1.15 07/12/24 - More Applications, Pencils of Curves, Introduction to Elliptic Curves

Today, we'll do more applications of Bézout's Theorem and start talking about elliptic curves, which will be our main focus for the last few lectures. Before we do that though, it is helpful to have a few handy corollaries and ideas. Here are two immediate applications of Bézout's Theorem.

Theorem 1.15.1. Let k be an algebraically closed field.

(a) If $C, D \subset \mathbb{P}^2_k$ are any two projective curves, then $C \cap D \neq \emptyset$.
(b) Any smooth projective curve is irreducible.

Proof. The statement (a) is an immediate corollary of Bézout's Theorem (Theorem 1.14.1). For (b), if a projective curve has multiple components, then some two of these components must intersect somewhere by (a), and then by Theorem 1.9.6, this point of intersection is a singular point of the curve. ■

Note that (a) is sharp in the sense that it is possible for two curves of any degrees $m, n \geq 1$ to intersect in a single point with multiplicity mn. We shall have occasion to use (b) repeatedly below.

1.15.1 Pencils of Curves and the Quartic Equation

Let's now talk about linear one parameter families of curves, starting with a couple of examples.

Example 1.15.2. The family $\mathcal{C} = \{C_\lambda\}_{\lambda \in k}$ of curves, where C_λ is the horizontal line defined by $y - \lambda = 0$ is a one-parameter family of curves of degree 1. When $\lambda \to \infty$, curve C_λ seems to disappear; one way to rectify this is to write this family projectively as given by the vanishing locus of $\mu Y - \lambda Z = 0$ for $\Lambda = [\lambda : \mu] \in \mathbb{P}^1_k$, so when λ is "infinity", i.e. $\Lambda = [1 : 0]$, then the corresponding line is simply $Z = 0$, the line at infinity–we could have predicted that. Note that in this case, each member of the family has degree exactly 1.

Example 1.15.3. Now consider the family $\mathcal{C} = \{C_\Lambda\}_{\Lambda \in \mathbb{P}^1_k}$ of curves, where C_Λ for $\Lambda = [\lambda : \mu]$ is the vanishing locus of $\lambda YZ - \mu X^2 = 0$. This is a one-parameter family of conics (specifically parabolae), and the member C_Λ is singular iff $\Lambda = [1 : 0]$ or $\Lambda = [0 : 1]$; in the former case, it is the union of the x-axis and L_∞, and in the latter case, it is the ("doubled") y-axis. Note that $\deg C_\Lambda = 2$ for all Λ except $[0 : 1]$, where $\deg C_{[0:1]} = 1$.

These examples motivate the following definition.

Definition 1.15.4.

(a) A pencil $\mathcal{C}$ of projective plane curves of degree d is a one-parameter linear family $\mathcal{C} = \{C_\Lambda\}_{\Lambda \in \mathbb{P}^1_k}$ of projective curves, all but finitely many members of which have degree d.
(b) Given a pencil $\mathcal{C}$ of curves, we define the base locus of $\mathcal{C}$ to be

$$\mathrm{BL}(\mathcal{C}) := \bigcap_{C \in \mathcal{C}} C$$

the intersection of all the curves in the pencil.

Concretely, a pencil $\mathcal{C}$ of degree d is given by specifying two linearly independent $F, G \in k[X, Y, Z]_d$ and then defining

$$C_\Lambda := C_{\lambda F + \mu G}$$

for $\Lambda = [\lambda : \mu] \in \mathbb{P}^1_k$. In this case, we have

$$\mathrm{BL}(\mathcal{C}) = C_F \cap C_G.$$

Of course, the choices for F and G are not unique: any two F', G' that form a basis for the span $k\langle F, G\rangle$ of F and G can be chosen as our F and G spanning the pencil, at the cost of changing the parameter Λ representing each curve C_Λ (by a projective change of coordinates in $\mathbb{P}^1_k$.) Saying that all but finitely many members of $\mathcal{C}$ have degree d is equivalent to saying that there is no homogeneous polynomial $H \in k[X, Y, Z]$ such that $H^2 \mid F, G$ (check!); this is a condition we will assume from henceforth as well.

