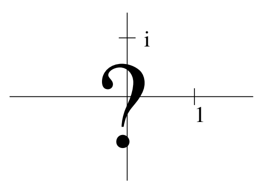
CHAPTER 1

Two theorems on conics in the plane

The primary subject of this course is *algebraic curves*, the simplest example of which is *the solution set of a two-variable polynomial equation in the plane*. *What* plane? $\mathbb{R}^2$, $\mathbb{C}^2$, $\mathbb{F}_p^2$, $\mathbb{Q}^2$...? For the purposes of this course, mainly $\mathbb{C}^2$, with excursions into the others.

1.0.1. REMARK. A perennial point of confusion is whether to call $\mathbb{C}$ the complex plane.



This is henceforth forbidden! It is the *complex (affine) line*, and a *real (affine) plane* via $\mathbb{C} \cong \mathbb{R}^2$. (A "complex plane" will mean something 2-dimensional over $\mathbb{C}$, so $\mathbb{C}^2$ will be the complex affine plane, $\mathbb{P}^2$ the complex projective plane, and so forth. We'll worry about affine vs. projective in the next chapter.) Note that $\mathfrak{H} := \{x + iy \mid x, y \in \mathbb{R},\, y > 0\} \subset \mathbb{C}$ will denote the "upper-half plane" in $\mathbb{C}$; that terminology is unavoidable.

The objects which shall concern us, then, will be 1-dimensional over $\mathbb{C}$ ("complex algebraic curves"), hence 2-dimensional over $\mathbb{R}$ ("Riemann surfaces"). Our approach will be quite intuitive and visual for the first few chapters, to get an idea of what algebraic geometry is before settling into a more measured approach. My feeling has always been that you need motivation for introducing formalism, in this case for layering lots of algebra onto geometry. In this chapter that motivation might consist of the subtle gaps that open as we try to prove some famous results on conics from (mostly) linear algebra.

1.0.2. EXAMPLE. (a) Consider the set of rational points on the Fermat quartic (degree 4) curve:

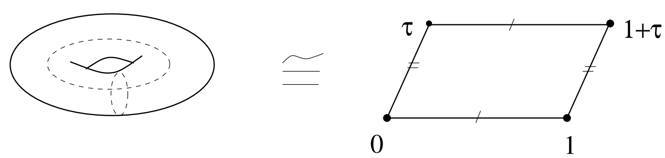
$$\{(x,y) \in \mathbb{Q}^2 \mid x^4 + y^4 = 1\} \subset \mathbb{Q}^2. \tag{1.0.3}$$

By a case of Fermat's last theorem, (1.0.3) $\cap (\mathbb{Q}^*)^2$ is the empty set, since $\left(\frac{a}{b}\right)^4 + \left(\frac{c}{d}\right)^4 = 1$ means $(ad)^4 + (bc)^4 = (bd)^4$ with $ad, bc, bd \in \mathbb{Z}$ and $bd \neq 0$. That is, (1.0.3) $= \{(1,0), (-1,0), (0,1), (0,-1)\}$.

(b) Next we look at the Fermat cubic (degree 3) curve

$$\{(x,y) \in \mathbb{C}^2 \mid x^3 + y^3 = 1\} \subset \mathbb{C}^2. \tag{1.0.4}$$

We will see that (1.0.4) has the structure of a complex 1-torus, shown on the left-hand side in

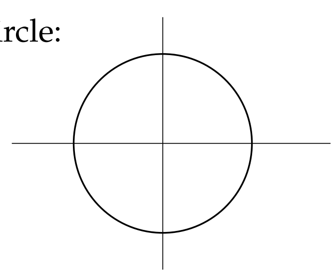


The right-hand side represents the quotient $\mathbb{C}/\Lambda$ of the complex line by the lattice $\Lambda := \mathbb{Z}\langle 1, \tau\rangle$ (for some $\tau \in \mathfrak{H}$). What is the isomorphism? It holds topologically (convince yourself of this visually) for any $\tau \in \mathfrak{H}$, but complex analytically only for the values $\tau = \frac{a\tau_0 + b}{c\tau_0 + d}$ where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ and $\tau_0 := \frac{1+\sqrt{-3}}{2}$. We call (1.0.4) an elliptic curve: it isn't an ellipse in any sense, but originally arose in connection with the arc-length of one.

