Courbes elliptiques

Master Class *Arithmétique et Géométrie Algébrique*

Rutger Noot

Dans le groupe additif $\mathbf{C}$ des nombres complexes, considérons un sous groupe de la forme $\Lambda = \{m + n\tau \mid m, n \in \mathbf{Z}\}$, pour $\tau \in \mathbf{C}$ avec $\mathrm{im}(\tau) > 0$ fixé. Le quotient $\mathbf{C}/\Lambda$ n'est pas seulement un groupe, mais aussi une *surface de Riemann* : une variété où chaque point possède un voisinage isomorphe à un disque ouvert dans $\mathbf{C}$. On montrera que $\mathbf{C}/\Lambda$ est isomorphe à une *courbe elliptique* : l'ensemble des solutions dans $\mathbf{P}^2(\mathbf{C})$ d'une équation de la forme $y^2z = P(x, z)$ où P est un polynôme homogène de degré 3. Le réciproque est vrai aussi, toute courbe elliptique est isomorphe à $\mathbf{C}/\Lambda$ pour un sous-groupe $\Lambda \subset \mathbf{C}$ approprié. L'ensemble des applications *holomorphes* $\mathbf{C}/\Lambda \to \mathbf{C}/\Lambda'$ est alors en bijection avec celui des applications *polynomiales* entre les courbes projectives correspondantes. Cela veut dire en particulier qu'une courbe elliptique est munie d'une loi de groupe définie par des applications polynomiales.

On étudiera cette construction remarquable, en s'intéressant particulièrement au cas où l'équation $y^2z = P(x, z)$ est à coefficients algébriques et où il a donc un sens de s'intéresser aux solutions *algébriques*, c'est-à-dire dans $\mathbf{P}^2(\overline{\mathbf{Q}})$.

Des phénomènes semblables se produisent pour les *courbes modulaires* : des quotients de la forme $\mathbf{H}/\mathrm{SL}_2(\mathbf{Z})$ où $\mathbf{H} = \{z \in \mathbf{C} \mid \mathrm{im}(z) > 0\}$ et $\mathrm{SL}_2(\mathbf{Z})$ opère sur $\mathbf{H}$ par des transformations de Moebius

$$z \mapsto \frac{az + b}{cz + d}.$$

Les propriétés géométriques et arithmétiques des courbes elliptiques et les courbes modulaires ont été étudiées depuis plusieurs siècles. La théorie a joué un rôle fondamentale dans la démonstration du théorème de Fermat.