

Atelier de Géométrie

Présentation de la courbe modulaire $X(1)$

1. Présentation et objectifs des deux ou trois séances

Je ne suis pas un géomètre mais en théorie des nombres, on peut être amené à considérer des objets à caractère géométrique (ex: courbes elliptiques...). Ainsi, mes travaux actuels consistent à trouver des points à coordonnées entières sur certaines courbes qu'on appelle modulaires. Ces courbes peuvent être vues comme des surfaces de Riemann et donc, cet exposé a deux objectifs: me permettre d'avoir votre point de vue de géomètres sur ces objets et ainsi éclaircir ma vision des choses mais aussi vous faire découvrir ou redécouvrir ce qu'est une courbe modulaire.

Pour cela, nous allons construire pas à pas $X(1)$ qui est la plus simple et la plus fondamentale de ces courbes. Les pré-requis sont la connaissance de \mathbb{C} et des matrices 2×2 . Nous n'admettrons aucun résultat jusqu'à ce que $X(1)$ soit construite comme surface de Riemann. Ensuite, je vous montrerai comment construire d'autres courbes modulaires sur le même modèle, comment les courbes modulaires ont un lien étroit avec les courbes elliptiques et jouent donc un rôle crucial en théorie des nombres et peut-être quelques mots sur les formes modulaires. Ces derniers points seront abordés s'une manière plus culturelle. En effet, tout développement rigoureux au sujet des courbes elliptiques ou des formes modulaires prendrait plusieurs heures et seraient bien éloignés de la géométrie. De plus, je suis encore loin d'être qualifié pour vous présenter quelque chose à ce sujet...

2. Action de $PSL_2(\mathbb{Z})$ sur \mathcal{H}

Definition 1. — Pour tout anneau commutatif R , on notera

$$SL_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid (a, b, c, d) \in R^4, ad - bc = 1 \right\},$$

$$PSL_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid (a, b, c, d) \in R^4, ad - bc = 1 \right\} / \{I, -I\}.$$

Definition 2. — Soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ et $z \in \mathbb{P}^1(\mathbb{C})$. On définit si $z \neq \infty$:

$$\gamma z = \frac{az + b}{cz + d},$$

et

$$g_\infty = \frac{a}{c}.$$

Lemme 3. — Cette application définit une opération du groupe $SL_2(\mathbb{R})$ sur $\mathbb{P}^1(\mathbb{C})$. Les seules matrices qui agissent trivialement sont I et $-I$. Autrement dit, $PSL_2(\mathbb{R})$ agit fidèlement sur $\mathbb{P}^1(\mathbb{C})$.

Démonstration. — Il suffit de montrer que si $\gamma, \gamma' \in SL_2(\mathbb{R})$, on a $(\gamma\gamma')(z) = \gamma(\gamma'z)$ pour tout $z \in \mathbb{P}^1(\mathbb{C})$. Ensuite, on résout $z = \gamma z$ pour obtenir $\gamma = \pm I$. \square

Definition 4. — On note \mathcal{H} et on appelle demi-plan de Poincaré

$$\mathcal{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}.$$

A partir de maintenant, on notera $\Gamma := PSL_2(\mathbb{Z})$ le **groupe modulaire**.

Lemme 5. — Γ agit sur \mathcal{H} et, pour tout $(\gamma, z) \in \Gamma \times \mathcal{H}$, on a

$$\Im(\gamma z) = |cz + d|^{-2} \Im(z).$$

Démonstration. — Il suffit de calculer... \square

3. Un domaine fondamental pour Γ

Definition 6. — Un **domaine fondamental** de \mathcal{H} pour le groupe Γ est une partie ouverte F de \mathcal{H} qui ne rencontre toute orbite de H qu'en un seul point et dont l'adhérence \overline{F} contient au moins un point de chaque orbite.

Ici, il faut dessiner F et montrer que c'est bien un domaine fondamental:

Proposition 7. — L'ensemble $F = \{z \in \mathcal{H} \mid |\Re(z)| < \frac{1}{2}, |z| > 1\}$ est un domaine fondamental de \mathcal{H} pour Γ . Les seuls points de \overline{F} dont le groupe d'isotropie n'est pas trivial sont $i = \exp(i\frac{\pi}{2})$, $\rho = \exp(i\frac{\pi}{3})$ et ρ^2 . Si on note

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

et Γ_z le groupe d'isotropie de z , on a

$$\Gamma_i = \{I, S\}$$

et

$$\Gamma_\rho = \{ST, (ST)^2, I\}.$$

Avant de démontrer cette proposition-clé, remarquons le fait suivant:

Lemme 8. — Soit $z \in \mathcal{H}$. Dans l'orbite de z sous l'action de Γ , il n'y a qu'un nombre fini d'ordonnés supérieures à une ordonnée fixée. En particulier, il y a des points dans cette orbite d'ordonnée maximale.

