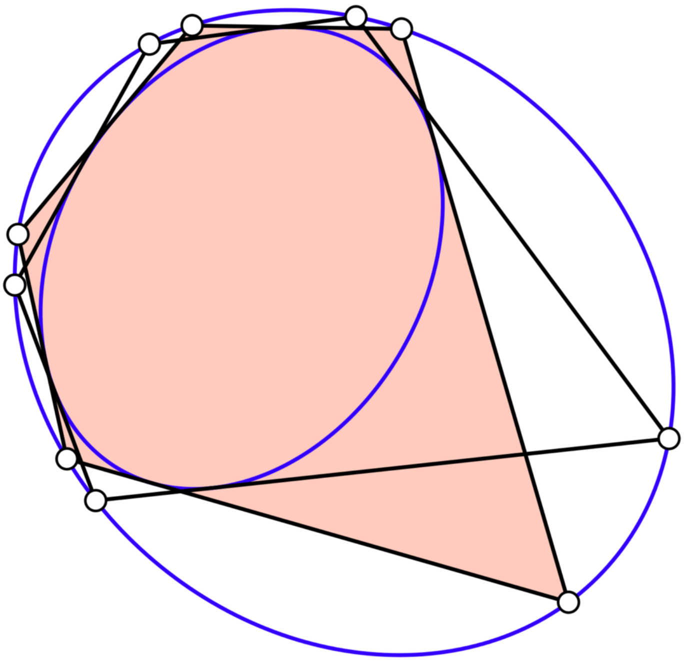
rijksuniversiteit
groningen

An explicit algebro-geometric proof of Poncelet's closure theorem

and a connection with dynamical billiards



Bachelor thesis in Mathematics
August 28, 2013
Student: R.T. Buring
Supervisor: Prof. dr. J. Top
Second assessor: Prof. dr. H.S.V. de Snoo

Abstract

Poncelet's closure theorem concerns pairs of conics in the plane, and the existence of a fixed point of a certain geometric construction. Griffiths and Harris gave an elegant modern proof of the closure theorem using methods from algebraic geometry, in which an elliptic curve takes the center stage. The proof presented here is similar, but differs in the details. Whereas they used the theory of Riemann surfaces for the details of the proof, a more algebraic and explicit approach is taken here. A connection between the closure theorem and dynamical billiards in ellipses is explored.

Contents

Introduction

Jean-Victor Poncelet took part in Napoleon's invasion of Russia in 1812. He was part of the group that did not follow Marshal Michel Ney at the Battle of Krasnoi, which was forced to surrender to the Russians. Poncelet did not disclose any information when he was interrogated, and he was held as a prisoner of war in Saratov. During his imprisonment from 1812 to 1814 he wrote his treatise on projective geometry, which is considered to be the founding work of the modern subject. He published his *Traité des propriétés projectives des figures* [Poncelet, 1822] after he was released, including his closure theorem that is the subject of this thesis.

The theorem concerns pairs of conics (circles, ellipses, parabolas, hyperbolas) in the plane, and the existence of a fixed point of a certain geometric construction. Let C_1 and C_2 be two plane conics. Fix a point P_1 on C_1 which is not on C_2 and a tangent line ℓ_1 to C_2 passing through P_1 which is not tangent to C_1. Let P_2 be the point of intersection of ℓ_1 and C_1 other than P_1, and let ℓ_2 be the tangent line to C_2 through P_2 other than ℓ_1.

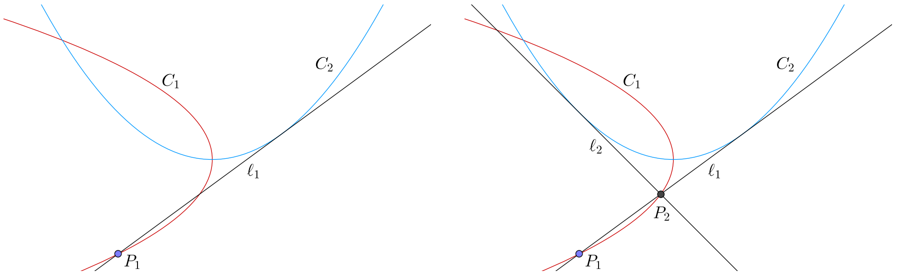


Figure 1: The construction of a Poncelet traverse.

