Chapter 3

The Associative Law

We have skated over one issue in defining addition on an elliptic curve, namely the fact that this operation is associative:

$$P + (Q + R) = (P + Q) + R.$$

3.1 The 9th point lemma

Our proof of associativity depends on the following remarkable geometric result, which asserts in effect that any 8 points in general position on the plane determine a 9th point.

Proposition 3.1 *Suppose P_i $(i = 1-8)$ are 8 points over k in the projective plane; and suppose there is a non-singular cubic curve passing through the points. Then there is a further point P_9 over k with the property that every cubic curve through $P_1, \ldots, P_8$ also passes through P_9.*

Proof ► The idea, in brief, is that the cubics through $P_1, \ldots, P_8$ form a pencil

$$\lambda_1 \Gamma_1 + \lambda_2 \Gamma_2;$$

and any two cubics Γ_1, Γ_2 in the pencil meet in 9 points, the given points $P_1, \ldots, P_8$ and one further point P_9.

To expand on this, consider the general cubic

$$\begin{aligned} &aX^3 + bX^2Y + cX^2Z + dXY^2 + eXYZ + fXZ^2 \\ &\quad + gY^3 + hY^2Z + iYZ^2 + jZ^3 = 0. \end{aligned}$$

This has 10 coefficients. Since 2 cubics that are scalar multiples of one another define the same curve, we may say that the cubic curves form a 9-dimensional projective space.

The requirement that the cubic should pass through a point P imposes a linear condition on the coefficients. Thus in our case the coefficients must satisfy 8 linear conditions.

A theorem in linear algebra states that the solutions to m homogeneous linear equations in n unknowns form a vector space of dimension $\geq n - m$. (More precisely, if the $m \times n$ matrix defining the equations has rank r then the solution space has dimension $n - r$.)

In our case, therefore, the space of cubics through the 8 points has dimension ≥ 2. We may say (in homogeneous terms) that the cubics form a *pencil* of dimension ≥ 1.

Lemma 1 *The cubic curves through $P_1, \ldots, P_8$ form a pencil of dimension 1.*

Proof of Lemma $\triangleright$ Suppose the pencil has dimension ≥ 2, ie we can find linearly independent cubics $F_1(X,Y,Z), F_2(X,Y,Z), F_3(X,Y,Z)$ such that the curves

$$\Gamma_{\lambda_1,\lambda_2,\lambda_3} : \lambda_1 F_1(X,Y,Z) + \lambda_2 F_2(X,Y,Z) + \lambda_3 F_3(X,Y,Z) = 0$$

all pass through the 8 points. Then *we can find a cubic in the pencil passing through any further 2 points U, V*; for each additional point will impose a linear condition on $\lambda_1, \lambda_2, \lambda_3$.

Case 1 Suppose first that 3 of the 8 points, say P_1, P_2, P_3 are collinear. Choose U to be the point where the lines

$$\ell = P_1P_2P_3 \text{ and } m = P_4P_5$$

meet, and choose V to be a further point on m. Then each of the lines l, m contains 4 points on the cubic, and so lies wholly in the cubic, which therefore takes the form

$$\Gamma = \ell m n,$$

where n is a third line. Thus the 5 points $P_4, \ldots, P_8$ lie on the two lines m, n.

It follows that there are *two* sets of 3 collinear points among the 8 points, say P_1, P_2, P_3 and P_4, P_5, P_6. Now choose U to be the point where these two lines meet. Then each line contains 4 points on the cubic, and so

$$\Gamma = \ell m n,$$

where $n = P_7P_8$.

It follows that there is just one cubic in the pencil through the additional point U, contrary to our assumption that the pencil has dimensions ≥ 2.

Case 2 Suppose alternatively that no 3 of the 8 points are collinear. In this case choose U, V on the line $\ell = P_1P_2$. Then this line lies wholly in the cubic, ie

$$\Gamma = \ell C,$$

where C is a conic through the 6 points $P_3, \dot{;} P_8$.

Now let us apply much the same ideas — but simpler — to conics.

Sublemma *There exists a unique conic through 5 points $Q_1, \dots, Q_5$, no 3 of which are collinear.*

Proof of Sublemma ▷ The general conic

$$G(X, Y, Z) \equiv aX^2 + bXY + cXZ + dY^2 + eYZ + fZ^2 = 0$$

has 6 coefficients. Consequently (by the same argument as above) we can always find a conic through 5 points.

Suppose there are 2 such conics. Then there is a pencil of conics

$$C_{\lambda_1,\lambda_2} : \lambda_1 G_1(X, Y, Z) + \lambda_2 G_2(X, Y, Z) = 0$$

through the 5 points, and so we can find such a conic through any further point U.

Let us choose U on the line $\ell = Q_1Q_2$. Then the line contains 3 points on the conic, and so lies wholly in the conic:

$$C = \ell m,$$

where the line m must contain Q_3, Q_4, Q_5, contrary to the hypothesis that no 3 of the points were collinear. ◁

We have shown, accordingly, that there is a unique conic C through the 5 points $P_4, \dots, P_8$; and this conic passes through P_3.

