9.2. **Linear systems and associativity.** We are aiming to prove that Construction 9.1 does define an abelian group law. The difficulty here is the associativity. We clear up the easy bits first.

Proposition 9.8. *In Construction 9.1 of the group law on a non-singular cubic curve C: the addition is commutative; O is the identity element; and every point has an inverse.*

Proof. For two points $A, B \in C$, there is no difference between the line AB and the line BA, hence $A + B = B + A$ is obvious. This justifies the commutativity.

To find $A+O$, the first step gives the third intersection point R of the line AO and C; the second step gives the third intersection point of the line OR and C, which is A. Hence $A + O = A$ is also obvious. This justifies that O is the identity element in the group law.

Given any $A \in C$, we claim its inverse can be given like this: assume the tangent line $T_O C$ meets C at a third point $\overline{O}$, and the line $A\overline{O}$ meets C at a third point B, then B is the inverse of A. We need to verify $A + B = O$. To compute $A + B$, the first step gives the third intersection point of the line AB and C, which is $\overline{O}$; the second step gives the third intersection point of the line $O\overline{O}$ and C, which is O by Proposition 8.11. This justifies $A + B = O$, hence the inverse of A is well-defined. □

Remark 9.9. Here is a special case that is worth mentioning: if O is an inflection point, then $T_O C$ meet C at O three times hence $\overline{O} = O$. In such a case the inverse of A is simply the third intersection point of the line AO and the curve C.

It remains to check the associativity in the group law. This requires some preparation, which is very interesting in their own stand.

Notation 9.10. Given finitely many points $P_1, \cdots, P_k \in \mathbb{P}^2$. For every $d \geqslant 0$, we write

$$S_d(P_1, \cdots, P_k) := \left\{ f \in \Bbbk[x, y, z] \;\middle|\; \begin{array}{c} f \text{ is homogeneous of degree } d \\ f(P_1) = \cdots = f(P_k) = 0 \end{array} \right\}.$$

It is easy to see that $S_d(P_1, \cdots, P_k)$ is a vector space over $\Bbbk$, as it is closed under addition and scalar multiplication. This vector space is sometimes called a *linear system*, but we do not need this terminology. In the following results we will need to look at $S_3(P_1, \cdots, P_8)$.

Lemma 9.11. *Let C_1 and C_2 be two cubic curves whose intersection consists of precisely 9 distinct points $P_1, \cdots, P_9$. Then $\dim_{\Bbbk} S_3(P_1, \cdots, P_8) = 2$.*

Proof. Non-examinable. We do not prove it but we explain what the proof is really about. It is easy to find out that a homogeneous polynomial $f \in \Bbbk[x, y, z]$ of degree 3 is determined by 10 coefficients. For each given point P_i, the requirement $f(P_i) = 0$ imposes one linear condition on the coefficients of f. If all the 8 linear conditions on the coeffcients are independent, then the remaining freedom in the coefficient is 2, which is precisely what we need. Therefore the whole point is to show that these linear conditions are guaranteed to be independent given the assumptions. The key ingredient in the proof is Bézout's Theorem 8.13. Interested reader can find the proof in [Proposition 2.6, Reid, Undergraduate Algebraic Geometry]. □

Lemma 9.12. *Let $C_1 = \mathbb{V}(F_1)$ and $C_2 = \mathbb{V}(F_2)$ be two cubic curves whose intersection consists of precisely 9 distinct points $P_1, \cdots, P_9$. Then any cubic curve $D = \mathbb{V}(G)$ through $P_1, \cdots, P_8$ also passes through P_9.*

Proof. By Lemma 9.11, we have $\dim_{\Bbbk} S_3(P_1, \cdots, P_8) = 2$. It is clear that $F_1, F_2 \in S_3(P_1, \cdots, P_8)$. Moreover F_1 and F_2 are linearly independent, as otherwise they would define the same cubic. Therefore F_1 and F_2 form a basis of $S_3(P_1, \cdots, P_8)$. Since $G \in S_3(P_1, \cdots, P_8)$, we can write $G = \lambda_1 F_1 + \lambda_2 F_2$ for some $\lambda_1, \lambda_2 \in \Bbbk$. Now $G(P_9) = \lambda_1 F_1(P_9) + \lambda_2 F_2(P_9) = 0$, hence D passes through P_9. □

Now we are ready to prove the associativity. To avoid excessive technicality while still keeping a grasp of the main idea in the proof, we will prove it under an extra mild assumption, which will be stated in the proof. Some extra work will be required if this assumption is not met, which we do not discuss.

Proposition 9.13. *In Construction 9.1 of the group law on a non-singular cubic curve C, the addition is associative.*

Proof. Let $A, B, E \in C$. The construction of $(A + B) + E = \overline{S}$ uses 4 lines:

$$L_1 : ABR; \quad L_2 : RO\overline{R}; \quad L_3 : E\overline{R}S; \quad L_4 : SO\overline{S}.$$

The construction of $A + (B + E) = \overline{T}$ uses 4 lines:

$$M_1 : BEQ; \quad M_2 : QO\overline{Q}; \quad M_3 : A\overline{Q}T; \quad M_4 : TO\overline{T}.$$

We need to show $\overline{S} = \overline{T}$, for which it suffices to show $S = T$. We consider two cubics

$$D_1 = L_1 \cup M_2 \cup L_3 \qquad \text{and} \qquad D_2 = M_1 \cup L_2 \cup M_3.$$

Then by construction we have

$$C \cap D_1 = \{A, B, E, O, R, \overline{R}, Q, \overline{Q}, S\};$$
$$C \cap D_2 = \{A, B, E, O, R, \overline{R}, Q, \overline{Q}, T\}.$$

Now we need a mild assumption that the 9 points in $C \cap D_1$ are distinct. Then the two cubics C and D_1 satisfy the conditions of Lemma 9.12. Since the cubic D_2 passes through 8 of the 9 points, it must pass through S as well, which means $S \in C \cap D_2$. Therefore $S = T$ since S cannot be any of the other points by the mild assumption that we imposed. This finishes the proof under this assumption. Extra work has to be done when this assumption is not met. □

Remark 9.14. This is a very beautiful piece of argument in projective algebraic geometry. Bézout's theorem plays a key role in the course of the proof, mostly in the proof of Lemma 9.11. A similar argument can be used to prove many other results, including the famous Pascal's theorem (aka the mystic hexagon), which we will see in the exercise.