Let P_3 be the point of intersection of ℓ_2 and C_1 other than P_2, let ℓ_3 be the tangent line to C_2 through P_3 other than ℓ_2, and so on. The figure consisting of the line segments between the points P_k is called the *Poncelet traverse* with initial point P_1 and tangent line ℓ_1. We say that it *closes* in k steps if $P_k = P_1$ and $\ell_k = \ell_1$ for some $k > 1$. The Poncelet traverse in figure 1 closes in four steps, yielding a triangle.

Theorem (Poncelet's closure theorem)**.** *If one Poncelet traverse closes in k steps, then every Poncelet traverse closes in k steps.*

In other words, the condition that a Poncelet traverse closes is independent of the initial point and tangent line; it depends only on the two conics. Throughout this thesis we understand an initial point to be one that is not on C_2 and an initial tangent line to be one that is not tangent to C_1, because if a Poncelet traverse would start there then it would close trivially.

The closure theorem admits an elegant modern proof using methods from algebraic geometry. Let X be the set of pairs (P, ℓ), where P is a point of C_1 and ℓ is a tangent line to C_2 passing through P. We define two maps $\sigma : X \to X$ and $\tau : X \to X$ as follows. For every pair $(P, \ell) \in X$, put $\sigma(P, \ell) = (P', \ell)$, where P' is the point of intersection of ℓ and C_1 other than P, and put $\tau(P, \ell) = (P, \ell')$, where ℓ' is the tangent line to C_2 passing through P other than ℓ. Note that σ and τ are involutions of X, i.e. they are their own inverses. We call their composition $\eta = \tau\sigma$. With the notation from the previous page, we have $\eta(P_1, \ell_1) = (P_2, \ell_2)$, and more generally $\eta^k(P_1, \ell_1) = (P_k, \ell_k)$. Hence we can rephrase the closure theorem in terms of the map $\eta : X \to X$.

Theorem (Poncelet's closure theorem)**.** *If there exists an integer $k > 1$ such that η^k has a fixed point which is not a fixed point of η, then η^k is the identity on X.*

It is this form of the theorem that admits an elegant algebro-geometric proof. Namely, it can be shown that the set X is a *variety* (the object studied in algebraic geometry) of such a particular kind that its involutions are very well understood. This understanding yields a swift proof of the closure theorem. The first proof of this kind was given by Griffiths and Harris [1977]. They used the theory of Riemann surfaces for the details of the proof.

In chapter 1 of this thesis we take a more explicit and algebraic approach. First we define *affine varieties* in section 1.1, which includes the conics that we are interested in, and we define *projective varieties* in section 1.2. Instead of showing that X is a variety, we construct a projective plane model M of X in section 1.3. We proceed in section 1.4 to introduce *morphisms* and *rational maps* between varieties. This allows us to define two birational maps $\sigma : M \dashrightarrow M$ and $\tau : M \dashrightarrow M$ in section 1.5 that are analogous to the maps of X with the same name. We call their composition $\eta = \tau\sigma$, and Poncelet's closure theorem is then restated in terms of the map $\eta : M \dashrightarrow M$. We go on in 1.6 to define the *dimension* of a variety, and we show that M has dimension 1, so M is a curve. In section 1.7 we define *nonsingularity* and we see that every projective curve is birational to a nonsingular curve, called its *nonsingular model.* In particular, M has a nonsingular model which we call E. We show that birational maps of M induce automorphisms of E, and hence Poncelet's closure theorem can be restated for the last time in terms of the automorphism $\eta : E \to E$. In section 1.8 we introduce the notion of a *divisor* on a nonsingular curve. This allows us to define the *genus* of a curve in section 1.9, and we show that E has genus 1. In section 1.10 we single out the curves of genus 1 with a given rational point on them, called *elliptic curves*, and it turns out that E is an elliptic curve. We show that elliptic curves have a natural additive group structure, and that every elliptic curve is isomorphic to one given by a *Weierstrass equation* such as $y^2 = x^3 + ax + b$. In section 1.11 we finally consider morphisms of elliptic curves. We find that the automorphism group $\operatorname{Aut}(E) = T_E \rtimes \operatorname{Aut}(E, O)$, and in particular every automorphism of E can be written uniquely as a product of a *translation* and an *isogeny*. We apply this to σ, τ and η to find that η is in fact a translation. Hence if η^k has a fixed point for some k, then η must be a translation by a point of finite order k, so η^k is the identity. This proves Poncelet's closure theorem.

