9. Elliptic Curves

A very special feature of a non-singular cubic curve C is the existence of an abelian group structure on the set of points in C. We will see how that works.

9.1. **The group law on non-singular cubics.** Given any non-singular cubic C and any point $O \in C$, there exists an abelian group structure on the set of points in C, with O being the identity element in the group law. That means, there is a binary operation "+" defined on the set of points in C, which satisfies the conditions required in the definition of an abelian group. The identity element O in the group law is also called the *neutral point*. We will first describe the operation geometrically, then show some explicit computations, finally explain why the construction defines an abelian group structure.

Construction 9.1 (The group law)**.** Given a non-singular cubic curve C with a point $O \in C$, there is an abelian group law on the set of points on C such that O is the identity element. For any two points $A, B \in C$, their sum $A + B$ is obtained in two steps

(1) The line AB meets the cubic C at a third point R;

(2) The line OR meets the cubic C at a third point $\overline{R} = A + B$.

If $A = B$ (resp. $O = R$), then the line AB (resp. OR) is defined to be the tangent line $T_A C$ (resp. $T_O C$). □

We can follow the above construction to make explicity computations. In each step, we need to write down the equation of a certain line, and compute its intersection points with the cubic. The reason for the existence of the third intersection point of a line and a cubic and the method for computing it has been discussed in the proof of Theorem 8.8. To find the line AB (or similarly OR), we need Definition 7.8 if $A = B$, or the follow simple result if $A \neq B$.

Lemma 9.2. *Given two distinct points $A = [a_0 : a_1 : a_2]$ and $B = [b_0 : b_1 : b_2]$ in $\mathbb{P}^2$, there is a unique line L passing through the two points, defined by the polynomial*

$$f(x, y, z) = \det \begin{pmatrix} x & a_0 & b_0 \\ y & a_1 & b_1 \\ z & a_2 & b_2 \end{pmatrix}.$$

Proof. We have seen in Exercise 4.3 (1) that there is a unique line L passing through A and B. It remains to verify that the given polynoial defines such a line. Notice that the given polynomial is non-zero and homogeneous of degree 1 hence defines a line. When $[x : y : z] = [a_0 : a_1 : a_2]$ or $[b_0 : b_1 : b_2]$, two columns of the matrix are identical hence the determinant is zero. This shows that A and B are points on this line. □

Example 9.3. Consider the cubic $C = \mathbb{V}(y^2z - x^3 + 4xz^2 - z^3)$ with the identity element $O = [0 : 1 : 0]$. Take two points $A = [2 : 1 : 1]$ and $B = [-2 : 1 : 1]$ on C. By Lemma 9.2, the line AB is defined by

$$\det \begin{pmatrix} x & 2 & -2 \\ y & 1 & 1 \\ z & 1 & 1 \end{pmatrix} = -4y + 4z.$$

By the method in the proof of Theorem 8.8, we can find the third intersection point R of AB and C to be $R = [0 : 1 : 1]$. By Lemma 9.2, the line OR is defined by

$$\det \begin{pmatrix} x & 0 & 0 \\ y & 1 & 1 \\ z & 0 & 1 \end{pmatrix} = x.$$

By the method in the proof of Theorem 8.8, we can find the third intersection point $\overline{R}$ of OR and C to be $\overline{R} = [0 : -1 : 1]$. Therefore $A + B = [0 : -1 : 1]$.

Construction 9.1 works for any non-singular cubic with any point on it as the identity element. In some special cases, the group law becomes particularly nice and simple. This simplified group law is applicable only when the following two conditions are satisfied

(1) The non-singular cubic is given by $C = \mathbb{V}_p(y^2z - x^3 - ax^2z - bxz^2 - cz^3)$ for some $a, b, c \in \Bbbk$, which is the projective closure of the affine curve $C_2 = \mathbb{V}_a(y^2 - x^3 - ax^2 - bx - c)$ with the only point $O = [0 : 1 : 0]$ at infinity;

(2) The point at infinity $O = [0 : 1 : 0]$ is the identity element.

It is important to observe that the graph of C_2 is symmetric with respect to the x-axis.

Construction 9.4 (Simplified group law)**.** Let $C = \mathbb{V}_p(y^2z - x^3 - ax^2z - bxz^2 - cz^3)$ be a non-singular cubic for some $a, b, c \in \Bbbk$. Let $O = [0 : 1 : 0]$ be the identity element of the group law and $C_2 = \mathbb{V}_a(y^2 - x^3 - ax^2 - bx - c)$ a standard affine piece of C. Given two points $A, B \in C$, we have:

(1) If $A = O$, then $A + B = B$; if $B = O$, then $A + B = A$;

(2) If $A, B \in C_2$, assume the line AB meet the cubic C at a third point R. If $A = B$, the line AB is defined to be the tangent line T_AC.

   (a) If A and B are symmetric with respect to the x-axis, then $A + B = O$;

   (b) Otherwise, let $R = (p, q) \in C_2$, then $\overline{R} = (p, -q) = A + B$. □

Remark 9.5. The simplified group law 9.4 also gives an easy way to compute the inverse of any point $A \in C$. If $A = O$, then $-A = O$. Otherwise, let $A = (x, y) \in C_2$, then the inverse $-A = (x, -y) \in C_2$ which is the reflection of A across the x-axis.

Example 9.6. We look at Example 9.3 again. It is clear that both conditions required for the simplified group law are met. The affine curve $C_2 = \mathbb{V}_a(y^2 - x^3 + 4x - 1)$. Neither A nor B is the identity element $O = [0 : 1 : 0]$. In non-homogeneous coordinates, $A = (2, 1)$ and $B = (-2, 1)$. The line AB in the affine plane is given by $L_2 = \mathbb{V}_a(y - 1)$. Solving the system given by equations $y^2 - x^3 + 4x - 1 = 0$ and $y - 1 = 0$, we get the third point of intersection $R = (0, 1)$. Therefore $A + B = \overline{R} = (0, -1)$, or in homogeneous coordinates $[0 : -1 : 1]$. This answer is consistent with that of Example 9.3.

Definition 9.7. A non-singular cubic curve with a chosen point on it as the identity element in the group law is called an *elliptic curve*.

The theory of elliptic curves is extremely rich and deep, and provides a good example of the profound connections between abstract algebraic geometry, complex analysis, and number theory. It constitutes an active area of current research, and plays a crucial role in the recent proof of Fermat's Last Theorem. Elliptic curves also have important applications in various aspects of cryptography, such as encryption, digital signatures, (pseudo-)random generators and so on. There are other higher dimensional projective varieties, on which there exist abelian group laws. They are called *abelian varieties*, which is also a major branch of algebraic geometry.