1.7 26/06/24 - Review of Projective Geometry V: Proof of Bézout's Theorem For Intersection with a Line; The Geometry of Cubic Curves I: The Group Law

Today, we'll wrap up our discussion of projective geometry, and start talking about the geometry of cubic curves in particular.

1.7.A Proof of Bézout's Theorem for Intersection with a Line

As promised, let us now prove Bézout's Theorem for intersection with a line.

Theorem 1.7.1 (Special Case of 1.6.9)**.** Let K be a field, $C \subset \mathbb{P}^2_K$, and $L \subset \mathbb{P}^2_K$ be a line such that C and L don't have a common component, i.e., that $L \not\subset C$. If Ω is an algebraically closed field containing K, then C and L intersect in exactly $\deg C$ points over Ω when counted with multiplicities.

The definitions of the intersection multiplicities will turn up naturally in the proof, which you will see is very easy and natural.

Proof. Without loss of generality, we may assume that L is the X-axis $L = \mathbb{V}(Y)$. In this case, intersecting with L amounts to setting $Y = 0$ in a defining equation for C. Let $F \in K[X, Y, Z]$ be a definiting equation for C; the intersection points then correspond to homogeneous solutions $[X : 0 : Z]$ to $F(X, 0, Z) = 0$.

Since $L \not\subset C$, the polynomial $F(X, 0, Z) \in K[X, Z]$ is not identically zero. Therefore, it is a homogeneous polynomial of degree $d := \deg F = \deg C \in \mathbb{Z}_{\geq 1}$. Since Ω is algebraically closed, $F(X, 0, Z)$ splits completely into linear factors in $\Omega[X, Z]$ as

$$F(X, 0, Z) = \prod_{i=1}^{k} (\mu_i X - \lambda_i Z)^{m_i}$$

corresponding to the say $k \in \mathbb{Z}_{\geq 1}$ points of intersection $P_i = [\lambda_i : 0 : \mu_i] \in C(\Omega)$, where P_i has multiplicity $m_{P_i}(C, L) := m_i \in \mathbb{Z}_{\geq 1}$. Therefore, the number of intersection points over Ω counted with multiplicity is precisely

$$\sum_{i=1}^{k} m_i = d.$$

■

Example 1.7.2. If $K = \mathbb{Q}$ and $F(X, 0, Z) = X^6Z - 2X^5Z^2 - X^4Z^3 + 4X^3Z^4 - 2X^2Z^5$, then this factors as $F(X, 0, Z) = X^2Z(X - Z)^2(X - \sqrt{2}Z)(X + \sqrt{2}Z)$ over an algebraically closed field, say $\Omega = \mathbb{C}$, and the corresponding points $[0 : 0 : 1], [1 : 0 : 0], [1 : 0 : 1], [\sqrt{2} : 0 : 1], [-\sqrt{2} : 0 : 1]$ have multiplicities $2, 1, 2, 1, 1$ respectively, adding up to $7 = \deg F(X, 0, Z)$.

That was straightforward! Actually, the above proof shows something a little stronger:

Corollary 1.7.3 (of the Proof of 1.7.1)**.** In the set-up of 1.7.1, suppose that $\deg C - 1$ of the points in $C \cap L$ have coordinates in K. Then so does the last one.

Proof. This is just the projective version of the fact that a polynomial $h(x) \in K[x]$ of degree d that has $d - 1$ roots in K (counted with multiplicity) must have its last root in K as well. ■

One last thing I want to point out about the above discussion is that the nonvanishing of $F(X, 0, Z)$ is equivalent to the statement that the monomial Y does not divide F. This would be automatic if F is *irreducible* as a polynomial, of degree $\deg F \geq 2$. A plane curve with irreducible defining polynomial is said to be an *integral* curve. (This applies to both affine and projective plane curves.)

Example 1.7.4. For any field K, the curves $\mathbb{V}(X^2 - Y^2) \subset \mathbb{P}^2_K$ and $\mathbb{V}(X^2) \subset \mathbb{P}^2_K$ are not integral.