Remark 1.15.5. With our description of the parameter space $\mathbb{P}^{d(d+3)/2}_k$ for all curves of degree $d \geq 1$, a pencil corresponds exactly to a line $\mathbb{P}^1_k \cong L \subset \mathbb{P}^{d(d+3)/2}_k$. Similarly, a two-parameter family (given by a plane $\mathbb{P}^2_k \cong \Lambda \subset \mathbb{P}^{d(d+3)/2}$) is called a net and a three-parameter family is called a web (which are some rather pictorial names); in general, a k-dimensional linear family of curves of degree d is also called a k-dimensional linear system of degree d curves. Note also that we cannot, in general, expect all curves in our pencil to have degree exactly d, as Example 1.15.3 illustrates that we cannot ask all members of our pencil to have the same degree; this can be done (e.g. if we consider the "double" y-axis to have degree 2), but needs the language of schemes. As we shall see below, the notion of base locus also behaves most nicely when we are in the world of schemes, so we can keep track of tangency of the members of our pencil as well.

Example 1.15.6. A pencil of lines is just the family of all lines in $\mathbb{P}^2_k$ passing through some fixed point $P \in \mathbb{P}^2_k$; in particular, there is only one kind of pencil of lines up to projective changes of coordinates, and the family of all pencils of lines in $\mathbb{P}^2_k$ is exactly $\mathbb{P}^2_k$.

Example 1.15.7. Over an algebraically closed field of characteristic other than 2, there are exactly 8 types of pencils of conics up to projective changes of coordinates. Ifa pencil $\mathcal{C}$ contains at least one smooth member, then the base locus of $\mathcal{C}$ consists of at most 4 distinct points, and the intersection multiplicities of at the base locus add up to 4; in other words, family containing one smooth member are indexed by partitions of 4, of which there are five. Conversely, if two pencils, each containing one smooth member, give rise to the same partition, then either one can be taken to the other by a projective change of coordinates. If all members of $\mathcal{C}$ are singular, then the base locus can be either a point, the union of a point and a line not passing through it, or a line. If it is a point P_0, then the pencil consists only of pairs of lines intersecting at that point, and no line is common to all such pairs. If it is the union $\{P_0\} \cup L$ for some point P_0 and line L such that $P_0 \notin L$, then the pencil consists of all reducible conics of the form $C_\Lambda = L \cup L_\Lambda$, where L_Λ is the pencil of all lines through P_0 (see Example 1.15.6). Finally, if the base locus is a line L, then there is a point $P_0 \in L$ such that the pencil again consists of all reducible conics of the form $C_\Lambda = L \cup L_\Lambda$, where L_Λ is the pencil of all lines through P_0. In these three degenerate case, the base locus completely determines the pencil up to projective changes of coordinates.[40] See Figure 1.10 for a picture illustrating these eight types, as well as their names. You are invited to prove these results in Exercise 2.6.2.

Example 1.15.8. We met examples of pencils of cubic curves in the proof of Pascal's Theorem (Theorem 1.13.5); see Figure 1.8 for an illustration.

[40] This happens also in the first case (i.e. when $\mathcal{C}$ has at least one smooth member), if we think of the base locus scheme-theoretically, i.e. as remembering what the multiplicities at each point of intersection are.