Démonstration. — C'est évident d'après la formule sur la partie imaginaire de γz et le fait que les points de la forme $cz + d$ forment un ensemble discret. \square

On peut maintenant prouver la proposition.

Démonstration. — Il est facile de ramener tout point z de \mathcal{H} dans \overline{F} . Il suffit de choisir un point de l'orbite de z d'ordonnée maximale et de le translater par action de T^m dans la bande verticale $|x| \leq \frac{1}{2}$. On doit avoir $|z| \geq 1$ sinon on fait agir S et on contredit la maximalité de l'ordonnée de z .

Il reste à décrire dans quelles conditions on peut avoir $z, z' \in \overline{F}$, $\gamma \in \Gamma$ et $z' = \gamma z$.

Premier cas: $\gamma = T^n$ est une translation horizontale. Alors $n = 1$ et z et z' appartiennent aux deux frontières verticales.

Supposons qu'on ne soit pas dans ce cas. Alors, si on note $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a $(c, d) \neq (0, 0)$ et $(c, d) \neq (0, \pm 1)$. Dans ce cas,

$$|cz + d|^2 = (cx + d)^2 + c^2y^2 = c^2(x^2 + y^2) + 2cdx + d^2 \geq c^2 - |cd| + d^2 \geq 1,$$

et donc $\Im(z') \leq \Im(z)$. On peut faire pareil avec $z = \gamma'z'$ et on obtient finalement $\Im(z) = \Im(z')$. Ainsi,

$$c^2 - |cd| + d^2 = 1.$$

Il ne reste que les cas $(c, d) = (\pm 1, \pm 1)$ et $(c, d) = (\pm 1, 0)$. Dans les deux cas, il suffit de combiner $|cz + d| = 1$ et le fait que les matrices sont de déterminant 1 pour obtenir le résultat. \square

4. Définition et compactification de la courbe modulaire

Nous avons maintenant tout en main pour définir la courbe modulaire.

Définition 9. — On note $Y(1)$ le quotient $\Gamma \backslash \mathcal{H}$.

En fait, il s'agit de coller les deux frontières verticales de F ainsi que de plier en deux l'arc de cercle au-niveau de i . Le problème est que la surface ainsi formée n'est pas compacte. On va lui rajouter un point pour qu'elle le devienne.

Pour cela, on définit

$$\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}.$$

Comme système fondamental de voisinages pour ∞ , on choisit les parties de \mathcal{H} au-dessus d'une droite horizontale donnée. On peut montrer que Γ agit transitivement sur $\mathbb{Q} \cup \{\infty\}$. On définit alors les voisinages de $r = \gamma\infty \in \mathbb{Q}$ comme les images par γ des voisinages de ∞ . Comme système fondamental de voisinages pour $r \in \mathbb{Q}$, on peut montrer qu'on obtient l'union de $\{r\}$ et de l'intérieur des disques tangents en r à l'axe réel.

On peut noter que ce n'est pas la topologie usuelle sur l'axe réel.

Ainsi, on peut définir

$$X(1) = \Gamma \backslash \mathcal{H}^*,$$

qui est compact (on n'a rajouté qu'un point en fait qu'on appelle pointe, comme si les deux frontières verticales de F se rejoignaient.).

On montre facilement que $\Gamma_\infty = \{T^n\}_{n \in \mathbb{Z}}$.

5. $X(1)$ est une surface de Riemann de genre 0

Pour pouvoir définir des voisinages de tous les points de $X(1)$, nous aurons besoin de la proposition fondamentale suivante.

Montrons d'abord le lemme suivant:

Lemme 10. — *Pour tous $z, z' \in \mathcal{H} \cup \{\infty\}$, il existe des voisinages V et V' de z et z' tels que l'ensemble des $\gamma \in \Gamma$ tels que $\gamma V \cap V' \neq \emptyset$ est fini.*

