mapsto X^\gamma$ qui sont compatibles par composition, autrement dit un morphisme $\Gamma \rightarrow \text{Aut}(C)$. S'en déduit une action ensembliste

$$\Gamma \curvearrowright \{\text{classes d'isomorphismes de } C\}$$

Cette action est à orbites finies si on se restreint aux schémas de type fini. On peut toujours considérer le foncteur oubli $(X \rightarrow \bar{S}) \mapsto X$ (je dis qu'un \bar{k} -schéma est donné par un morphisme $X \rightarrow \text{Spec}(\bar{k})$) qui induit une inclusion

$$\mathcal{M}(X) \subset \mathcal{M}(X \rightarrow \bar{S})$$

Définition 2. *Soit K une sous-extension de $\bar{k}|k$. On dit que K est un corps de définition pour $X \rightarrow \bar{S}$ ou que $X \rightarrow \bar{S}$ admet un modèle sur K si existe $Y \rightarrow T$ un morphisme de K -schémas tel que $(\bar{Y} \rightarrow \bar{T}) \simeq (X \rightarrow \bar{S})$.*

En suit immédiatement la proposition suivante.

Proposition 1. 1)

$$\mathcal{M}(X \rightarrow \bar{S}) \subset \bigcap_{K \text{ déf de } X \rightarrow \bar{S}} K$$

2) Dans le cas des courbes projectives lisses y a égalité dans l'inclusion.

En général le corps des modules n'est pas un corps de définition !

3 Courbes.

Dans la suite « courbe » signifie « courbe projective lisse ». On pose $k = \mathbb{Q}$ et $S = \text{Spec } \overline{\mathbb{Q}}$, et \mathcal{C} est la catégorie des courbes avec les morphismes entres courbes algébriques. Je note (en laissant de côté sa définition champêtre...) $\mathcal{M}_g(\overline{\mathbb{Q}})$ l'ensemble des courbes de genre g à isomorphisme près sur $\overline{\mathbb{Q}}$.

$[g = 0]$. Dans ce cas $\mathcal{M}_0(\overline{\mathbb{Q}}) = \{\mathbb{P}_{\overline{\mathbb{Q}}}^1\}$ et la droite projective est défini sur $\overline{\mathbb{Q}}$. Donc tout courbe X de genre 0 vérifie $\mathcal{M}(X) = \mathbb{Q}$ et est un corps de définition pour X .

$[g = 1]$. Y a un isomorphisme $\mathcal{M}_1(\overline{\mathbb{Q}}) \xrightarrow{\sim} \overline{\mathbb{Q}}$ donné par le j -invariant, si E est une courbe elliptique donnée par l'équation $y^2 = x^3 + ax + b$ alors

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2} \in \mathbb{Q}(a, b)$$

En suit que $\forall \gamma \in \Gamma, j(E^\gamma) = j(E)^\gamma$, et donc $\text{Stab}_\Gamma(E) = \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}(j(E)))$, c'est-à-dire

$$\mathcal{M}(E) = \mathbb{Q}(j(E))$$

et est un corps de définition pour E car $E \simeq E'$ où E' est donnée par l'équation

$$y^2 = 4x^3 - \frac{27j(E)}{j(E) - 1728}(x - 1)$$

$[g = 2]$. Toutes les courbes de genre 2 sont hyperelliptiques et on a un revêtement

$$(\mathbb{P}^1 \setminus \{0, 1, \infty\})^3 \setminus \{\exists i \neq j | \alpha_i = \alpha_j\} \longrightarrow \mathcal{M}_2(\overline{\mathbb{Q}})$$

qui envoie un triplet $(\alpha_1, \alpha_2, \alpha_3)$ sur la courbe donnée par l'équation

$$y^2 = x(x - 1)(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

La fibre est donnée par les triplets obtenus par les six transformations engendrées par $\alpha_i \mapsto 1/\alpha_i$, $\alpha_i \mapsto 1 - \alpha_i$ ainsi que les permutations des α_i . En genre 2 le corps de modules d'au moins une courbe n'est pas un corps de définition. Par exemple la courbe X donnée par le triplet $(-1, \zeta t, \zeta/t)$, où $\zeta = \exp(2i\pi/3)$ et $t \in \mathbb{Q} \setminus \{0, 1\}$. En effet y a au plus un conjugué par Galois, le conjugué complexe \overline{X} dont le triplet est donné par