(c) Finally, take the real degree 2 (a.k.a. "quadric" or "conic") curve

$$\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\} \subset \mathbb{R}^2, \tag{1.0.5}$$

which is of course a circle:



First we shall pursue conics to get a preliminary feel for the interplay between algebra and geometry. These aren't too hard to visualize: you know what the real solution sets look like (ellipses, hyperbolas, pairs of lines, etc.) and the complex solutions are all spheres once we add "points at infinity".

1.1. Algebraic curves in $\mathbb{R}^2$

Let $\mathcal{P}_2^n$ denote the real polynomials of degree $\leq n$ in x and y. (If there is no possibility for confusion, I'll just write $\mathcal{P}^n$.) In an exercise below, you are asked to prove that $\mathcal{P}_2^n$ is a real vector space of dimension $\binom{n+2}{2}$.

1.1.1. EXAMPLE. (a) A basis for $\mathcal{P}^2$ is given by $\{1, x, y, xy, x^2, y^2\}$, so $\dim(\mathcal{P}_2) = 6$.

(b) For $\mathcal{P}^3$, the basis is $\{1, x, y, xy, x^2, y^2, x^3, x^2y, xy^2, y^3\}$ (and the dimension is 10).

For a configuration of distinct points

$$\mathcal{S} = \{p_1, \ldots, p_m\} \subset \mathbb{R}^2,$$

define a linear "**ev**aluation" map

$$ev_{\mathcal{S}}^n : \mathcal{P}^n \longrightarrow \mathbb{R}^m$$

via

$$f \longmapsto \begin{pmatrix} f(p_1) \\ \vdots \\ f(p_m) \end{pmatrix}.$$

Recall from linear algebra the **Rank + Nullity** theorem:

$$\underbrace{\dim(\mathrm{image}(ev_{\mathcal{S}}))}_{rank} + \underbrace{\dim(\ker(ev_{\mathcal{S}}))}_{nullity} = \dim(\mathcal{P}^n). \tag{1.1.2}$$

1.1.3. DEFINITION. $\mathcal{S}$ is called *n-general*[1] $\iff$ $ev_{\mathcal{S}}^n$ is surjective (i.e., onto).

[1] or just "general" or "generic" if the context is understood

Now if $ev^n_{\mathcal{S}}$ is surjective, its rank is m; while its kernel is just the space of polynomials vanishing on $\mathcal{S}$. By (1.1.2) we have:

1.1.4. PROPOSITION. *The space of degree $\leq n$ polynomials vanishing on a general configuration of m points has dimension $\binom{n+2}{2} - m$.*

What does all this have to do with algebraic curves? Well, given a polynomial in $\mathcal{P}^n$, I can look at its solution set in $\mathbb{R}^2$. More precisely, we have the assignment[2]

$$\mathcal{P}^n \backslash \mathcal{P}^{n-1} \rightsquigarrow \{\text{degree } n \text{ real affine algebraic curves}\}$$

given by

$$f \longmapsto C_f := \{(x,y) \in \mathbb{R}^2 \mid f(x,y) = 0\}.$$

Notice that

$$f \in \ker(ev_{\mathcal{S}}) \iff C_f \supset \mathcal{S}. \tag{1.1.5}$$

1.1.6. PROPOSITION. *Through five (2-)general points A, B, C, D, E in the real plane, there exists a unique conic Q.*

PROOF. $6 - 5 = 1$. ☐

OK, OK, so what the proof means is: by Prop. 1.1.4, the space of degree ≤ 2 polynomials vanishing on a general configuration of 5 points has dimension $\binom{2+2}{2} - 5 = 1$. So given two degree-2 polynomials $f, g \in \mathcal{P}^2$ vanishing at all 5 points in $\mathcal{S}$, we must have $g = a \cdot f$ (for some $a \in \mathbb{R}$). But $f = 0$ and $a \cdot f = 0$ define the same curve Q; and by (1.1.5) Q contains A, B, C, D, E.