Remark 1.7.5. This notion of irreducibility of polynomials (and hence integrality of curves) depends crucially on the base field. For instance, the polynomial $X^2 + Y^2$ is irreducible in $\mathbb{R}[X, Y, Z]$ (check!), but the same polynomial is not irreducible in $\mathbb{C}[X, Y, Z]$, since it factors as $(X + iY)(X - iY)$. A polynomial $F \in K[X, Y, Z]$ is said to be *geometrically irreducible* if it remains irreducible even after replacing K by any field extension L/K. (Again, by arguments similar to those in 1.5.5, it suffices to check one algebraically closed field $L = \Omega$ containing K.) Therefore, the polynomial $X^2+Y^2 \in \mathbb{R}[X, Y, Z]$ is irreducible but not geometrically irreducible. A curve cut out by a geometrically irreducible defining polynomial is said to be *geometrically integral*. Therefore, the curve $C = \mathbb{V}(X^2 + Y^2) \subset \mathbb{P}^2_{\mathbb{R}}$ is integral but not geometrically integral.

As a fun exercise, you could try

Exercise 1.7.6. Show that the "circle" $\mathbb{V}(X^2 + Y^2 - Z^2) \subset \mathbb{P}^2_{\mathbb{R}}$ is geometrically integral.

We will show later that for any field K, the curve $\mathbb{V}(Y^2Z - X^3 - Z^3) \subset \mathbb{P}^2_K$ is geometrically integral. Let's now actually begin talking about the main subject matter for the summer: cubic curves.

1.7.B The Group Law on Points of a Cubic Curve

Let's start by talking about cubic curves. We'll focus on the smooth case for now, and leave the singular case for later.

So suppose that K is field, $C \subset \mathbb{P}^2_K$ is a smooth cubic curve. Suppose that we are given two points $P, Q \in C(K)$. We can then draw the line $L = L_{PQ}$ through them. By 1.6.9, this will intersect C in a third point, say R. (This R could be P, e.g., if L_{PQ} is tangent to C at P. It could be both P and Q if $P = Q$ is a flex!) In fact, since P and Q have coordinates in K, 1.7.3 tells us that $R \in C(K)$ as well. This gives us a way of producing a new K-point from two K-points on C. Following [1], let us temporarily denote the R obtained by such a procedure from P and Q by $P * Q$. What should we do when $P = Q$? Of course, we should take L to be the tangent line $L = \mathbb{T}_P C$, and take $R = P * P$ to be the third point of intersection.

What properties does this $*$ operation have? We would like it to be a group law, but a little experimentation shows that this doesn't work. For instance, could it have an identity element? Suppose it did, and call it $\mathscr{O} \in C(K)$. Then for $\mathscr{O} = \mathscr{O} * \mathscr{O}$ to be true, we would need $\mathscr{O}$ to be a flex point. (That's not horrible yet.) But now for every $P \in C(K)$, we must have $P = \mathscr{O} * P$, which is to say that the line joining $\mathscr{O}$ and P is tangent to C at P. This would mean that *every line through* $\mathscr{O}$ is tangent to C. It is geometrically very believable that it would be very hard to find such a point! We can show with a little effort that such a point does not exist for any smooth cubic curve C over any field K, but let's not bother with this.[3] We have concluded that we need to modify this procedure slightly. Perhaps it is believable from the above discussion, that the procedure is missing a "reflection in $\mathscr{O}$" step. Therefore, let us consider a slightly different operation given as follows.

Fix a smooth cubic $C \subset \mathbb{P}^2_K$ and a point $\mathscr{O} \in C(K)$. (The point $\mathscr{O}$ doesn't have to be a flex point to begin with, but we'll see that taking it to be a flex point does simplify some operations below. We will also see that the choice of $\mathscr{O}$ doesn't matter–at least when considering only the abstract isomorphism type of the group. See below.) Given two points $P, Q \in C(K)$, we can take the line $L = L_{PQ}$ joining them, and then take the third point of intersection $R \in C(K)$ of L with C (where again R is a K-point thanks to 1.7.3). Next, take the line $L_{R\mathscr{O}}$ joining R and $\mathscr{O}$, and take *its* third intersection point with C. Call this intersection point $P \oplus Q$. As above, if $P = Q$, then we start by taking $L = \mathbb{T}_P C$ instead, with the rest being the same. Symbolically, we have in all cases that $P \oplus Q := \mathscr{O} * (P * Q)$.