$$(-1, \zeta^2 t, \zeta^2/t) = ((-1)^{-1}, (\zeta/t)^{-1}, (\zeta t)^{-1})$$

qui est donc dans la même fibre que $(-1, \zeta/t, \zeta t)$ qui lui est dans la même fibre que $(-1, \zeta t, \zeta/t)$. En suit que $X \simeq \overline{X}$ et donc que $\mathcal{M}(X) = \mathbb{Q}$, mais Earle a donné un argument de géométrie projective pour démontrer que si $t > 0$ alors X n'admet pas de modèle sur \mathbb{Q} .

Comme dans le cas de genre 1 on peut se demander si en fait n'existeraient pas des quantités qui génèreraient $\mathcal{M}(X)$. En fait, leur nom l'indiquant, les corps de modules doivent être considérés comme des corps résiduels sur des espaces de modules grossiers des objets étudiés (\mathbb{A}^1 pour \mathcal{M}_1) et donc générés par des coordonnées sur l'espace (comme j pour \mathcal{M}_1).

Igusa a construit un espace de modules grossier pour les courbes de genre 2, qui sont toutes hyperelliptiques, comme le quotient d'un schéma affine sur

\mathbb{Z} par $\mathbb{Z}/5\mathbb{Z}$. Et on peut en effet définir 4 nombres, appelés invariants d'Igusa, $i_1(X), i_2(X), i_3(X), i_4(X)$ vérifiant

$$i_1 i_3 - i_2^2 - 4i_4 = 0$$

qui sont des expressions polynomiales à coefficients entiers des coefficients du polynôme de droite dans une équation pour X donnée par

$$y^2 = x^5 + \dots$$

Théorème 1. (Igusa) *Considérons la relation d'équivalence \sim engendrée par*

$$(j_1, j_2, j_3, j_4) \sim (\xi j_1, \xi^2 j_2, \xi^3 j_3, \xi^4 j_4) \quad (\xi \in \mu_5)$$

Alors les invariants d'Igusa induisent une bijection entre $\mathcal{M}_2(\overline{\mathbb{Q}})$ et

$$\{(j_1, j_2, j_3, j_4) \in \overline{\mathbb{Q}}^4, j_1 j_3 - j_2^2 - 4j_4 = 0\} / \sim$$

Il en suit que

$$\mathcal{M}(X) \subset I(X) := \mathbb{Q}(i_1(X), i_2(X), i_3(X), i_4(X))$$

Réciproquement, notons L la clôture galoisienne de $I(X)$. Si les invariants sont $\neq 0$ alors on peut en déduire qu'existe un cocycle $\theta : \text{Gal}(L|\mathcal{M}(X)) \rightarrow \mu_5$ tel que

$$i_k(X)^\gamma / i_k(X) = \theta(\gamma)^k$$

En supposant que $H^1(\text{Gal}(L|\mathcal{M}(X)), \mu_5) = 0$ on obtient l'inclusion

$$\mathbb{Q}(i_1(X)/\xi, i_2(X)/\xi^2, i_3(X)/\xi^3, i_4(X)/\xi^4) \subset \mathcal{M}(X)$$

où $\xi \in \mu_5$. Il en suit que $\xi \in \mathcal{M}(X)$ et donc finalement $I(X) = \mathcal{M}(X)$.

On peut également dès le début adjoindre les éléments de μ_5 . Soit $\xi \in \mu_5$. Si le groupe de cohomologie à coefficients triviaux $H^1(\text{Gal}(L|\mathcal{M}(X)(\xi)), \mathbb{Z}/5\mathbb{Z})$ s'annule alors on a

$$\mathcal{M}(X)(\mu) = I(X)(\mu)$$

$g \geq 3$. Les courbes ne sont pas toutes hyperelliptiques et même pour celles-ci l'étude devient difficile, par exemple \mathcal{M}_3 est de dimension 6 mais les courbes hyperelliptiques forment une sous-variété de dimension 5 pour lesquelles on peut définir 9 invariants, dits de Shioda, avec 4 relations algébriques.

4 Obstructions.

On possède un théorème très général sur les variétés quasi-projectives.

