Second degenerate case Suppose $P_1, \dots, P_6 \in C$ are conconic, with $C : (Q = 0)$ a nondegenerate conic. Then choose $P_9 \in Q$ distinct from $P_1, \dots, P_6$. By Corollary 2.5 again,

$$S_3(P_1, \dots, P_9) = Q \cdot S_1(P_7, P_8);$$

the line $L = P_7P_8$ is unique, so that $S_3(P_1, \dots, P_9)$ is the 1-dimensional space spanned by QL, and hence $\dim S_3(P_1, \dots, P_8) \leq 2$. Q.E.D.

Corollary 2.7 *Let C_1, C_2 be two cubic curves whose intersection consists of 9 distinct points, $C_1 \cap C_2 = \{P_1, \dots, P_9\}$. Then a cubic D through $P_1, \dots, P_8$ also passes through P_9.*

Proof If 4 of the points $P_1, \dots, P_8$ were on a line L, then each of C_1 and C_2 would meet L in ≥ 4 points, and thus contain L, which contradicts the assumption on $C_1 \cap C_2$. For exactly the same reason, no 7 of the points can be conconic. Therefore the assumptions of (2.6) are satisfied, so I can conclude that

$$\dim S_3(P_1, \dots, P_8) = 2;$$

this means that the equations F_1, F_2 of the two cubics C_1, C_2 form a basis of $S_3(P_1, \dots, P_8)$, and hence $D : (G = 0)$, where $G = \lambda F_1 + \mu F_2$. Now F_1, F_2 vanish at P_9, hence so does G. Q.E.D.

2.8 Group law on a plane cubic

Suppose $k \subset \mathbb{C}$ is a subfield of $\mathbb{C}$, and $F \in k[X, Y, Z]$ a cubic form defining a (nonempty) plane curve $C : (F = 0) \subset \mathbb{P}^2_k$. Assume that F satisfies the following two conditions:

(a) F is irreducible (so that C does not contain a line or conic);

(b) for every point $P \in C$, there exists a unique line $L \subset \mathbb{P}^2_k$ such that P is a repeated zero of $F|L$.

Note that geometrically, the condition in (b) is that C should be nonsingular, and the line L referred to is the tangent line $L = T_PC$ (see Ex. 2.3). This will be motivation for the general definition of nonsingularity and tangent spaces to a variety in §6.

Fix any point $O \in C$, and make the following construction:

Construction *(i) For $A \in C$, let $\overline{A}$ = 3rd point of intersection of C with the line OA;*

(ii) for $A, B \in C$, write R = 3rd point of intersection of AB with C, and define $A + B$ by $A + B = \overline{R}$ (see diagram below).

Theorem *The above construction defines an Abelian group law on C, with O as zero (= neutral element).*

Proof Associativity is the crunch here; I start the proof by first clearing up the easy bits.

(I) I have to prove that the addition and inverse operations are well defined. If $P, Q \in C$ are any two points, then either $P \neq Q$, and the line $L = PQ \subset \mathbb{P}^2_k$ is uniquely determined, or $P = Q$, and then by the assumption (b), there is a unique line $L \subset \mathbb{P}^2_k$ such that P is a repeated zero of $F|L$; in either case, $F|L$ is a cubic form in two variables, having 2 given k-valued zeros. It therefore splits as a product of 3 linear factors, and hence without exception, the 3rd residual point of intersection R is defined and has coordinates in k. Note that any of $P = Q$, $P = R$, $Q = R$, or $P = Q = R$ is allowed; these correspond algebraically to $F|L$ having multiple zeros, and geometrically to tangent and inflexion points.

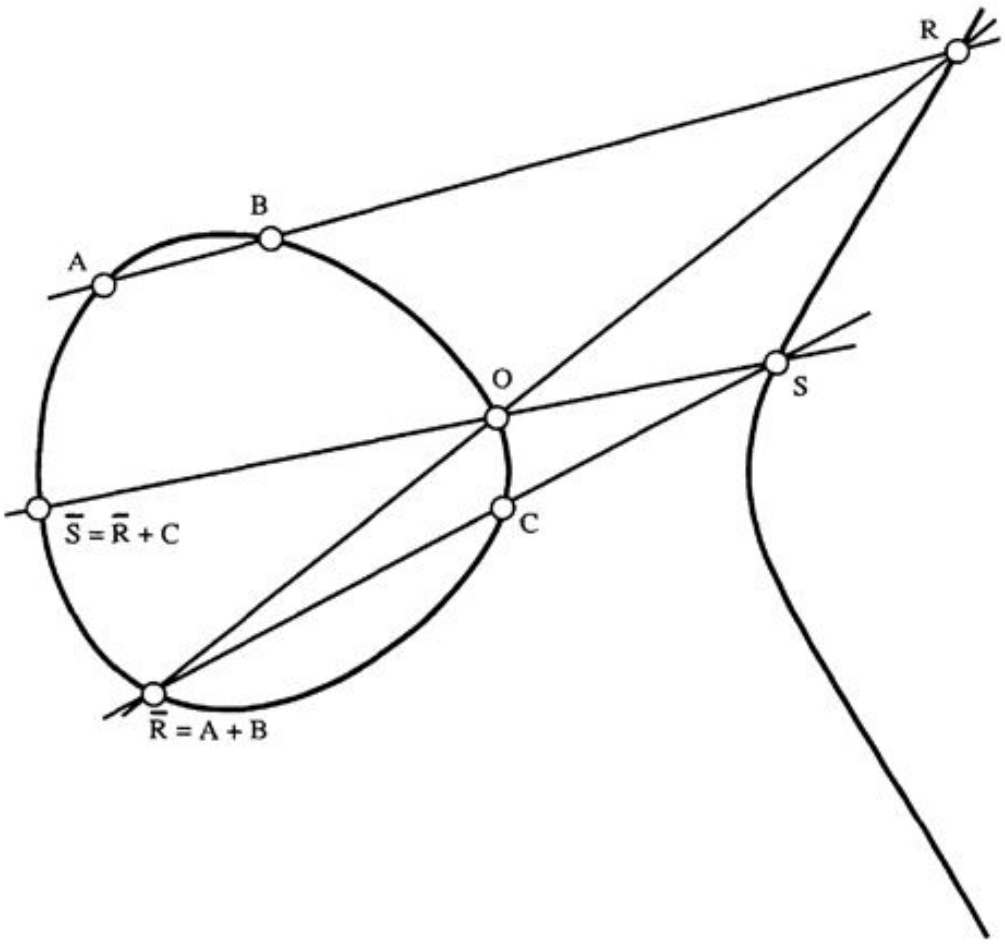

Figure 2.3: Cubic curve and its group law

(II) Verifying that the given point O is the neutral element is completely formal: since $OA\overline{A}$ are collinear, the construction of $O + A$ consists of taking the line $L = OA$ to get the 3rd point of intersection $\overline{A}$, then the same line $L = O\overline{A}$ to get back to A.

(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.