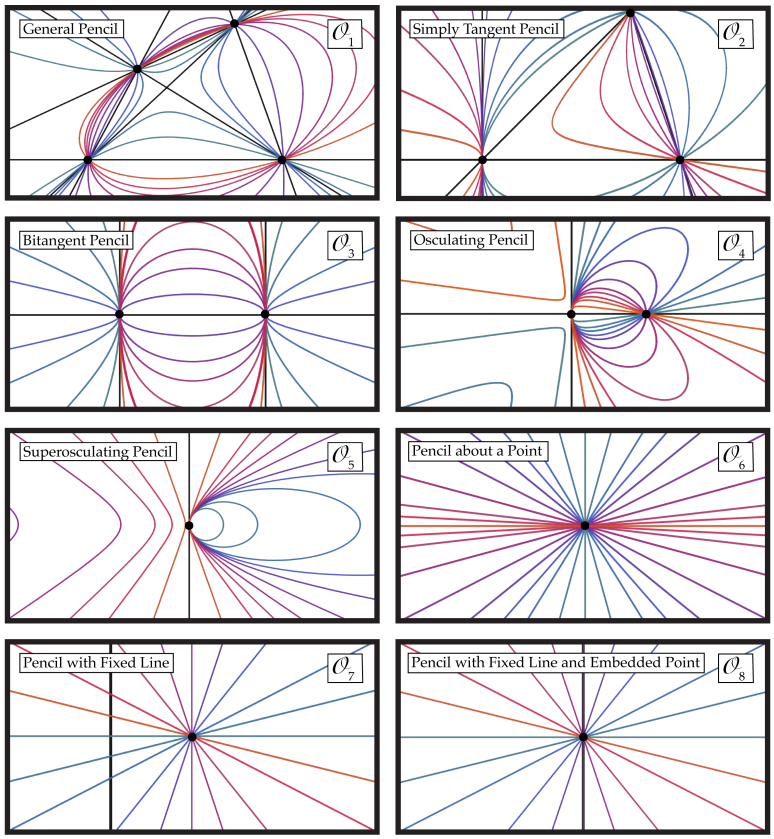

Figure 1.10: The eight types of pencils of conics up to projective changes of coordinates. Picture(s) made with Desmos.

Unfortunately, there are only finitely many types of pencils of degree d curves in $\mathbb{P}^2_k$, up to projective changes of coordinates, iff $d \in \{1, 2\}$. In general, for $d \geq 3$, classification of all pencils of curves of degree d, even in $\mathbb{P}^2_k$, is a very difficult problem. We will discuss the case of $d = 3$ in detail when we talk about the classification of elliptic curves in $\mathbb{P}^2_k$.

Here's one cool thing we can say about pencils of conics.

Theorem 1.15.9. Let k be an algebraically closed field of characteristic other than 2, and let $\mathcal{C}$ be a pencil of conics in $\mathbb{P}^2_k$. Then either every member of $\mathcal{C}$ is reducible, or at most 3 are.

Proof. Note that if $\operatorname{ch} k \neq 2$, then a quadratic homogeneous polynomial $Q \in k[X, Y, Z]_2$ can be written as

$$Q = \begin{bmatrix} X & Y & Z \end{bmatrix} \begin{bmatrix} A & H & E \\ H & B & F \\ E & F & C \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix},$$

where the matrix in the middle determines, and iis uniquely determined, by Q[41] If we denote

[41] This is the reason that the classification of projective conics is intimately related to the theory of binary quadratic forms. See Remark 1.12.15

this matrix by M_Q, then we see that

$$\begin{bmatrix} \partial_X Q \\ \partial_Y Q \\ \partial_Z Q \end{bmatrix} = 2 \cdot M_Q \cdot \begin{bmatrix} X \\ Y \\ Z \end{bmatrix}.$$

In particular, it follows from the Projective Jacobi Criterion (Theorem 1.12.10) that the conic C_Q defined by Q (when $Q \neq 0$) is singular iff M_Q has a nonzero kernel (i.e. a nonzero eigenvector with eigenvalue 0), which happens iff $\det M_Q = 0$, as we have talked about several times. Now given two such linearly independent Q_1, Q_2 and corresponding matrices $M_i := M_{Q_i}$ for $i = 1, 2$, the pencil $\mathcal{C}$ containing $C_i = C_{Q_i}$ for $i = 1, 2$ is given by taking C_Λ to be the curve defined by the vanishing of $\lambda Q_1 + \mu Q_2 = 0$. The matrix representative of this quadric is given exactly by

$$\lambda M_{Q_1} + \mu M_{Q_2}.$$

By the first observation, the reducible conics of the pencil $\mathcal{C}$ correspond exactly to the roots Λ of the equation

$$\det(\lambda M_{Q_1} + \mu M_{Q_2}) = 0.$$

Since this is homogeneous cubic equation in λ and μ, it is either identically zero (in which case every member of $\mathcal{C}$ is reducible), or it has at most three roots, in which case at most three members of $\mathcal{C}$ are reducible, and the rest smooth. ■

Note that a pencil can have any number of singular members between 1 and 3 (inclusive)– the precise number corresponds to the multiplicities of the roots of the cubic polynomial $\det(\lambda M_{Q_1} + \mu M_{Q_2})$, and can also be read off from the geometry of the base locus (how?).

