Groupes et Courbes Algébriques

Michel Jambu

Professeur Émérite
Laboratoire J. A Dieudonné, Université Côte d'Azur
Nice, France

La notion de groupe est centrale en mathématiques et dans ce mini-cours, nous montrerons que certaines courbes algébriques, i.e. définies par des polynômes, possèdent une structure "naturelle" de groupe abélien. Par exemple, une droite, un cercle qui sont des courbes définies par une équation polynomiale à deux variables, sont aussi des groupes abéliens.
Un exemple, sans doute beaucoup moins évident, est celui des courbes elliptiques. Ces courbes jouent un rôle très important en cryptographie.
Dans un premier temps, nous examinerons en détails le cas du cercle et son addition naturelle qui en fait un groupe abélien et nous expliquerons que le cadre du plan projectif est nécessaire.
Le cercle est une conique (ellipse) très particulière et nous montrerons comment étendre les résultats précédents aux coniques. Un résultat très important de géométrie classique, le théorème de Pascal sera introduit. Ce théorème permettra d'affirmer que l'addition est une loi associative.
Une conique est définie par un polynôme de degré deux. Ce polynôme peut dégénérer en un produit de deux polynômes de degrés un, ce qui signifie que la courbe algébrique associée est composée de deux droites. Les résultats obtenus sur les coniques seront étendus aux deux droites. En particulier, le théorème de Pappus remplacera le théorème de Pascal.
La seconde partie de ce cours sera consacrée aux courbes elliptiques et nous verrons les liens très étroits avec la première partie. Les courbes elliptiques sont équipées d'une structure de groupe abélien et nous montrerons que cette addition est naturellement une extension de l'addition sur le cercle. L'associativité de l'addition est le point non trivial et le théorème de Cayley-Bacharach dont les corollaires sont les théorèmes de Pascal et de Pappus, est le résultat qui permet de montrer l'associativité.
Finalement, les courbes elliptiques peuvent être vues comme des courbes d'Edwards (introduites en 2007 par Edwards) qui sont des déformations du cercle et nous pourrons montrer que les additions sur les courbes elliptiques et sur le cercle ne sont qu'un seul et même concept.
Toutes les notions introduites dans ce cours seront définies et aucun prérequis particulier n'est nécessaire.