1.16 07/15/24 - Max Noether's Theorem, Proof of Chasles's Theorem, Weierstrass Normal Form

The first order of business today is to prove Chasles's Theorem, for which we will need

Theorem 1.16.1 (Max Noether). Let $F, G, H \in k[X, Y, Z]$ be relatively prime homogeneous polynomials of degrees $m, n, d \geq 1$ such that F and G are relatively prime. Then H can be written as

$$H = AF + BG$$

for some homogeneous $A, B \in k[X, Y, Z]$ of degrees $d - m, d - n$ iff for each point $P \in \mathbb{P}^2_k$, we have

$$(H)\mathcal{O}_{\mathbb{P}^2_k, P} \subset (F, G)\mathcal{O}_{\mathbb{P}^2_k, P}.$$

This theorem, often called Max Noether's $AF + BG$ Theorem, or Max Noether's Fundamental Theorem, is again an upgraded version of the local-to-global principal Lemma 1.14.2, and says that H is globally a polynomial-linear combination of F, G iff it is locally a polynomial-linear combination of F and G at each point P.

Proof. One direction is clear. For the other, assume that $(H)\mathcal{O}_{\mathbb{P}^2_k, P} \subset (F, G)\mathcal{O}_{\mathbb{P}^2_k, P}$ for all $P \in \mathbb{P}^2_k$, and suppose by a projective change of coordinates that all points of $C_F \cap C_G$ are in the finite plane, i.e. not on L_∞. If $f, g, h \in k[x, y]$ are the dehomogenizations of F, G, H respectively, then it follows that $h \in (f, g)\mathcal{O}_P$ for all $P \in C_f \cap C_g$, so from Lemma 1.14.2 it follows that $h \in (f, g)k[x, y]$, i.e. $h = af + bg$ for some $a, b \in k[x, y]$. Homogenization then yields

$$Z^r H = AF + BG$$

for some $r \geq 0$ and $A, B \in k[X, Y, Z]$ homogeneous of degrees $d+r-m$ and $d+r-n$ respectively. The result then follows by induction from the following lemma. ∎

Lemma 1.16.2. Let $F, G \in k[X, Y, Z]$ be relatively prime homogeneous polynomials of degrees $m, n \geq 1$ such that $C_F \cap C_G \cap L_\infty = \emptyset$. If $H \in k[X, Y, Z]$ is a homogeneous polynomial of degree $d \geq 1$ such that

$$ZH = AF + BG$$

for some homogeneous $A, B \in k[X, Y, Z]$ of degrees $d + 1 - m, d + 1 - n$ respectively, then there are $A', B' \in k[X, Y, Z]$, homogeneous of degrees $d - m, d - n$ respectively such that

$$H = A'F + B'G.$$

In other words, if C_F and C_G do not intersect on the line at infinity, then multiplication by Z is injective on the quotient ring $k[X, Y, Z]/(F, G)$.

Proof. For $P \in k[X, Y, Z]$, let P° denote the specialization $P^\circ := P(X, Y, 0) \in k[X, Y, Z]$; then $Z \mid P$ iff $P^\circ = 0$. Specializing the equation $ZH = AF + BG$ yields

$$A^\circ F^\circ + B^\circ G^\circ = 0.$$

Since $C_F \cap C_G \cap L_\infty = \emptyset$, the polynomials $F^\circ, G^\circ \in k[X, Y]$ are relatively prime, and hence there is a $C \in k[X, Y]$ such that $A^\circ = CG^\circ$ and $B^\circ = -CF^\circ$. In this case, the polynomial

$A - CG$ has the property that $(A - CG)^\circ = A^\circ - CG^\circ = 0$, whence there is an $A' \in k[X, Y, Z]$ such that $A - CG = A'Z$. Similarly, there is a $B' \in k[X, Y, Z]$ such that $B + CF = B'Z$. These A' and B' work. ■

We are now ready to prove Chasles's Theorem. For simplicity, I will do the case when the nine points of intersection are distinct, leaving the general case (with multiplicities) to the dedicated reader. This is not too unfair, since we have developed all the necessary tools for this extension already. The advantage of working with distinct points is that it makes Theorem 1.16.1 very easy to apply.

Lemma 1.16.3. Let $D, E \subset \mathbb{P}^2_k$ be projective curves of degrees $m, n \geq 1$ which intersect in exactly mn distinct points, and let $Y \subset \mathbb{P}^2_k$ be a curve that passes through all mn of these points. If $F, G, H \in k[X, Y, Z]$ are minimal polynomials for D, E, Y respectively, then there are homogeneous polynomials $A, B \in k[X, Y, Z]$ of degrees $\deg(H) - \deg(F), \deg(H) - \deg(G)$ respectively such that $H = AF + BG$.