Example 1.15.10. Let k be an algebraically closed field and let $C, D \subset \mathbb{P}^2_k$ be two conics that intersect in exactly 4 distinct points $P_1, \ldots, P_4$. In this case, these four points must be in general position (Definition 1.12.4); indeed, if some three of them were to lie on a line L, then every conic through them would have to contain L (by Bézout's Theorem for lines or conics), and hence any two distinct conics passing through them would intersect in all points along L, of which there are infinitely many (Proposition 1.11.13).

In this case, the pencil of conics containing C and D is said to be a general pencil; see the case $\mathcal{O}_1$ in Figure 1.10 for an illustration of this type of pencil. The claim is that such a pencil consists of all conics passing through these four points (and, in particular, always contains smooth members). This can be proven using Max Noether's Fundamental Theorem (Theorem 1.16.1) which we will use to prove Chasles's Theorem (Theorem 1.15.14) next time, or using a dimension argument on the number of linear constraints imposed on conics by four points in general position, but an alternative, direct, proof runs as follows. Let E be any other conic passing through these four points, and pick a fifth point P_5 on E distinct from $P_1, \ldots, P_4$. Since no four of $P_1, \ldots, P_5$ are collinear, it follows that E is the unique conic passing through $P_1, \ldots, P_5$ (Theorem 1.13.12(b)). In particular, if we can find a conic E' in the pencil spanned by C and D that contains P_5, then we would have shown that $E = E'$ and hence that E is in the pencil spanned by C and D.

For this, we claim first that $P_5 \notin C \cup D$; indeed, if $P_5 \in C$, then by Bézout's Theorem for conics (Theorem 1.13.4), we know that E and C share a component. Since E and C are distinct conics, this can only happen in $E = L_1 \cup L_2$ and $C = L_2 \cup L_3$ for some distinct lines $L_1, L_2, L_3 \subset \mathbb{P}^2_k$ with $P_5 \in L_2$. Since L_2 contains exactly two of the four points P_i, say P_1 and P_2, and both E and C pass through P_3 and P_4 as well, it follows that both L_1 and L_3 are lines joining P_1 and P_4, whence $L_1 = L_3$, which is a contradiction. Therefore, as in the proof of Theorem 1.13.5, if we take F and G to be homogeneous equations defining C and D respectively, and

pick a representative (X_0, Y_0, Z_0) for $P_5 = [X_0 : Y_0 : Z_0]$, then $F(X_0, Y_0, Z_0) \cdot G(X_0, Y_0, Z_0) \neq 0$, and the curve $E' = C_\Lambda = C_{\lambda F + \mu G}$ in the pencil spanned by C and D, where

$$\Lambda = [\lambda : \mu] = [-G(X_0, Y_0, Z_0) : F(X_0, Y_0, Z_0)]$$

contains P_5, and we are done. (That Λ is well-defined uses that $P \notin C \cup D$, or at least that one of $P \notin C$ and $P \notin D$ holds.)

Therefore, we have shown that a general pencil of conics is exactly the set of all conics that pass through four points $P_1, \ldots, P_4$ in $\mathbb{P}^2_k$ in general position. Since any such tuple of points can be taken to any other by a projective change of coordinates (this was Proposition 1.12.5), it follows that any two general pencils are related by a projective change of coordinates. This is an $1/8^{\text{th}}$ of the solution to Exercise 2.6.2.

Finally, note that if $\mathcal{C}$ is a general pencil of conics through the points $P_1, \ldots, P_4$, then we can see explicitly what the exactly three reducible conics in $\mathcal{C}$, as suggested by Theorem 1.15.9 are: namely, they are the three pairs of lines that are opposite edges of the complete quadrilateral with vertices $P_1, \ldots, P_4$; i.e. if for $1 \leq i < j \leq 4$, we let L_{ij} be the line joining P_i and P_j, then the three reducible conics are exactly $L_{12} \cup L_{34}, L_{13} \cup L_{24}$ and $L_{14} \cup L_{23}$.