But by the same argument, it also passes through P_1 and P_2, ie all 8 points lie on a conic C. But in that case every cubic Γ through the 8 points is degenerate,

$$\Gamma = \ell C$$

for some line ℓ, contrary to the hypothesis that there is a non-singular cubic through the 8 points.

◁

We have shown therefore that the pencil of cubics through the 8 points is 1-dimensional:

$$\lambda_1 F_1(X, Y, Z) + \lambda_2 F_2(X, Y, Z) = 0,$$

where the cubics

$$\Gamma_1 : F_1(X, Y, Z) = 0,\ \Gamma_2 : F_2(X, Y, Z) = 0$$

meet in the 8 points $P_1, \ldots, P_8$.

But now it follows that the two cubics meet in a 9th point defined over k; for when we eliminate say Z we are left with a homogeneous polynomial of degree 9 in X, Y, of which we know 8 roots, and whose 9th root is therefore determined by the fact that — in inhomogeneous language — the sum of the roots of

$$t^n + a_1 t^{n-1} + \cdots + a_n = 0$$

is equal to $-a_1$.) ◀

3.2 An alternative version of associativity

Recall that we defined addition on $\mathcal{E}$ by

$$P + Q = O * (P * Q),$$

where $P * Q$ denotes the poing where the line PQ (or the tangent at P if $P = Q$) meets the curve again, and O is the zero point.

Proposition 3.2 *The operation $P + Q$ is associative if and only if*

$$(P * Q) * (R * S) = (P * R) * (Q * S)$$

for all points $P, Q, R, S \in \mathcal{E}$.

Proof ▶ Suppose first that the associative law holds, so that the operation $P + Q$ defines an additive group on $\mathcal{E}$. In that case

$$P * Q = -(P + Q),$$

and so

$$(P * Q) * (R * S) = P + Q + R + S = (P * R) * (Q * S).$$

Conversely, suppose

$$(P * Q) * (R * S) = (P * R) * (Q * S).$$

We must show that the associative law holds.

We have

$$P + (Q + R) = O * (P * (Q + R)),\ (P + Q) + R = O * ((P + Q) * R).$$

But

$$O * A = O * B \iff A = B,$$

since $O * (O * A) = A$.

Thus we have to show that

$$P * (Q + R) = (P + Q) * R,$$

ie

$$P * (O * (Q * R)) = (O * (P * Q)) * R.$$

But now if we set

$$P' = P * Q,\ R' = Q * R$$

then

$$P = P' * Q,\ R = Q * R',$$

and the equation becomes

$$(P' * Q) * (O * R') = (O * P') * (Q * R'),$$

which is just our condition, with P', Q, O, R' in place of P, Q, R, S. ◂

Note that the associative law in this form does not involve the zero point O, and thus makes sense for any non-singular cubic Γ, taking any point $O \in \Gamma$ as zero point.

(Recall that if $a \in A$, where A is an abelian group, then the binary operation

$$x * y = x + y - a$$

defines a new abelian group structure on A, with a as zero element, since $a * x = a + x - a = x$.)

Note too that it is sufficient to prove the result in any extension field $K \supset k$. In particular we may assume, if necessary, that k is infinite.

3.3 Proof of associativity

Now we use this geometric theorem to establish the above proposition, which we have shown is equivalent to the associative law.

Proof ► Take the 8 points $P, Q, R, S, P*Q, R*S, P*R, Q*S$. These all lie on the elliptic curve $\mathcal{E}$.

Consider the 6 lines ℓ, m, n and L, M, N defined in the following table:

	L	M	N
ℓ	P	Q	$P*Q$
m	R	S	$R*S$
n	$P*R$	$Q*S$	?

Thus ℓ is the line $P, Q, P*Q$.

The singular cubics ℓmn and LMN each contain the 8 points, and so generate the pencil defined by the 8 points. (Thus $\mathcal{E} = \lambda \ell mn + \mu LMN$.)

But now we see that the point $(P*Q)*(R*S)$ lies on the line N, and so on the cubics LMN and $\mathcal{E}$. Hence it is the 9th point of the pencil (that is, the 9th point common to all the cubics in the pencil).

But similarly the point $(P*R)*(Q*S)$ lies on the line n, and so on the cubics lmn and $\mathcal{E}$. Hence this point is also the 9th point of the pencil.

It follows that

$$(P*Q)*(R*S) = (P*S)*(Q*R),$$

as required. ◄

3.4 Two remarks

1. The 'true' explanation of associativity is usually assigned to the Riemann-Roch theorem, which applies to all curves (singular and non-singular). But that is outside the scope of this course.

2. The associative law is immediate for elliptic curves $\mathcal{E}(\mathbb{C})$ defined the Weierstrass elliptic function associated to a lattice, since we showed that $P(z) + P(w) = P(z + w)$.