Proof. By Theorem 1.16.1, it suffices to show that $(H)\mathcal{O}_{\mathbb{P}^2_k, P} \subset (F, G)\mathcal{O}_{\mathbb{P}^2_k, P}$ for all $P \in \mathbb{P}^2_k$. When $P \notin D \cap E$, this is clear, since the right hand side is all of $\mathcal{O}_{\mathbb{P}^2_k, P}$. Now suppose that $P \in D \cap E$. Our hypothesis coupled with Bézout's Theorem implies that $i_P(D, E) = 1$, and we have to show that this combined with $P \in Y$ implies the result. This is clearly a local computation, so we can pass to the affine case; let f, g, h denote the respective dehomogenizations. Then $\mathrm{eval}_P : \mathcal{O}_{\mathbb{A}^2_k, P} \to k$ is surjective with kernel containing (f, g) such that the quotient $\mathcal{O}_{\mathbb{A}^2_k, P}/(f, g)$ has dimension one; this gives us an isomorphism $\mathrm{eval}_P : \mathcal{O}_{\mathbb{A}^2_k, P}/(f, g) \to k$. In particular, $Y \ni P$ iff h lies in the kernel of this evaluation map iff $h \in (f, g)\mathcal{O}_{\mathbb{A}^2_k, P}$. ■

The only difference in the general case is that one needs to check the "Noether condition" $(H)\mathcal{O}_{\mathbb{P}^2_k, P} \subset (F, G)\mathcal{O}_{\mathbb{P}^2_k, P}$ by hand for each $P \in D \cap E$, so to speak. See [3, §5.5]. We are now ready to prove

Theorem 1.15.14 (Chasles). Let $D, E \subset \mathbb{P}^2_k$ be two cubic curves that intersect in 9 points, and suppose one of D or E is irreducible. If $X \subset \mathbb{P}^2_k$ is another cubic curve that passes through 8 of 9 of these points, then X also passes through the 9th one.

Proof. Suppose that D is irreducible, and write $D \cap E = \{P_1, \ldots, P_9\}$, with $P_i \in X$ for $i = 1, \ldots, 8$. Let the ninth point of intersection of X with D be Q, and suppose for the sake of contradiction that $Q \neq P_9$. Pick a general line L through P_9; it suffices to take one not passing through Q and meeting D in two distinct other points R, S. Then $E \not\ni R, S$. Applying Lemma 1.16.3 to $Y := X \cup L$, we conclude that if F, G, H are the homogeneous cubic polynomials defining D, E, X respectively, then there are homogeneous linear polynomials $A, B \in k[X, Y, Z]$ such that

$$LH = AF + BG.$$

(Here we are using L also to denote the linear polynomial defining the line L; we will also do this for A and B.) Now $R, S \notin E$ implies that the line G contains R and S, and hence must be identical with L. It follows that $L \mid AF$, but since F is assumed to be irreducible, this can only happen if $L = A$ (upto scaling). Cancelling the factor of L tells us that $H = \alpha F + \beta G$ for some scalars $\alpha, \beta \in k$, i.e. that X is in the pencil spanned by D and E. In particular, $X \ni P_9$, which is a contradiction. This shows that our assumption $Q \neq P_9$ is false, proving $X \ni P_9$ as needed. ■

With this we have now completed the proof of the associativity of the elliptic curve addition law–at least as long as all the points involved are distinct; see Remark 1.15.16. Let us now move on to some explicit examples illustrating how to work with elliptic curves.

1.16.1 Weierstrass Normal Form and Legendre Form, Two and Three Torsion

Recall our convention that k is an algebraically closed field of characteristic other than 2 or 3. In these circumstances, we given a smooth cubic $E \subset \mathbb{P}^2_k$, we can make a convenient choice of basepoint $O \in E$ and coordinates that makes the study of the elliptic curve (E, O) particularly convenient.

Firstly, the choice of basepoint O doesn't really matter all that much (see Exercise 2.6.9), but a convenient choice of O can make the addition law particularly easy. Namely, by Exercise 2.5.5, E has exactly 9 inflection points, and we pick O to be one of these flexes. The upshot of this is that in the addition law on E, we have $O' = O$ by definition (see the proof of Theorem 1.15.13), and hence the $-A, O$ and A are collinear for each $A \in E$; in fact, it is easy to see in this case (check!) that three points $A, B, C \in E$ (counted with multiplicity) are collinear iff $A + B + C = 0$ in the group law.

As a first consequence, not that this means that given a fixed $P \in E$, the point P is an inflection point on E iff the "points" P, P, P are collinear iff $3P = 0$ iff $P \in E[3]$ is a 3-torsion point. In particular, Exercise 2.5.5 gives us that $E[3]$ is an abelian group with 9 elements, each of order 3, and hence that $E[3] \cong \mathbb{Z}/3 \times \mathbb{Z}/3$. This is the first observation in a very large story, another part of which we shall see below and which you will be asked flesh out in detail in Exercise 2.6.10.