The fundamental result in the theory is then

[3] Here's a quick proof for the cognoscenti: If such a point exists, then $\pi_P : C \to \mathbb{P}^1_K$ is a purely inseparable morphism of degree 2. This forces $\operatorname{ch} K = 2$ and $g(C) = g(\mathbb{P}^1_K) = 0$ ([6, Proposition IV.2.5]), but this is not possible because $g(C) = 1$. Such "strange" points which lie on every tangent to a given curve can only exist for (lines in any characteristic and) conics in characteristic two; see [6, Theorem IV.3.9].

Theorem 1.7.7 (Fundamental Theorem of Elliptic Curve Theory)**.** For any field K, smooth cubic $C \subset \mathbb{P}^2_K$, and $\mathscr{O} \in C(K)$. The operation $P, Q \mapsto P \oplus Q$ described above makes $C(K)$ an abelian group with identity element $\mathscr{O}$. Further, for any field extension L/K, the natural inclusion $C(K) \subset C(L)$ makes $C(K)$ a subgroup of $C(L)$.

Before, we prove this, let's remark that this is really cool. We started with the set of points on a curve, and gave it an algebraic structure similar to that found on $\mathbb{Z}$ or $\mathbb{Z}/3$. Finally, we can use this additional structure to say something about the set of points on this curve. It is probably an understatement to say that this fundamental theorem is precisely the result that makes the theory of elliptic curves so rich and vast. No such phenomenon exists for (smooth plane) curves of higher degree than 3.

Unimportant Remark 1.7.8. In fact, much more is true than 1.7.7. The group operations on C really come from *algebraic operations*, and this makes C into a *group variety* (or even *abelian variety*). We're not going to use this result (or even this terminology). If you're really interested, you can find a proof of this fact in various places such as [6, IV.4.8], [7, Theorem 3.6], or [8, 19.10.3-4].

Let's try to prove 1.7.7

Proof Sketch of 1.7.7 . Let's go through the abelian group axioms one at a time. Commutativity is clear, as is the fact that $\mathscr{O}$ is the identity. To create inverses, one could try $\ominus P := \mathscr{O} * P$, but it is easy to see this doesn't work in general. In fact, a little experimentation shows that the right thing to do is to let $\mathscr{O}' := \mathscr{O} * \mathscr{O}$, and then define $\ominus P := \mathscr{O}' * P$. (This is where we see it would be nice to take $\mathscr{O}$ to be an inflection point, because then $\mathscr{O}' = \mathscr{O}$, and the negation is simply $\ominus P = \mathscr{O} * P$. However, you should remember that this really needs $\mathscr{O}$ to be an inflection point.)

The only thing that remains to be checked is associativity. This is the hardest. Let's see what that involves. A simple geometric argument tells us that associativity is the same as the statement that if $P, Q, R \in C(K)$, then $(P \oplus Q) * R = P * (Q \oplus R)$ (draw a picture!). This step genuinely requires argument. There are three proofs of this result I know, each somewhat nontrivial. One pedestrian approach is to write everything out in coordinates and check that the algebra works. However, this is a very daunting task. The classical geometers had a better proof of this result using something known as Chasles's Theorem. This really amounts to either using some dimensional estimates on the set of cubic curves or some local properties of plane curve intersections (an exposition of this proof I gave two years ago at Ross can be found at [4, 1.15.13-14]; you can also read about in [9, §7]). Finally, the third and modern approach uses divisors on curves and the Riemann-Roch Theorem; such a proof can be found in modern books such as [7, III.3.4(e)] or [8, 19.9.3, 19.9.10]. ■

By popular demand, I will give a brief outline of the third proof (using the Riemann-Roch Theorem) next time.