This observation gives us a way to find the intersection points of two conics that intersect in 4 points as follows. Given equations Q_1 and Q_2 of conics intersecting in 4 distinct points, we find the roots of the cubic polynomial $\det(\lambda M_{Q_1} + \mu M_{Q_2})$ (say via Cardano's method), and use this to find the singular members of the pencil spanned by Q_1 and Q_2. Then we decomposition the equation of these singular members into equations of the corresponding lines (by solving quadratic equations). Finally, the four intersection points of the original conics will be contained in the 6 pairwise intersection points of these lines, and lines are easy enough to intersect.

Example 1.15.11. Here's an example of how to use pencils of conics to solve the quartic equation, at least when the characteristic of the base field is other than 2. Suppose we are trying to solve the equation

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

over a field k with $\operatorname{ch} k \neq 2$. It is easy to see (check!) that solving this equation is equation amounts to finding the intersection points of the two parabolae given by the vanishing of the homogeneous polynomials

$$\begin{aligned} Q_1 &= Y^2 + aXY + bYZ + cXZ + dZ^2, \text{ and} \\ Q_2 &= YZ - X^2, \end{aligned}$$

since they do not intersect on the line at infinity. Then the corresponding matrices M_{Q_1} and M_{Q_2} are easily seen to be

$$M_{Q_1} := \begin{bmatrix} 0 & a/2 & c/2 \\ a/2 & 1 & b/2 \\ c/2 & b/2 & d \end{bmatrix} \text{ and } M_{Q_2} := \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1/2 \\ 0 & 1/2 & 0 \end{bmatrix},$$

whence

$$\det(\lambda M_{Q_1} + \mu M_{Q_2}) = -\frac{1}{4}\left[\left(a(ad - bc) + c^2\right)\lambda^3 + (ac - b^2 + 4d)\lambda^2\mu + 2b\lambda\mu^2 - \mu^3\right].$$

Then, we may solve this cubic, and use this as suggested in Example 1.15.10 to find the intersection points of C_{Q_1} and C_{Q_2}, and hence the roots of the quartic equation. You are invited to work out one (carefully chosen) example in detail in Exercise 2.6.3. The whole procedure above can be simplified slightly by first depressing the quartic (i.e. replacing X by $X - (1/4)a$) and then applying the above procedure. For a (slightly) more detailed explanation of the procedure and its connection to Galois theory, as well as references, see [5, §1.14].

1.15.2 An Introduction to Elliptic Curves

We now want to focus on the next simplest case of curves after the conics, namely the cubic curves. We already classified all singular plane cubics up to projective changes of coordinates (at least over algebraically closed fields of characteristic other than 3) in Exercise 2.4.4, so we may now focus on the case of smooth cubics–it turns out that such curves admit a very rich theory, which makes them very powerful objects in modern algebraic geometry.

Definition 1.15.12. An elliptic curve (over a field k) is a pair (E, O), where $E \subset \mathbb{P}^2_k$ is a smooth cubic curve, and $O \in E$.

The reader will not lose much by imagining k to be algebraically closed (otherwise our definition of smoothness is not quite the right one), and soon we will be assuming $\operatorname{ch} k \neq 2, 3$ as well for convenience, but it is helpful to have the right level of generality and to be able to talk about points of elliptic curves over finite fields, for instance.

Now consider the binary operation $+ : E \times E \to E$ defined as follows: given a pair $(A, B) \in E \times E$, let the line[42] $L_{A,B}$ joining A and B intersect the curve E in the third point D.[43] Then we define $A + B := +(A, B)$ to be the third point of intersection of E and the line $L_{O,D}$ joining O and D. See Figure 1.11. The key claim, from which the power of elliptic curves comes, is

Theorem 1.15.13. Let (E, O) be an elliptic curve. Then the binary operation $+ : E \times E \to E$ defined above makes E into an abelian group with identity O.