There are two issues with this. First, in order for f to define a conic, we need to know that the 1-dimensional space of solutions doesn't lie in $\mathcal{P}^1$ (inside $\mathcal{P}^2$). But if a linear (degree 1) polynomial h vanishes at all 5 points, so does h^2; and then since $h, h^2 \in \mathcal{P}^2$ are not linearly dependent, $ev^2_{\mathcal{S}}$ doesn't have maximal rank, contradicting the genericity condition on $\mathcal{S}$. (At this point, Proposition 1.1.6 is completely proved as stated.)

[2]notation: $\mathcal{A} \backslash \mathcal{B}$ denotes set-theoretic exclusion, sometimes also written $\mathcal{A} - \mathcal{B}$. "Affine" just means that the curves are in $\mathbb{R}^2$.

The second problem is more interesting: what exactly does it mean for A, B, C, D, E to be 2-general? If you think about our little proof, the existence of Q has nothing to do with this genericity, but the uniqueness has everything to do with it. Moreover, the statement that "Q is unique if $\mathcal{S}$ is generic" is somewhat circular without knowing (beyond Definition 1.1.3) what the genericity condition is: namely, that *no four of the points are collinear.* It's best to wait until we're doing projective geometry to prove that, and so we will.

1.1.7. REMARK. More generally, the abstract ethos surrounding the word "general" in algebraic geometry is that you are working in the complement of finitely many algebraic conditions. The "algebraic condition" we are avoiding in this section is the vanishing of all $m \times m$ minors in a matrix representing $ev^n_{\mathcal{S}}$.

1.2. Blaise Pascal and the mystic hexagon

Similarly, given eight points

$$A,\ B,\ C,\ D,\ E,\ P_1,\ P_2,\ P_3$$

in (3-)general position, the vector space of cubic polynomials vanishing at all of them has dimension

$$\binom{3+2}{2} - 8 = 2.$$

Call this vector space V, and write $(x_A, y_A), \ldots, (x_{P_3}, y_{P_3})$ for the coordinates of given points. V lies in $\mathcal{P}^3$, which consists of elements of the form

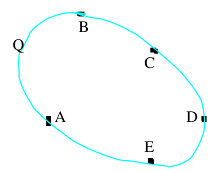
$$a_1 + a_2 x + a_3 y + \cdots + a_9 x y^2 + a_{10} y^3 = f_{\underline{a}}(x, y).$$

Asking a polynomial of this form to vanish at our 8 points yields the 8 equations

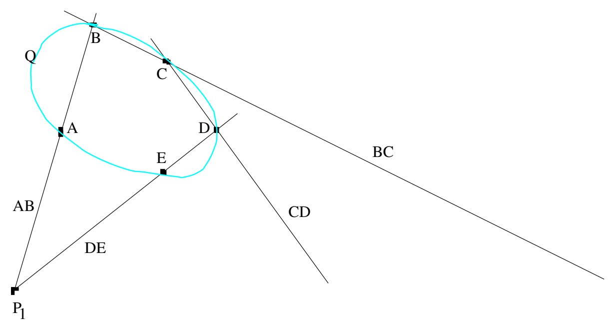
$$\left\{ \begin{array}{rcl} 0 & = & a_1 + a_2 x_A + a_3 y_A + \cdots + a_9 x_A y_A^2 + a_{10} y_A^3 \\ & \vdots & \\ 0 & = & a_1 + a_2 x_{P_3} + a_3 y_{P_3} + \cdots + a_9 x_{P_3} y_{P_3}^2 + a_{10} y_{P_3}^3 \end{array} \right. ,$$

i.e. 8 linear constraints on the 10 variables $\{a_j\}$ expressing what it means for $f_{\underline{a}}$ to lie in V.

