MMA320 Introduction to Algebraic Geometry

The group law on cubic curves

Let k be a field of characteristic different from 2. Consider an irreducible curve $X \subset \mathbb{P}^2$ given by a cubic equation $F(X,Y,Z) = 0$, which is also irreducible over the algebraic closure of k. Let K be an extension of k, not necessarily closed; an important case is $K = k$. We shall construct a group law on the set of non-singular points $X^{\mathrm{ns}}(K) \subset X(K)$. Therefore we assume that this set is nonempty. We will see later that irreducibility implies that the set of non-singular points is open in $X(\bar{k})$.

We fix a point $e \subset X^{\mathrm{ns}}(K)$, which will be the neutral element. Let x and y be two non-singular points on $X(K)$, with homogeneous ideal I_x and I_y in $K[X,Y,Z]$. If x and y are distinct points the line passing through them is given by the unique (up to scalars) linear form in $I_x \cap I_y$. If $y = x$ we consider the homogeneous ideal $I = (F) + I_x^2$. Its saturation contains again a linear form, which is in fact the tangent line L to X in the point x. In this way two non-singular points determine a line, even if they coincide. We call this the line through x and y.

As X is irreducible, the line L through x and y is not a component, and intersects $X(K)$ in three points: the restriction of F to the line $L \cong \mathbb{P}^1$ is a homogeneous polynomial of degree three in two variables, which is divisible by linear forms defining x and y, so $F|_L$ factorises over k in three linear factors. The point defined by the third linear factor will be called the third intersection point of L and X, and denoted by xy; it may coincide with x or y. It is again a non-singular point.

Definition. The addition $x \oplus y$ on $X^{\mathrm{ns}}(K)$ is determined in the following way: let xy be the third intersection point of the line through x and y with $X(K)$, then $x \oplus y$ is the third intersection point $(xy)e$ on the line through xy and e, cf. Figure 6.1 in [Dolgachev].

Theorem. *This operation makes $(X^{\mathrm{ns}}(K), \oplus)$ into an abelian group with neutral element e.*

Proof. Apart from associativity this is easy.

Commutativity is obvious.

Let us construct $x \oplus e$. Let xe be the third intersection point on the line L through x and e. Then x is the third intersection point on the line through xe and e (which is the line L), so $x \oplus e = x$.

For the inverse, let ee be the third intersection point on the tangent line at X in the point e, then the third point $x(ee)$ on the line through x and ee satisfies $x \oplus x(ee) = e$, so $-x$ is the point $x(ee)$.

For associativity $\big((x \oplus y) \oplus z = x \oplus (y \oplus z)\big)$ it suffices to show that points $(x \oplus y)z$ and $x(y \oplus z)$ in the penultimate step of the construction coincide. There are 8 more points involved, which we write in the following 3×3 square.

$$\begin{array}{ccc} x & y \oplus z & ? \\ xy & e & x \oplus y \\ y & yz & z \end{array}$$

The points in each row and each column are collinear. The question mark stands in the first row for the point $x(y \oplus z)$, while it represents in the last column the point

$(x \oplus y)z$, so the points which we want to prove to be equal. All the eight named points in the square lie not only on $X(K)$, but also on two other cubics, being the product of the lines determined by the rows, respectively the columns, of the square; note that multiple factors may occur.

First consider the case that all eight points are distinct. Then the equality $(x \oplus y)z = x(y \oplus z)$ follows from the following

Claim. *Each cubic (distinct from $X(K)$ itself) through eight points intersects $X(K)$ in one and the same point, besides the eight points; this point may coincide with one of the eight points.*

Usually one concludes the proof by appealing to continuity. But in fact the claim holds in general, if we give the correct meaning to the phrase 'passing through eight points'. We require that the intersection multiplicity at each point is at least the number of times the point occurs in the list of eight points. Apart from the proof of the claim, which will be given later, this finishes the proof. □

We need some preparations. Let V_d be the vector space of all homogeneous polynomials of degree d in X, Y and Z (plus the zero polynomial). It has dimension $\binom{d+2}{2}$; a basis consists of all monomials. For $d = 3$ we get

$$\begin{array}{ccccccc} & & & Z^3 & & & \\ & & XZ^2 & & YZ^2 & & \\ & X^2Z & & XYZ & & Y^2Z & \\ X^3 & & X^2Y & & XY^2 & & Y^3 \end{array}$$

Each non-zero $F = \sum a_{ijk} X^i Y^j Z^k$ defines a curve $X \subset \mathbb{P}^2$, with proportional polynomials defining the same curve.

Definition. The space S_d of all projective plane curves is $\mathbb{P}(V_d)$, a projective space of dimension $\frac{d(d+3)}{2}$. A *linear system* of curves of degree d is a linear subspace of S_d.

Given a point $p \in \mathbb{P}^2$, the condition that the curve $F = 0$ passes through p, is that $F(p) = 0$, and this gives one linear condition on the coefficients of F. The linear systems $S_d(p_1, \ldots, p_k)$ of degree d curves passing through k given points, has dimension at least $\frac{d(d+3)}{2} - k$.

The proof of the claim will follow from the statement that the linear system $S_3(e, x, y, z, xy, yz, x \oplus y, y \oplus z)$ has dimension 1. Then each cubic is of the form $\lambda F + \mu G$, and the intersection of such a cubic with F is given by the ideal (F, G), independent of $(\lambda : \mu)$.