Given an elliptic curve (E, O) with $O \in E$ an inflection point, we can now bring E into what is called the (reduced) Weierstrass normal form. Here's how this goes: pick a coordinate system in which $O = [0 : 1 : 0]$ with the tangent line $\mathrm{T}_O E$ being the line at infinity $Z = 0$. Let F be the minimal polynomial of E, and write F as

$$F = A_0 Y^3 + A_1 Y^2 + A_2 Y + A_3$$

for $A_i \in k[X, Z]_i$ homogeneous of degree i for $i = 0, \ldots, 3$. The condition $O \in E$ implies $A_0 = 0$, the condition $\mathrm{T}_O E = \mathbb{V}(Z)$ implies that $A_1 = Z$ (possibly after scaling, which we do), and the condition that $O \in E$ is an inflection point says that $Z \mid A_2$. Therefore, the polynomial F looks like

$$Y^2 Z + (\lambda X + \mu Z) Y Z + A_3.$$

Since $\operatorname{ch} k \neq 2$, we can replace Y by $Y - (\lambda X + \mu Z)/2$ to eliminate the middle term, so that the equation looks like

$$Y^2 Z = \alpha_0 X^3 + \alpha_1 X^2 Z + \alpha_2 X Z^2 + \alpha_3 Z^3$$

for some $\alpha_i \in k$ for $i = 0, \ldots, 3$. Since E is irreducible, we must have $\alpha_0 \neq 0$; replacing Z by $\alpha_0 Z$, we may assume that $\alpha_0 = 1$ to get an equation of the form

$$Y^2 Z = X^3 + \beta_1 X^2 Z + \beta_2 X Z^2 + \beta_3 Z^3.$$

Finally, using $\operatorname{ch} k \neq 3$, we may replace X by $X - \frac{1}{3}\beta_1 Z$ to depress this last cubic to obtain the reduced Weierstrass normal form

$$Y^2 Z = X^3 + p X Z^2 + q Z^3$$

for some $p, q \in k$, or in affine coordinates

$$y^2 = x^3 + px + q.$$

By (a salvage of) Exercise 2.3.10 combined with Exercise 2.2.5(b), this curve is smooth iff

$$4p^3 + 27q^2 \neq 0.$$

One thing this form enables us to see immediately is the two-torsion $E[2]$ on E. Firstly, the only point on E at infinity (i.e. on $Z = 0$) is the point O. Next, given a(n) (affine) point $P = (x, y)$ on E, when E is in Weierstrass form, since P, O and $-P$ are collinear, we see that $-P = (x, -y)$. In particular, $2P = 0$ iff $P = -P$ iff $P = O$ or $P = (x, y)$ with $y = 0$. In other words, the two-torsion points other than O correspond directly to the roots of $x^3 + px + q$; if these roots are $e_1, e_2, e_3 \in k$ (using here that $k = \overline{k}$), then

$$E[2] = \{O, (e_1, 0), (e_2, 0), (e_3, 0)\}.$$

Note that the discriminant condition $4p^3 + 27q^2 \neq 0$ (or equivalently the nonsingularity of E) implies the roots e_1, e_2, e_3 are pairwise distinct, whence $E[2]$ is an abelian group of size 4; since every nontrivial element of $E[2]$ has order 2, we see immediately that

$$E[2] \cong \mathbb{Z}/2 \times \mathbb{Z}/2.$$

The two examples here suggest the following generalization: is it always true that for any $n \geq 1$ we have

$$E[n] \cong \mathbb{Z}/n \times \mathbb{Z}/n,$$

as we have shown for $n = 1, 2, 3$? In fact, this is always true in characteristic zero, or more generally if $\operatorname{ch} k \nmid 2n$; for a proof, see Exercise 2.6.10. The best way I know of understanding this result, however, involves seeing connections to a different branch of math, namely complex analysis; I'll cover this in the story time during the next lecture–see §1.17.2.

The above version of the Weierstrass normal form is convenient, but it doesn't make it clear how the isomorphism class of E depends on (p, q). For starters, replacing Z by uZ tells us that the curves given by (p, q) and (u^2p, u^3q) are the same for any $u \in k^\times$. It turns out, but is more difficult to prove, that two elliptic curves are in short Weierstrass form are isomorphic iff there is such a transformation between them. We'll pursue a slightly different line of study, via a slightly different variant of the Weierstrass form.

Namely, recall as above that we by a chance of coordinates assume that the curve is given as

$$Y^2Z = X^3 + \beta_1 X^2 Z + \beta_2 XZ^2 + \beta_3 Z^3.$$

This time, we'll factor the right hand side as

$$(X - e_1 Z)(X - e_2 Z)(X - e_3 Z)$$

for some distinct $e_i \in k$. Next, replacing X by $X - e_1 Z$, we will assume that $e_1 = 0$; then $e_2 e_3 \neq 0$. Finally, by replacing Z by $e_2^{-1} Z$ and Y by $e_2^{1/2} Y$ (again using $k = \overline{k}$), we arrive at the Legendre form

$$Y^2Z = X(X - Z)(X - \lambda Z)$$

for some $\lambda \in k \smallsetminus \{0, 1\}$. Written in affine coordinates, this is

$$y^2 = x(x - 1)(x - \lambda).$$

Let us denote this curve by E_λ. One can then ask: when are E_λ and E_μ for $\lambda, \mu \in k \smallsetminus \{0, 1\}$ related by a projective change of coordinates? Giving a complete answer to this question will allow us to give a classification of elliptic curves. This is what we will pursue next time.