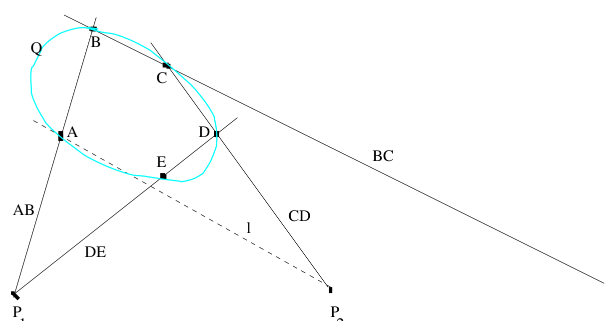
Now let A, B, C, D, E be (2-)general, and take Q to be the unique conic through them:



In fact, we shall make the stronger assumption that no three of A, B, C, D, E are collinear, so that Q is smooth (an ellipse or hyperbola, not a pair of lines). We would like to construct (arbitrarily many) points on Q using only a straightedge. Start by drawing secant lines connecting adjacent points:

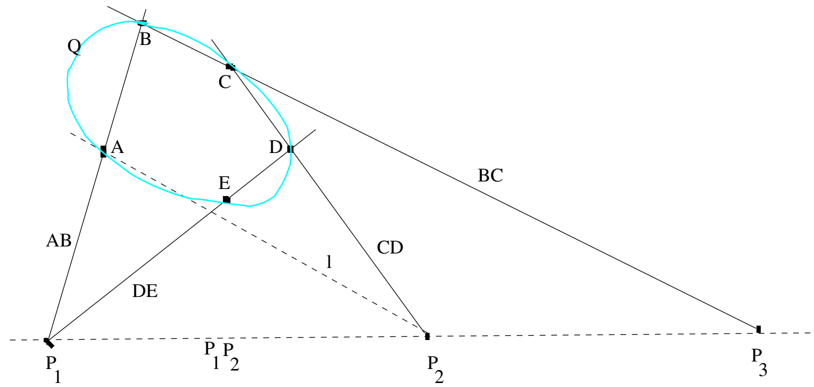


where we have labelled $AB \cap DE =: P_1$.[3] Next, draw any line ℓ through A that does not pass through B, C, D, or E, and set $\ell \cap CD =:$ P_2 as in the next figure:

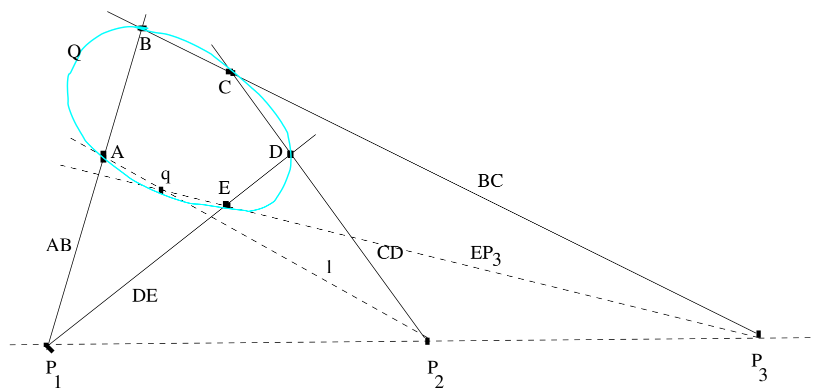


[3]Of course, the lines may be parallel. There are two ways to fix this: either make A, B, C, D, E "more" general so that none of the lines we intersect are parallel; or work projectively. Since this chapter is entirely motivational we won't worry about that level of detail.

(Note that our choice of ℓ will determine the point $q \in Q$ we end up constructing.) Next, draw P_1P_2, and label $P_1P_2 \cap BC =: P_3$.



Finally, we draw EP_3 and set $q := EP_3 \cap \ell$.



1.2.1. PROPOSITION. $q \in Q$.

To prove this, we shall require:

1.2.2. LEMMA. *$A, B, C, D, E, P_1, P_2, P_3$ is in (3-)general position, when A, B, C, D, E are general in the strong sense assumed above.*

We won't prove the lemma here. (It is a special case of something called the Cayley-Bacharach Theorem, which will be easy to prove once we know a little about residues in algebraic geometry.)