Proof. Commutativity of $+$ is clear, as is the fact that $A + O = A$ for all $A \in E$: indeed, if the line $L_{A,O}$ meets the curve again in A', then the line $L_{O,A'}$ meets the curve again in A. To find inverses, consider once and for all the point $O' \in E$ which is the third point of intersection of the tangent line $L_{O,O} = \mathrm{T}_O E$ with E; then it is easy to see that given any $A \in E$, the third intersection point A'' of $L_{AO'}$ with E has the property that $A + A'' = O$. Finally, we have to show associativity.

For this, consider points $A, B, C \in E$. Let D denote the third intersection of $L_{A,B}$ with E, let F denote the third intersection of $L_{A+B,C}$ with E, and let G denote the third intersection of $L_{B,C}$ with E. (See Figure 1.11.) To show associativity, it suffices to show that the line $L_{A,B+C}$ passes through F (check!). Temporarily denote the third intersection point of $L_{A,B+C}$ with E by F'; then we have to show that $F = F'$.

Consider the cubic curves $\Gamma := L_{A,B} \cup L_{C,F} \cup L_{O,G}$ and $\Sigma := L_{B,C} \cup L_{A,B+C} \cup L_{O,D}$, and note that

$$E \cap \Gamma = \{O, A, B, C, D, G, A + B, B + C, F\} \text{ and}$$
$$E \cap \Sigma = \{O, A, B, C, D, G, A + B, B + C, F'\}.$$

In particular, Σ is a cubic curve that passes through 8 of the 9 intersection points of the cubic curves E and Γ. Therefore, the proof is finished by the following theorem (Theorem 1.15.14). ■

[42] When $A = B$, we take $L_{A,B}$ to be the tangent line to E at A, which we can do uniquely since E smooth.

[43] Here we are using Bézout's Theorem (Theorem 1.14.1 or at least Theorem 1.12.12). We do not disallow the possibility that $D = A, B, O$. For instance, $D = A$ if $A \neq B$ but the line $L_{A,B}$ is tangent to E at A, or if $A = B$ and $L_{A,B}$ meets E with multiplicity three at A (i.e. A is an inflection point of E). I will leave such considerations to the reader, but see also Remark 1.15.16.

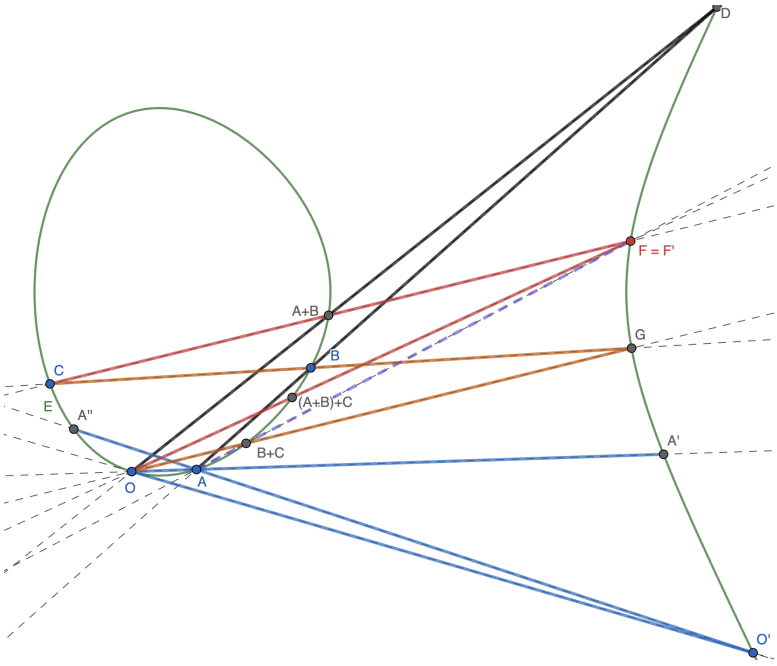

Figure 1.11: The addition law on an elliptic curve. Picture made with GeoGebra.

Theorem 1.15.14 (Chasles). Let $D, E \subset \mathbb{P}^2_k$ be two cubic curves that intersect in 9 points $P_1, \ldots, P_9$. 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.

