(III) I think I'll leave $A + B = B + A$ to the reader.

(IV) To find the inverse, first define the point $\overline{O}$ as in (i) of the construction: let L be the line such that $F|L$ has O as a repeated zero, and define $\overline{O}$ to be the 3rd point of intersection of L with C; then it is easy to check that the 3rd point of intersection of $\overline{O}A$ with C is the inverse of A for every $A \in C$.

2.9 Associativity "in general"

Now I give the proof of associativity for 'sufficiently general' points: suppose that A, B, C are 3 given points of C; then the construction of $(A + B) + C = \overline{S}$ uses 4 lines (see diagram above)

$$L_1 : ABR, \quad L_2 : RO\overline{R}, \quad L_3 : C\overline{R}S \quad \text{and} \quad L_4 : SO\overline{S}.$$

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

$$M_1 : BCQ, \quad M_2 : QO\overline{Q}, \quad M_3 : A\overline{Q}T \quad \text{and} \quad M_4 : TO\overline{T}.$$

I want to prove $\overline{S} = \overline{T}$, and clearly for this, it is enough to prove $S = T$; to do this, consider the 2 cubics

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

Then by construction,

$$\begin{aligned} C \cap D_1 &= \{A, B, C, O, R, \overline{R}, Q, \overline{Q}, S\}, \\ \text{and} \quad C \cap D_2 &= \{A, B, C, O, R, \overline{R}, Q, \overline{Q}, T\}. \end{aligned}$$

Now provided the 9 points $A, B, C, O, R, \overline{R}, Q, \overline{Q}, S$ are all distinct, the two cubics C and D_1 satisfy the conditions of Corollary 2.7; therefore, D_2 must pass through S, and the only way that this can happen is if $S = T$.

There are several ways to complete the argument. The most thorough of these gives a genuine treatment of the intersection of two curves taking into account multiple intersections (roughly, in terms of 'ideals of intersection'), and the statement corresponding to Corollary 2.7 is Max Noether's Lemma (see [Fulton, p. 120 and p. 124]).

2.10 Proof by continuity

I sketch one version of the argument 'by continuity', which uses the fact that $k \subset \mathbb{C}$. Write $C_{\mathbb{C}} \subset \mathbb{P}^2_{\mathbb{C}}$ for the complexified curve C, that is, the set of ratios $(X : Y : Z)$ of complex numbers satisfying the same equation $F(X, Y, Z) = 0$. If the associative law holds for all $A, B, C \in C_{\mathbb{C}}$, then obviously also for all points in C. Therefore, I can assume that $k = \mathbb{C}$.

The reader who cares about it will have no difficulty in finding proofs of the following two statements (see Ex. 2.8):

Lemma *(i) $A + B$ is a continuous function of A and B;*

(ii) for all $A, B, C \in C$ there exist $A', B', C' \in C$ arbitrarily near to A, B, C such that the 9 points $A', B', C', O, R, \overline{R}, Q, \overline{Q}, S$ constructed from them are all distinct.

The addition law is a map $\varphi\colon C \times C \to C$ given by $(A, B) \mapsto A + B$. By (i), φ is continuous, and hence so are the two maps (sorry!)

$$f = \varphi \circ (\varphi \times \mathrm{id}_C) \quad \text{and} \quad g = \varphi \circ (\mathrm{id}_C \times \varphi)\colon C \times C \times C \to C$$

given by $(A, B, C) \mapsto (A + B) + C$ and $A + (B + C)$. Also, by (ii), the subset $U \subset C \times C \times C$ consisting of triples (A, B, C) for which the 9 points of the construction are distinct is dense; by the above argument, f and g thus coincide on U, and since they are continuous, they coincide everywhere. Q.E.D.

Remark The continuity argument as it stands involves the topology of $\mathbb{C}$, and is thus not purely algebraic. In fact the addition map φ is a morphism of varieties $\varphi\colon C \times C \to C$, as will be proved later (see (4.14)), and the remainder of the argument can also be reformulated in this purely algebraic form: the subset of $C \times C \times C$ for which the 9 points are distinct is a dense open set for the Zariski topology, and two morphisms which coincide on a dense open set coincide everywhere. (I hope that this remark can provide useful motivation for the rest of the course; if you find it confusing, just ignore it for the moment.)

2.11 Pascal's Theorem (the mystic hexagon)

The diagram consists of a hexagon $ABCDEF$ in $\mathbb{P}^2_k$ with pairs of opposite sides extended until

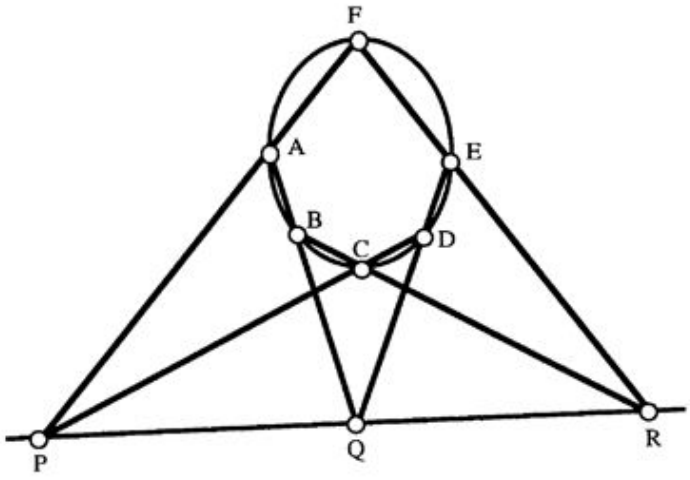

Figure 2.4: The mystic hexagon

they meet in points P, Q, R. Assume that the nine points and the six lines of the diagram are all distinct; then

$$ABCDEF \text{ are conconic} \iff PQR \text{ are collinear.}$$

This famous theorem is a rather similar application of (2.7), and is given just for fun; of course, other proofs are possible, see any text on geometry, for example [Berger, 16.2.10 and 16.8.3–5].