PROOF OF PROP. 1.2.1. We write $f_{AB}(x, y) = 0$ for the (linear) equation of the line AB, $f_Q(x, y) = 0$ for the conic Q, and so forth.

Consider the three cubic polynomials

$$f_1(x,y) := f_Q(x,y) \cdot f_{P_1P_2}(x,y),$$

$$f_2(x,y) := f_{AB}(x,y) \cdot f_{CD}(x,y) \cdot f_{EP_3}(x,y),$$

$$f_3(x,y) := f_\ell(x,y) \cdot f_{BC}(x,y) \cdot f_{DE}(x,y).$$

Their vanishing sets are

$$C_1 := Q \cup P_1P_2,$$

$$C_2 := AB \cup CD \cup EP_3,$$

$$C_3 := \ell \cup BC \cup DE,$$

each of which contains the set

$$\mathcal{S} := \{A, B, C, D, E, P_1, P_2, P_3\}.$$

So by (1.1.2), f_1, f_2, f_3 belong to $V := \ker(ev^3_{\mathcal{S}})$. Since the dimension of V is 2, f_1, f_2, f_3 cannot be linearly independent and we have a nontrivial[4] relation

$$\alpha f_1 + \beta f_2 + \gamma f_3 = 0 \tag{1.2.3}$$

with real coefficients.

Suppose $\alpha = 0$ in (1.2.3). Then $\beta f_2 = -\gamma f_3$, so that f_2 and f_3 are proportional hence cut out the same curve:

$$AB \cup CD \cup EP_3 = \ell \cup BC \cup DE.$$

But this means $\ell = AB$, CD or EP_3, which implies that ℓ contains A, B, C, D, or E — a contradiction to our choice of ℓ!

So $\alpha \neq 0$, and we may rewrite (1.2.3) as

$$f_1 = -\frac{\beta}{\alpha} f_2 - \frac{\gamma}{\alpha} f_3. \tag{1.2.4}$$

Now since ℓ and EP_3 both contain q, f_2 and f_3 both vanish at q. By (1.2.4), f_1 also is zero at q, so one of its factors has to be. Therefore q is contained in Q or P_1P_2.

[4]not all of α, β, γ are zero

Suppose $q \in P_1P_2$. Then the lines P_1P_2, EP_3, and ℓ "collapse" to the same line (look at the last diagram) and so in particular $E \in \ell$, again in contradiction to our choice of ℓ.

We conclude that $q \in Q$. $\square$

In the construction described pictorially above, q was — in light of Proposition 1.9 — ultimately just the point where ℓ meets Q. Since our choice of ℓ was essentially free, A, B, C, D, E, and q can be thought of as 6 distinct but otherwise arbitrary points of Q. Consequently, we have proved the beautiful statement:

1.2.5. THEOREM. [B. PASCAL, 1639] *Intercepts of opposite edges of a hexagon inscribed in a conic, lie on a line.*

When we get to the notion of duality in projective geometry, Theorem 1.2.5 will "dualize" for free to:

1.2.6. COROLLARY. *The (three) lines joining opposite vertices of a hexagon circumscribed about a conic, meet in a single point.*

1.3. Poncelet's Porism

According to my dictionary, a *porism* is a "proposition that uncovers the possibility of finding such conditions as to make a specific problem capable of innumerable solutions". The result of Poncelet I'll describe here just had a whole book devoted to it,[5] and in the late 1970's P. Griffiths (my Ph.D. advisor) and J. Harris devoted two nice articles to it. If your local watering hole had an ellipse-shaped pool table it would even have practical applications.

So let C and D be two conics in $\mathbb{R}^2$. They are the vanishing sets of some $f_C, f_D \in \mathcal{P}_2$. For simplicity, assume they are ellipses, with D contained in the interior of C.

