Structure de groupe sur les courbes elliptiques réelles

2 juillet 2024

Une courbe elliptique réelle est une courbe donnée par une équation cubique de la forme

$$y^2 + axy + by = x^3 + cx^2 + dx + e \tag{1}$$

L'intérêt majeur d'une telle courbe réside dans l'existence d'une structure naturelle de groupe commutatif sur l'ensemble de ses points (en incluant le point à l'infini).

Dans un premier temps, à l'aide d'un changement de variable adapté, on se ramènera à l'équation de Weierstraß qui est une forme réduite de l'équation (1) puis on donnera une construction géométrique de la loi de composition sur les points de la courbe. Dans un second temps, on vérifiera que cette loi est bien une loi de groupe commutatif (i.e. existence du neutre, inversibilité, commutativité et associativité).

S'il reste du temps, on pourra s'intéresser aux courbes elliptiques sur un autre corps (par exemple $\mathbb{C}$, $\mathbb{Q}$ ou $\mathbb{F}_p$).