In chapter 2 we explore a connection between Poncelet's closure theorem and dynamical billiards in ellipses. In particular, we apply Poncelet's closure theorem to a billiard table and we ask two interesting and difficult questions.

Chapter 1

The proof of Poncelet's closure theorem

In this chapter we give an algebro-geometric proof of the closure theorem. Our basic definitions concerning varieties are a combination of those of Hartshorne [1977] and Shafarevich [1994]. Throughout we do algebraic geometry over the field of complex numbers, which we deem sufficiently general for the task at hand. For the material on divisors and the genus we have consulted Fulton [2008], and the material on elliptic curves is based on that of Silverman [2009]. In order to make the thesis relatively self-contained we have included all the relevant definitions and theorems from algebraic geometry, although our treatment is brief and we have omitted some of the more technical proofs. The reader familiar with basic algebraic geometry will know which parts to skip.

1.1 Affine varieties

In this section we begin to set the stage for our proof of Poncelet's closure theorem. We introduce the first kind of varieties that we will meet (the affine ones), among which are the conics (circles, ellipses, parabolas, hyperbolas).

We define *affine n-space*, denoted $\mathbf{A}^n$, to be the set of all n-tuples of elements of $\mathbf{C}$, the complex numbers. We use the notation $\mathbf{A}^n$ instead of $\mathbf{C}^n$ to distinguish affine spaces from vector spaces, in which the origin and vector subspaces are special. By contrast, we shall encounter "subspaces" of $\mathbf{A}^n$ that do not include the origin, and these will be just as important as those that do. An element $P = (a_1, \dots, a_n) \in \mathbf{A}^n$ will be called a *point*, and the a_i will be called its *coordinates*. The closure theorem concerns the affine plane (2-space). In our pictures of $\mathbf{A}^2$ we shall draw only the points with real coordinates, for practical reasons.

Now, for the "subspaces" just mentioned, let $\mathbf{C}[x_1, \dots, x_n]$ be the polynomial ring in n variables over $\mathbf{C}$. The elements of $\mathbf{C}[x_1, \dots, x_n]$ can be interpreted as functions $\mathbf{A}^n \to \mathbf{C}$ in the obvious way. If $f \in \mathbf{C}[x_1, \dots, x_n]$ is a polynomial, then we can talk about the set of *zeros* of f, namely $Z(f) = \{P \in \mathbf{A}^n : f(P) = 0\}$. More generally, if T is any subset of $\mathbf{C}[x_1, \dots, x_n]$, we define the *zero set* of T to be the common zeros of all the elements of T, that is $Z(T) = \{P \in \mathbf{A}^n : f(P) = 0 \text{ for all } f \in T\}$.

Definition. A set $Y \subset \mathbf{A}^n$ is an *algebraic set* if there exists a subset $T \subset \mathbf{C}[x_1, \dots, x_n]$ such that $Y = Z(T)$.

In particular, the empty set $Z(1)$ and the whole space $Z(0)$ are algebraic.

Definition. We define the *Zariski topology* on $\mathbf{A}^n$ by declaring the complements of the algebraic sets to be open. It's easy to verify that this is indeed a topology.