Problem: *Does there exist a closed polygon (self-intersections are OK) inscribed in C and circumscribed about D?*

[5] L. Flatto, "Poncelet's Theorem", AMS, 2009.

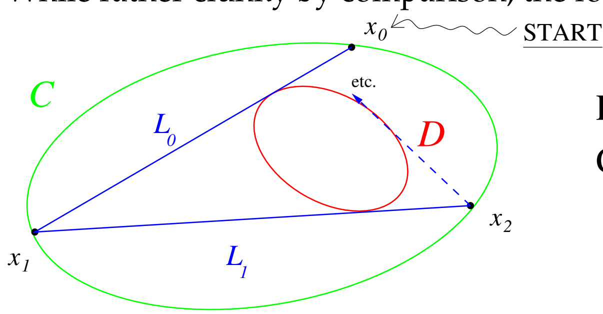
Solution: *Sometimes. But existence of one such polygon implies that there are infinitely many.*

This is clearly a "porism". We shall call such polygons as in the "Problem" *circuminscribed* when a specific pair C,D is understood. The precise statement is:

1.3.1. THEOREM. [PONCELET, 1822] *If the pair C, D has an n-sided circuminscribed polygon, then for any point on C there is a circuminscribed n-sided polygon with one vertex on C.*

Another way of putting this is that circuminscribed polygons can be rotated continuously: there are some nice interactive demonstrations of this online.[6]

While rather clunky by comparison, the following picture



Poncelet Construction

allows us to characterize Theorem 1.3.1 in one more way:

$$\text{If } x_n = x_0 \text{ for } \textit{any } x_0, \text{ then } x_n = x_0 \text{ for } \textit{every } x_0. \tag{1.3.2}$$

We will skirt around projective geometry in explaining the idea here, but can't avoid $\mathbb{C}$. Henceforth, C and D shall denote all complex solutions to $f_C = 0$ and $f_D = 0$ — that is, $C, D \subset \mathbb{C}^2$. Topologically these are "real surfaces" (in fact, spheres with one or two missing points), and are complex-analytically isomorphic to $\mathbb{C}$ or $\mathbb{C}^*$, but it won't hurt to draw them schematically as real curves on a sheet of paper. You can think of this as the real solutions standing in for the complex ones. In general, when we want to see the topology of

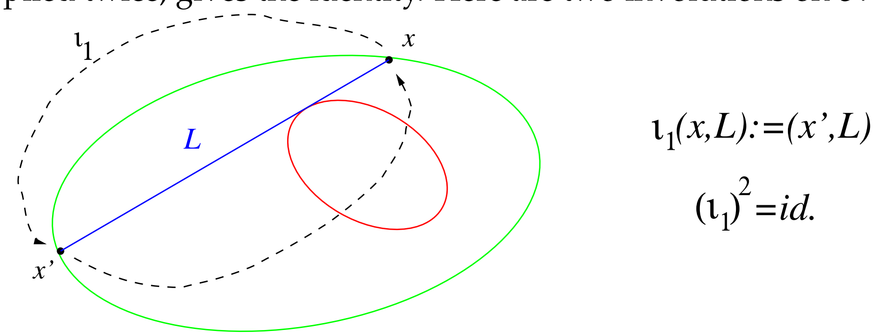
[6]e.g. https://demonstrations.wolfram.com/PonceletsPorismForQuadrilaterals/ and http://olivernash.org/2018/07/08/poring-over-poncelet/index.html

a complex algebraic curve, we'll draw a "surface"; when we want to see how different curves intersect or how they lie in space, we'll draw a "curve".