We describe $S_d(p_1, \ldots, p_k)$ in a different way. Let I_i be the radical homogeneous ideal defining the point p_i, and set $I = I_1 \cap \ldots \cap I_k$. Then

$$S_d(p_1, \ldots, p_k) = \{[F] \in S_d \mid F \in I\} = \mathbb{P}(V_d \cap I) \; .$$

The last formula can be generalised by allowing saturated, non-radical ideals.

We consider only so called curvilinear fat points: points lying on a locally smooth curve. In affine coordinates (x, y) with the point at the origin, and tangent of the curve the x-axis, the ideal of a point of multiplicity m looks like $(y + f_2(x, y) + \dots f_d(x, y), y^m, y^{m-1}x, \dots, x^m)$. One can write $y = g(x) \bmod (x^m)$, so other generators for the ideal are $(y - g(x), x^m)$. Let I be the intersection of a finite number of saturated homogeneous ideal, defining points p_i with multiplicity m_i, with total multiplicity $\sum m_i = k$. Then

$$S_d(m_1p_1, \dots, m_jp_j) = \mathbb{P}(V_d \cap I) \ .$$

We need some assumptions which guarantee that the conditions imposed by the points are independent. This is obviously not the case if all points lie on one and the same line.

Definition. We say that n points of the variety defined by I are *collinear*, i.e., lie on a line, if there exists a line L with equation $H = 0$ such that the restriction of I to L defines a collection of points of multiplicity at least n; this means that the ideal $(H) + I$ defines such a collection. We say that n points are conconic, if they lie on a nondegenerate conic $Q = 0$: if $(Q) + I$ defines points with total multiplicity at least n.

Let I define a collection of points (with multiplicities) on an irreducible cubic $F = 0$. Then by Bézout no four points are collinear and no seven points are conconic.

Proposition. *Let I be the ideal of a curvilinear fat point $\sum m_ip_i$ with total multiplicity 8. Assume that no four points are collinear and no seven points conconic. Then the linear system $S_3(m_1p_1, \dots, m_jp_j)$ has dimension 1.*

Proof. As the dimension cannot go down under field extension, we may assume that K is infinite. Suppose for a contradiction that the linear system has dimension at least two.

We first assume that no three points are collinear and no six conconic. (This holds if the points are in general position.) Let $L\colon H = 0$ be a line through two points (either through two distinct points, or tangent to a multiple point). We choose two points p_9, p_{10} on L outside the eight given points; this is possible as K is infinite. Then there is a cubic $G \in S_3(m_1p_1, \dots, m_jp_j, p_9, p_{10})$. As L intersects it with multiplicity at least four, the line is a component, so we can write $G = HQ$. The remaining six of the original eight points have to lie on $Q = 0$. In the case of multiple points this means: the remaining points are given by the ideal $I' = I : H$, which by definition is $I : H = \{G \in K[x, y] \mid GH \in I\}$. In local coordinates as above, if L is tangent, then we have the ideal $(y - ax^2 + \dots, x^m)$ with $a \neq 0$, and $H = y$; then $x^{m-2} \in I : H$. So indeed the ideal I' defines points of total multiplicity 6. According to our assumption Q has to be a degenerate conic, either two lines, or a double line. But then there must be a line containing at least three points.

Now suppose that three points are collinear, lying on a line $L\colon H = 0$. Choose a point $P_9 \in L$. The linear system $S_3(m_1p_1, \dots, m_jp_j, p_9)$ has dimension at least one. Every element is reducible, of the form HQ. The Q form a linear system of conics throug five points, of dimension at least one. Two elements have therefore a line in common, which cannot contain four points, so we end up with a linear system of lines though at least two points, of dimension at least one, which is impossible.

The last possibility is that six points are conconic, on the conic $Q = 0$. We choose p_9 on the conic. Then every element of the linear system $S_3(m_1p_1, \dots, m_jp_j, p_9)$ is reducible, of the form QH, and the H form a linear system of through at two points, given by $I : Q$, of dimension at least one, which we already concluded to be impossible. □

The group law can be simplified by taking an inflection point, if the cubic has one, as neutral element. Then the third point, in which the tangent at e intersects the curve, is e itself. So the inverse $-x$ is the third point on the line ex. Therefore we obtain

$$x + y + z = 0 \quad \Leftrightarrow \quad x,\ y \text{ and } z \text{ collinear} .$$

We can take coordinates with the flex being the line at infinity and the inflection point $(0 : 1 : 0)$. By completing the square ($\operatorname{char} K \neq 2$) we get an equation of the form $y^2 = x^3 + px^2 + qx + r$, which if $\operatorname{char} K \neq 3$ can be simplified further to

$$y^2 = x^3 + ax + b .$$

If $z = (x, y)$, then $-z = (x, -y)$.

Over the compex numbers a non-singular cubic curve is a Riemann surface of genus 1, so topologically a torus. Let τ be a point in the upper half plane. Then the Riemann surface is $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)$. The group structure comes from addition on $\mathbb{C}$. Meromorphic functions on the Riemann surface are doubly periodic functions in the complex plane. In particular, one has the Weierstraß $\wp$ function given by

$$\wp(z) = \frac{1}{z^2} + \sum_{(m,n)\neq(0,0)} \left(\frac{1}{(z - m - n\tau)^2} - \frac{1}{(m + n\tau)^2} \right) .$$

It satisfies the equation

$$\left(\wp'(z)\right)^2 = 4\left(\wp(z)\right)^3 - g_2\wp(z) - g_3 .$$