A basis for the topology is given by the complements of zero sets of single polynomials. This follows from the fact that if $Y_\alpha = Z(T_\alpha)$ is any family of algebraic sets, then $\bigcap Y_\alpha = Z(\bigcup T_\alpha)$. Points are closed in this topology because for $P = (a_1, \ldots, a_n) \in \mathbf{A}^n$ we have $\{P\} = Z(x_1 - a_1, \ldots, x_n - a_n)$. However, the topology is not Hausdorff, i.e. any two distinct points need not have disjoint neighborhoods. To show this, it suffices to show that any two basic open subsets have a nonempty intersection. This is equivalent to the statement that any two basic closed proper subsets $Z(f)$ and $Z(g)$ have a union which is not all of $\mathbf{A}^n$. But $Z(f) \cup Z(g) = Z(fg)$, and $fg \neq 0$, so (because our base field is infinite) there is a point $P \in \mathbf{A}^n$ such that $(fg)(P) \neq 0$, and hence $P \not\in Z(fg)$.

Some algebraic sets consist of more than one part. For instance, the algebraic set $Z(xy)$ can be written as the union of $Z(x)$ and $Z(y)$.

Definition. A nonempty subset Y of a topological space is called *irreducible* if it cannot be written as the union $Y = Y_1 \cup Y_2$ of two proper closed subsets. The empty set is not irreducible.

Note that the proper closed subsets need not be disjoint, so we can say that a set is reducible if it can be covered by proper closed subsets. Every algebraic set $Y \subset \mathbf{A}^n$ can be written uniquely as a union $Y = Y_1 \cup \ldots \cup Y_r$ of irreducible algebraic subsets, no one containing another. The Y_i are called the *irreducible components* of Y. Now we can define the first type of object that we will be working with.

Definition. An *affine variety* is an irreducible Zariski-closed subset of $\mathbf{A}^n$ with the subspace topology. An open subset of an affine variety is a *quasi-affine variety*.

For any subset of $\mathbf{A}^n$, let us define an ideal of $\mathbf{C}[x_1, \ldots, x_n]$.

Definition. For $Y \subset \mathbf{A}^n$, the set $I(Y)$ of $f \in \mathbf{C}[x_1, \ldots, x_n]$ that vanish identically on Y is obviously an ideal, called the *ideal* of Y.

We say an algebraic set Y is *defined over the field $k \subset \mathbf{C}$* if its ideal $I(Y)$ is generated by polynomials in $k[x_1, \ldots, x_n]$. For example, the unit circle $Z(x^2 + y^2 - 1)$ is defined over $\mathbf{Q}$. A set of generators of $I(Y)$ is also called a set of *defining polynomials* of Y. Algebraic sets are related to certain ideals of $\mathbf{C}[x_1, \ldots, x_n]$.

Theorem 1.1.1. *There is a one-to-one inclusion-reversing correspondence between algebraic sets in $\mathbf{A}^n$ and radical ideals in $\mathbf{C}[x_1, \ldots, x_n]$, given by $Y \mapsto I(Y)$ and $\mathfrak{a} \mapsto Z(\mathfrak{a})$.*

Recall that the *radical* $\sqrt{\mathfrak{a}}$ of an ideal $\mathfrak{a}$ in a ring A consists of the elements $f \in A$ such that $f^n \in \mathfrak{a}$ for some $n > 0$. A *radical ideal* is an ideal which is its own radical. The theorem follows from Hilbert's Nullstellensatz (a result in commutative algebra), and some properties of the maps Z and I. Hilbert's Nullstellensatz states that $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$. For a proof, see Lang [2005, p. 380]. The fact that the correspondence is inclusion-reversing implies that maximal ideals in $\mathbf{C}[x_1, \ldots, x_n]$ correspond to points (the minimal algebraic sets) in $\mathbf{A}^n$.