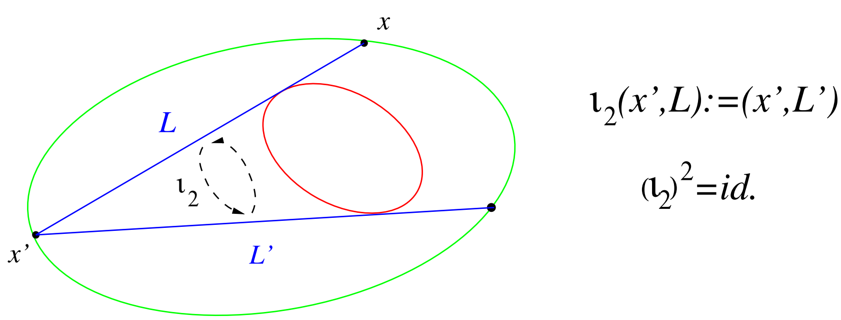
Consider the set of pairs

$$\mathcal{E} := \{(x, L) \in C \times \check{D} \mid x \in L\},$$

where $\check{D}$ is the set of lines tangent to D. An *involution* is a map which, applied twice, gives the identity. Here are two involutions on $\mathcal{E}$:



and



The composition

$$\jmath := \iota_2 \circ \iota_1$$

takes

$$(x, L) \overset{\iota_1}{\longmapsto} (x', L) \overset{\iota_2}{\longmapsto} (x', L') =: (x_1, L_1)$$

(ι_1, ι_2 and $\jmath$ are all maps from $\mathcal{E}$ to $\mathcal{E}$). More generally,

$$\jmath(x_i, L_i) =: (x_{i+1}, L_{i+1})$$

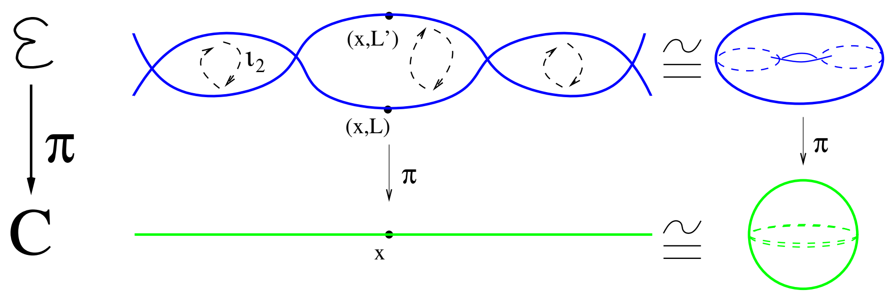
defines the i^{th} iteration of the Poncelet construction. The construction starting from some (x, L) closes if and only if

$$\jmath^n(x, L) = (x, L) \text{ for some } n. \tag{1.3.3}$$

Thinking of complex points, and assuming C and D aren't tangent anywhere and don't meet "at infinity" — that is, C and D are in general position in some sense — they meet in exactly four points. This is a first taste of Bezout's theorem, which we will prove carefully later. Now let $x \in C$: if $x \notin C \cap D$, there are exactly two lines containing x and tangent to D; if $x \in C \cap D$, there is only one. So we find that the projection

$$\begin{array}{rccc} \pi : & \mathcal{E} & \longrightarrow & C \\ & (x, L) & \longmapsto & x \end{array}$$

is a *two-sheeted branched covering* with four branch points:



This turns out to mean that $\mathcal{E}$ is an elliptic curve, hence isomorphic to $\mathbb{C}$/lattice. One deduces that $\jmath : \mathcal{E} \to \mathcal{E}$ is a translation

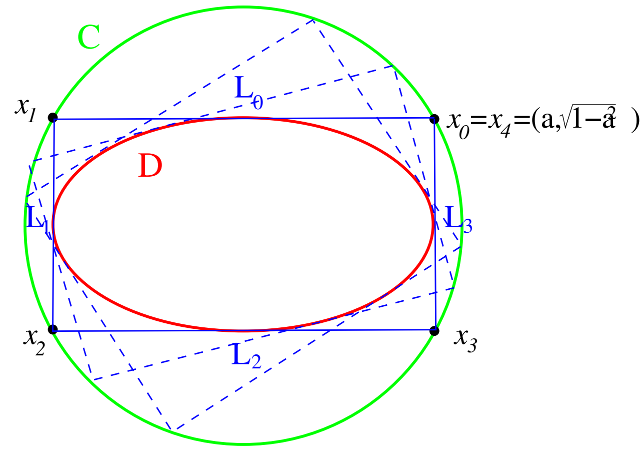
$$\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$$