There are many ways to prove Theorem 1.15.14. One approach is to use a dimension count: each point of intersection imposes one linear condition on the space $\mathbb{P}^9_k$ of homogeneous cubic equations, and so imposing 8 such general conditions brings us down to a $\mathbb{P}^1_k \subset \mathbb{P}^9_k$, i.e. a pencil of cubic curves. If C and D are two members of this pencil, then any other cubic curve passing through these 8 points belongs to the pencil spanned by C and D and hence also passes through the 9th point. For this argument to work, the points need to be in sufficiently general position–it turns out to be sufficient to assume that no 7 of the points $P_1, \ldots, P_9$ lie on a conic. For an argument along these lines, see either [5, Prop. 2.6], or this blog post [7] by Terry Tao. This $8 \Rightarrow 9$ phenomenon can be fruitfully generalized in the direction of the number of linear conditions imposed by points in projective space, resulting in the so-called the Cayley-Bacharach Theorem. Sometimes Theorem 1.15.14 itself is called the Cayley-Bacharach theorem, but this is a misnomer–see this paper [8] by Eisenbud, Green, and Harris[44] for an explanation of the Cayley-Bacharach Theorem and its relation to Chasles's Theorem. Next time, we will give a proof of Theorem 1.15.14 using a local-to-global principle called Max Noether's Fundamental Theorem (Theorem 1.16.1).

Remark 1.15.15. Chasles's Theorem (Theorem 1.15.14) immediately implies those of Pascal (Theorem 1.13.5) and Pappus (Theorem 1.13.7); for instance, to deduce Pascal's Theorem in the notation used in that section, we can take the two cubic curves to be $D := L_1 \cup L_3 \cup L_5$ and $E := L_2 \cup L_4 \cup L_6$ (so the intersection points are $P_1, \ldots, P_6, Q_1, Q_2, Q_3$), and then take X to be the union of the conic C and the line L joining Q_1 and Q_2.

[44] Harris was my advisor!

Remark 1.15.16. The proof of Theorem 1.15.13 and the statement of Theorem 1.15.14 certainly work as written when all the 9 involved points are distinct, but that is not quite sufficient to prove Theorem 1.15.13. We also need to take into account intersection multiplicites and tangencies. There are a few ways to get around this. Over fields such as $k = \mathbb{R}$ or $k = \mathbb{C}$, we may use continuity arguments, as in indicated for instance in [5, §I.2]. Over general fields, we can use a similar argument, but using the rigidity of complete varieties instead, as explained in [9, Chapter 3]. Alternatively, one can write down explicit formulae for the group law and verify all the claims directly via (very tedious computation). Finally, we can treat the whole theory as above somewhat more carefully using the notion of intersection multiplicities already introduced, and note that Theorem 1.15.14 also works when we counts point with intersection multiplicity[45]. This last one is, generally speaking, the approach we will take, as we shall see in the proofs next time.

Remark 1.15.17. Suppose that an elliptic curve E defined over a field k is smooth over its algebraic closure $\overline{k}$. The above addition law tells us then that the set of k-rational points $E(k)$ of E form a subgroup of $E(\overline{k})$–indeed, this follows from the group law because the third intersection point of a L joining two k-points with a cubic curve defined over k is also defined over k–this is because a cubic equation with coefficients in k and two roots in k must also have its last root in k.

In particular, for instance, it makes sense to talk about, say, the subgroup real points of a complex elliptic curve which is defined over the real numbers and has $O \in E(\mathbb{R})$. Such a "real elliptic curve" is then a topological–even Lie–group. It seems also from Figure 1.11 above that the sums $A+B, B+C$ and $A+B+C$ lie on the same component of the two-component elliptic curve as A, B, C, as long as this component contains O, i.e. that the component containing O of a real two-component elliptic curve is a subgroup of the whole curve under the addition law, although it is not an algebraic curve itself (Example 1.7.15). You are invited to explore this in Exercise 2.6.8.

Next time, we will prove Theorem 1.15.14 and start working with explicit examples of elliptic curves.

[45] For instance, if instead of 9 distinct points $P_1, \ldots, P_9$ we have only 8 distinct points $P_1, \ldots, P_8$ of intersection but tangency at P_8, then the statement says also that if X passes through $P_1, \ldots, P_8$, then it is also tangent to both D and E at P_8.