Théorème 2. *Soit X une variété quasi-projective définie sur un corps de nombres F . Soit $F|M$ une extension galoisienne. Alors l'action de Γ se factorise par $\text{Gal}(F|M)$, et X admet un modèle sur M si et seulement si existe une famille d'isomorphismes $(\rho(g) : X^g \rightarrow X)_{g \in \text{Gal}(F|M)}$ vérifiant la condition de cocycle donnée par la commutativité du diagramme*

$$\begin{array}{ccc} X^{gh} & \longrightarrow & X^h \\ & \searrow & \downarrow \\ & & X \end{array}$$

Soit G le groupe de monodromie de $X \rightarrow \bar{S}$ un revêtement de courbes. On note $\mathcal{M} = \mathcal{M}(X \rightarrow \bar{S})$. Dans [1] on montre le théorème suivant

Théorème 3. *Existe une action de $\text{Gal}(\bar{\mathbb{Q}}|\mathcal{M})$ sur G stabilisant son centre et une famille $(\Omega_\delta)_{\delta \in \Delta}$ de classes de $H^2(\text{Gal}(\bar{\mathbb{Q}}|\mathcal{M}), Z(G))$ vérifiant la propriété que \mathcal{M} est un corps de définition pour $X \rightarrow \bar{S}$ si et seulement si une des classes Ω_δ est nulle.*

Dans [2] on a un critère plus simple mais moins général

Proposition 2. *Supposons que $A := \text{Aut}(X \rightarrow \bar{S})$ soit abélien et que $X \rightarrow \bar{S}$ admette un modèle sur F extension galoisienne de \mathcal{M} . Alors $X \rightarrow \bar{S}$ admet un modèle sur \mathcal{M} si et seulement si $H^2(\text{Gal}(F|\mathcal{M}), A) = 0$.*

5 Exemple.

Traisons l'exemple du revêtement $\beta : E \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ donné par $E : y^2 = x(x-1)(x-\lambda)$, où $\lambda = \frac{1+\sqrt{2}}{2}$, et

$$\beta = \frac{v(1-v)}{4} \quad v = 2x(x-1) + \frac{1}{2}$$

Ici on a donc $F = \mathbb{Q}(\sqrt{2})$. Comme β ne dépend que de x le revêtement admet l'involution elliptique $(x, y) \mapsto (x, -y)$ comme automorphisme, et on vérifie que c'est le seul automorphisme. Donc $G \simeq \mathbb{Z}/2\mathbb{Z}$ et est un module trivial sous $\text{Gal}(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$. Par ailleurs on vérifie que $\mathcal{M}(E \rightarrow \mathbb{P}_{\mathbb{Q}}^1) = \mathbb{Q}$ car E et son conjugué par $\text{Gal}(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$ sont isomorphes via

$$(x, y) \mapsto (1-x, \sqrt{-1}y)$$

Or $H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} \neq 0$ donc d'après la proposition 2 le revêtement n'admet pas de modèle sur \mathbb{Q} . Remarquons que E admet un modèle sur \mathbb{Q} car

$$j(E) \in \mathcal{M}(E) \subset \mathcal{M}(E \rightarrow \mathbb{P}_{\mathbb{Q}}^1) = \mathbb{Q}$$

(ou plus simplement car $j(E) = 8000\dots$) Par conséquent si on choisit un modèle sur \mathbb{Q} pour E alors le modèle pour β sera nécessairement à coefficients irrationnels !

Pourquoi cet exemple ? On peut définir la classe d'isomorphisme sur $\bar{\mathbb{Q}}$ de $E \rightarrow \mathbb{P}_{\bar{\mathbb{Q}}}^1$ par un objet combinatoire (un dessin d'enfant, voir [3]) pour lequel aucun corps de définition n'est privilégié : seul fait sens son corps de modules.

6 Références.

[1] : Algebraic covers : field of moduli versus field of definition, Pierre Dèbes, Jean-Claude Douai, Annales scientifiques de l'É.N.S., 1997.

[2] : On the fields of definition of genus-one covers of \mathbb{P}^1 , Bulletin of the London Mathematical Society, 2023.

[3] : Dessins d'Enfants on Riemann Surfaces, Gareth Jones, Jürgen Wolfart, Springer, 2016.