$$u \longmapsto u + \xi,$$

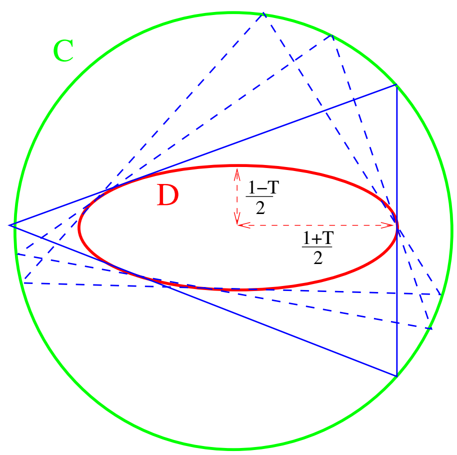
and our initial (x, L) is some point u_0. Whether or not $\jmath^n(u_0) \equiv u_0$ has everything to do with whether $n\xi \in \Lambda$, and nothing to do with the choice of u_0, and so (1.3.2) follows.

We will see a more in-depth treatment of this after studying elliptic curves, including an algebraic criterion for deciding when $\jmath^n =$ id. for a given C, D, and an analysis of elliptical billiards. For now, here are some examples of "Poncelet in action":

1.3.4. EXAMPLE. (a) $C = \{x^2 + y^2 = 1\}$, $D = \{\frac{x^2}{a^2} + \frac{y^2}{1-a^2} = 1\}$, $n = 4$.



(b) $C = \{x^2 + y^2 = 1\}$, $D = \{\frac{4x^2}{(1+T)^2} + \frac{4y^2}{(1-T)^2} = 1\}$, $n = 3$.



That these Poncelet trajectories really do close can be checked by hand, though it is a little messy (see Exercise (4)). A more efficient criterion will be developed later in the course.

Exercises

(1) Show that $\mathcal{P}_2^n$ is a vector space of dimension $\binom{n+2}{2}$. How does this generalize for polynomials in m variables instead of two?

(2) Consider the two conics $C = \{x^2 + y^2 = 1\}$ and $D = \{x^2 + y^2 = r^2\}$. The corresponding "Poncelet elliptic curve" $\mathcal{E}$ is singular

(see Definition 2.1.16), which means that the problem "degenerates" and is solvable by hand using high school math. For which r (say, between 0 and 1) does the n^{th} iterate of the Poncelet construction (starting at an arbitrary point on C) return to the starting point? (Hint: for each n, there are finitely many; just find how many, and the equation they must satisfy.)

(3) When the Poncelet construction doesn't close, its orbit is "equidistributed" in $\mathcal{E}$. In the setting of Exercise (2), where Poncelet orbits on the unit circle S^1 (i.e. real points of C) by adding multiples of some angle θ to the starting point/angle, this simply means that the orbit is equidistributed with respect to angular measure iff $\frac{\theta}{2\pi} \notin \mathbb{Q}$. Use this to show that in the $\infty \times 8$ matrix $M_{k\ell} := \langle\!\langle \ell^k \rangle\!\rangle$ ($k \geq 1$, $2 \leq \ell \leq 8$), where $\langle\!\langle \cdot \rangle\!\rangle$ takes the leftmost digit (in base 10), the frequency of $d \in \{1, 2, \ldots, 9\}$ in the ℓ^{th} column is independent of ℓ. What is this frequency?

(4) Check Example 1.3.4(b) for one, hence (granting Poncelet) all, starting points. (Hint: work out the bold triangle.)

(5) Given a quadrilateral $ABCD$ inscribed in a conic Q, show (by taking limits of hexagonal Pascal) that the four points given by $AB \cap CD$, $BC \cap AD$, $T_A Q \cap T_C Q$, and $T_B Q \cap T_D Q$ ($T_p Q$ is the tangent line to Q at p) lie on a line. Also state a version for triangles inscribed in Q.