Proposition 1.1.2. *An algebraic set $Y \subset \mathbf{A}^n$ is a variety if and only if $I(Y)$ is prime.*

PROOF. Suppose Y is irreducible. If $fg \in I(Y)$, then $Y \subset Z(fg) = Z(f) \cup Z(g)$. Thus $Y = (Y \cap Z(f)) \cup (Y \cap Z(g))$, both being closed subsets of Y. Since Y is irreducible, we have either $Y = Y \cap Z(f)$, in in which case $Y \subset Z(f)$, or $Y \subset Z(g)$. Hence either $f \in I(Y)$ or $g \in I(Y)$. Conversely, let $\mathfrak{p}$ be a prime ideal, and suppose that $Z(\mathfrak{p}) = Y_1 \cup Y_2$. Then $\mathfrak{p} = I(Y_1) \cap I(Y_2)$, so either $\mathfrak{p} = I(Y_1)$ or $\mathfrak{p} = I(Y_2)$. Thus $Z(\mathfrak{p}) = Y_1$ or Y_2, hence it is irreducible. □

In particular, $\mathbf{A}^n$ is irreducible because the zero ideal is prime. Another feature of the Zariski topology is that nonempty open sets are automatically dense. Indeed, if a nonempty open set U were not dense, then the proper closed subsets $\mathbf{A}^n \setminus U$ and $\overline{U}$ would cover $\mathbf{A}^n$, contradicting its irreducibility.

Recall that an irreducible polynomial is one that does not admit any nontrivial factorizations. Since $\mathbf{C}[x_1, \dots, x_n]$ is a unique factorization domain, an irreducible polynomial generates a prime ideal. Hence we have the following.

Corollary 1.1.3. *The zero set $Z(f)$ of an irreducible polynomial $f \in \mathbf{C}[x_1, \dots, x_n]$ is an affine variety.*

Such a variety defined by a single polynomial is sometimes called a *hypersurface*. A hypersurface in $\mathbf{A}^n$ has dimension (to be defined in section 1.6) $n-1$, just as a surface in $\mathbf{A}^3$ has dimension 2. In the case $n = 2$ the variety has dimension one, so it is more commonly called a curve. Almost all of the varieties considered in this thesis will be curves of this kind, defined by a single irreducible polynomial. For example, lines and *conics* are varieties in $\mathbf{A}^2$ given by the zero sets of irreducible polynomials of degree one and and two respectively. The irreducibility criterion excludes unions of lines such as $Z(xy) = Z(x) \cup Z(y)$ from the conics. What remains are the circles, ellipses, parabolas and hyperbolas, as intended.

1.2 Projective varieties

In this section we introduce projective varieties in a manner analogous to that of the previous section. In particular, we define the projective closure of an affine hypersurface. This will allow us to define the Poncelet variety in the next section.

We define *projective n-space*, denoted $\mathbf{P}^n$, to be the set of all lines through the origin in $\mathbf{A}^{n+1}$. The line through the point $(a_0, \dots, a_n) \in \mathbf{A}^{n+1}$ is denoted in *homogeneous coordinates* by $[a_0 : \dots : a_n]$, and is called a *point* in $\mathbf{P}^n$. If we let $\mathbf{C}^*$ denote the nonzero complex numbers, this same point may be denoted by $[\lambda a_0 : \dots \lambda a_n]$ for any $\lambda \in \mathbf{C}^*$, hence the name homogeneous coordinates. We might as well consider the lines to go through any other point than the origin in affine space. In this way the relevance of $\mathbf{P}^1$ to the closure theorem should be clear. Recall that a polynomial $f \in \mathbf{C}[x_0, \dots, x_n]$ is *homogeneous* of degree d if $f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n)$ for all $\lambda \in \mathbf{C}$. Analogously to the affine case, we can define the *zero set* of a collection of homogeneous polynomials in $\mathbf{C}[x_0, \dots, x_n]$. While homogeneous polynomials cannot be interpreted as functions $\mathbf{P}^n \to \mathbf{C}$, it's clear that their set of zeros is well-defined.