Démonstration. — Soit d'abord $z, z' \in \mathcal{H}$. On peut choisir comme voisinages U et U' des disques centré en z et z' de rayon R et R' aussi petits qu'on le souhaite. Il n'y a qu'un nombre fini de couples (c, d) vérifiant $|cz + d|^2 < 100\Im(z)/\Im(z')$ (faire un dessin du réseau) (on notera $\gamma \in \Gamma'$ si γ est une matrice correspondant à ces couples (c, d)). Il y a une infinité de matrices dans Γ' mais pour chaque (c, d) , les images de U par ces matrices sont des disques situés dans la même bande horizontale, de même rayon; ceux de ces cercles qui coupent U' sont clairement en nombre fini) Lorsque ζ parcourt le voisinage choisi U , $c\zeta + d$ parcourt un disque de rayon $|cR|$ centré en $cz + d$. On peut donc choisir R assez petit (faire un dessin du réseau) (inférieur à $1/2$ de la distance entre deux lignes horizontales du réseau au-dessus du disque $|z| < 10\sqrt{\Im(z)/\Im(z')}$ divisé par le c correspondant à la ligne la plus près du disque) pour que tous ces disques n'intersectent pas $\{|z| < 10\}$ (exceptés un nombre fini sur les lignes en-dessous ou sur les côtés, on peut prendre R encore plus petit pour qu'il n'y en ait pas du tout). Ainsi, si on note M l'ordonnée maximale des points de U , toutes les points des images du voisinage U par des matrices qui ne sont pas dans Γ' ont pour ordonnée maximale $M\Im(z')/(100\Im(z'))$ et ainsi, ces images ne peuvent pas intersecter U' (si R est suffisamment petit), d'où le résultat.

Considérons maintenant le cas $z = z' = \infty$. Choisissons comme voisinage V_Y les points $x + iy$ avec $y > Y$, cette borne étant fixé. Ainsi, pour tous $\gamma \in \Gamma$ et $z \in V_Y$, on a

$$\Im(\gamma z) = \frac{1}{|cx + d + iy|^2} \Im(z) \leq \frac{y}{(cx + d)^2 + y^2} \leq \frac{1}{y} < \frac{1}{Y}.$$

Il suffit donc d'avoir $Y > \frac{1}{Y}$ pour que les voisinages γV_Y soient sans intersection avec V_Y .

Le cas $z \in \mathcal{H}$ et $z' = \infty$ est trivial. \square

Corollaire 11. — $X(1)$ est un espace topologique séparé.

Démonstration. — Soit x et y dans \mathcal{H} qui ne sont pas dans la même orbite. On peut choisir deux voisinages A et B de x et y comme dans le lemme précédent. Soient $\{\gamma_1, \dots, \gamma_n\}$ les éléments de Γ tels que $\gamma_i A \cap B \neq \emptyset$. On a clairement $\gamma_i x \neq y$ et donc, on peut définir des voisinages distincts U_i de $\gamma_i x$ et V_i de y . On pose alors

$$U = A \cap_{1 \leq i \leq n} \gamma_i^{-1} U_i; \quad V = B \cap_{1 \leq i \leq n} V_i.$$

Les images de U et V dans $X(1)$ sont bien des voisinages distincts de Γx et Γy .

Si x ou y est l'antécédent de la pointe, on le prend égal à ∞ . \square

Proposition 12. — Pour tout $z \in \mathcal{H} \cup \{\infty\}$, il existe un voisinage U de z tel que $U \cap \gamma U \neq \emptyset$ implique $\gamma \in \Gamma_z$.

Démonstration. — Soit V le voisinage de z défini dans le lemme précédent ($z = z'$). Il y a un nombre fini d'éléments de Γ tel que $\gamma V \cap V \neq \emptyset$. Notons-les $\{\gamma_1, \dots, \gamma_n\}$ où $\gamma_i \in \Gamma_z$ pour $i \leq s \leq n$. Pour $i > s$ choisissons des voisinages disjoints V_i de z et W_i de $\gamma_i z$ et posons

$$U = V \cap \left(\bigcap_{i > s} (V_i \cap \gamma_i^{-1} W_i) \right).$$

Pour $i > s$, $\gamma_i U \subseteq W_i$ qui est disjoint de V_i qui contient U . \square

On a aussi clairement la conséquence suivante.

Corollaire 13. — Soit $z \in \mathcal{H} \cup \{\infty\}$, et U le voisinage défini dans la proposition précédente. L'application suivante est injective et permet de prendre $\Gamma_z \backslash U$ comme voisinage ouvert de $[z] \in X(1)$:

$$p : \Gamma_z \backslash U \hookrightarrow \Gamma \backslash \mathcal{H}^*.$$

Il ne reste qu'à donner les fonctions coordonnées sur ces voisinages qui feront de $X(1)$ une surface de Riemann. Pour z différent de $[i]$, $[\rho]$ et $[\infty]$, Γ_z est trivial et on prendra l'application p^{-1} , c'est-à-dire "grosso modo" l'identité. Il reste à déterminer des fonctions holomorphes (et de réciproque holomorphe du coup) définies sur les $\Gamma_z \backslash U$.

On prendra:

- Pour i , $f_i(z) = \left(\frac{z-i}{z+1}\right)^2$,
- pour rho , $f_j(z) = \left(\frac{z-\rho^2}{z-\bar{\rho}^2}\right)^3$,
- pour ∞ , $f_\infty = \exp(2i\pi z)$.

On vérifie facilement que $X(1)$ est ainsi équipée d'une structure de surface de Riemann.

Proposition 14. — $X(1)$ est de genre 0.

Démonstration. — Par construction, il semble bien que $X(1)$ soit topologiquement isomorphe à une sphère. On pourrait dire que la sphère de Riemann est la seule surface de Riemann compacte simplement connexe (je l'ai lu quelque part!) Pour montrer qu'elle est bien de genre 0, nous allons utiliser la caractéristique d'Euler qui dépend d'une part du genre ($= 2g - 2$) et d'autre part du nombre de sommets, faces et arêtes de la surface une fois triangulée par exemple (ρ , i et ∞ et un quatrième sommet) ($S - A + F = 4 - 6 + 4$). On obtient bien $g = 0$. \square

6. Prolongements. Intéprétation de $X(1)$

1. Une **courbe elliptique** est \mathbb{C} quotienté par un ceratin réseau. On peut voir la courbe comme un tore. On dira que ces courbes sont isomorphes (au sens des surfaces de Riemann) si les réseaux qui les définissent sont proportionnels. En multipliant le réseau par un nombre complexe convenable, on peut se ramener à $\mathbb{Z} + \tau\mathbb{Z}$ où $\tau \in \mathcal{H}$. En faisant agir un èlément de Γ sur le réseau, on ne le modifie pas. En fait, on peut associer à tout point de $X(1)$ une classe d'isomorphisme de courbes elliptiques. Des résultats sur les points de $X(1)$ peuvent donc avoir une interprétation en ces termes...
2. On peut faire la même construction en quotientant par des sous-groupes de Γ . Parmi cela, on peut remarquer **les sous-groupes dits de congruence**, c'est-à-dire ceux qui contiennent

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \pmod{N} \right\}.$$

Il y a par exemple ceux où c est multiple de N . N est appelé le niveau. Ces groupes ont une importance arithmétique. Par exemple, à un point de la courbe modulaire $X(N)$ on peut associer une classe d'isomorphisme de (courbes elliptiques+sous-groupe cyclique d'ordre N) (incapable de rentrer dans les détails, cf Milne). Le genre et le nombre de pointes sont connues

et donnés par exemple dans le livre de Shimura. On peut également faire de la géométrie (reêtements, ramifications, domaine fondamental...)

3. En théorie des nombres, on retrouve dans nombre de domaines **les formes modulaires**. Ce sont des fonctions vérifiant $f(\gamma z) = (cz + d)^k f(z)$ et holomorphe sur \mathcal{H} et dont le développement en série de Fourier en ∞ (à justifier par l'invariance par translation) ne compte pas de puissances négatives de $q = \exp(2i\pi z)$. k est appelé le poids et on peut construire en divisant des formes modulaires de même poids des fonctions définies sur la courbe modulaire. On peut citer la plus célèbre qui est le j -invariant qui est un isomorphisme entre $X(1)$ et $\mathbb{P}^1(\mathbb{C})$. C'est le même que l'invariant j qui caractérise les classes d'isomorphismes de courbes elliptiques. Elle est fondamentale: on peut dire que $\mathbb{C}(X(1))$ le corps des fonctions méromorphes est $\mathbb{C}(j)$ et que $\mathbb{C}(X_0(N)) = \mathbb{C}(j, j_N)$.
4. Enfin, on a pas mal entendu parler des courbes modulaires lors de la preuve de Wiles du dernier théorème de Fermat. Juste un mot là-dessus. En fait, il a démontré un cas particulier de l'ancienne **la conjecture de Taniyama et Shimura** qui dit la chose suivante et qui a été montrée en 1997 par un groupe de mathématiciens (paramétrisation des courbes elliptiques)

Pour toute courbe elliptique E définie sur \mathbb{Q} , il existe $N \in \mathbb{N}$ et un morphisme algébrique surjectif $\phi : X_0(N) \rightarrow E$ défini sur \mathbb{Q} . (forme faible) C'est surtout pour montrer l'importance que ces objets peuvent avoir.