Definitions. A subset Y of $\mathbf{P}^n$ is an *algebraic set* if there exists a set T of homogeneous polynomials in $\mathbf{C}[x_0, \dots, x_n]$ such that $Y = Z(T)$. We define the *Zariski topology* on $\mathbf{P}^n$ by declaring the complements of the algebraic sets to be open. As in the affine case, it is easy to verify that this is indeed a topology.

Again, the complements of zero sets of single homogeneous polynomials form a basis for the topology. Points are closed, nonempty open sets are dense, and the topology is not Hausdorff. The definition of irreducibility from section 1.1 also applies here.

Definitions. A *projective variety* is an irreducible algebraic subset of $\mathbf{P}^n$ with the subspace topology. An open subset of a projective variety is a *quasi-projective variety*. If Y is any subset of $\mathbf{P}^n$, we define the *(homogeneous) ideal* of Y in $\mathbf{C}[x_0,\dots,x_n]$, denoted $I(Y)$, to be the ideal generated by the $f \in \mathbf{C}[x_0,\dots,x_n]$ such that f is homogeneous and f vanishes on Y. We say an algebraic set Y is *defined over the field* $k \subset \mathbf{C}$ if its ideal $I(Y)$ is generated by polynomials in $k[x_0,\dots,x_n]$.

The ideal in $\mathbf{C}[x_0,\dots,x_n]$ generated by the homogeneous elements of degree greater than zero is sometimes called the *irrelevant ideal* for the following reason.

Theorem 1.2.1. *There is a one-to-one inclusion-reversing correspondence between algebraic sets in* $\mathbf{P}^n$ *and homogeneous radical ideals in* $\mathbf{C}[x_0,\dots,x_n]$ *not equal to the irrelevant ideal.*

Here, a *homogeneous ideal* is an ideal that is generated by homogeneous elements. This is not the usual definition of a homogeneous ideal (which would take slightly more time to state precisely), but it is equivalent to it. For the usual definition, see Hartshorne [1977, I.2, p. 9].

Proposition 1.2.2. *An algebraic set* $Y \subset \mathbf{P}^n$ *is a variety if and only if* $I(Y)$ *is prime.*

The proof is analogous to that of theorem 1.1.2, although a lemma is needed stating that a homogeneous ideal $\mathfrak{a}$ is prime if and only if for any *homogeneous* polynomials $fg \in \mathfrak{a}$ implies $f \in \mathfrak{a}$ or $g \in \mathfrak{a}$. We also have the analogous corollary.

Corollary 1.2.3. *The zero set* $Z(f) \subset \mathbf{P}^n$ *of an irreducible homogeneous polynomial* $f \in \mathbf{C}[x_0,\dots,x_n]$ *of positive degree is a projective variety.*

Finally we consider embeddings of $\mathbf{A}^n$ in $\mathbf{P}^n$. For example, the map (of sets) from $\mathbf{A}^n$ to $\mathbf{P}^n$ given by $(a_1,\dots,a_n) \mapsto [a_1 : \dots : a_n : 1]$ is clearly an injection. We shall see later that it is indeed a morphism of varieties. Obviously we can also send the 1 to an other coordinate, so there are multiple ways to embed $\mathbf{A}^n$ in $\mathbf{P}^n$. We elect the embedding that sends the 1 to the last coordinate to be our *favorite* embedding for the rest of this thesis. The points outside the image of an embedding are called *points at infinity*. For example, if we embed $\mathbf{A}^1$ in $\mathbf{P}^1$ using $x \mapsto [x:1]$, then there is one point at infinity, namely $[1:0]$, which is sometimes denoted ∞. Upon embedding $\mathbf{A}^2$ in $\mathbf{P}^2$, we obtain a line at infinity.

Hypersurfaces in $\mathbf{A}^n$ are related to hypersurfaces in $\mathbf{P}^n$ in a natural way. Namely, let $Z(f)$ be a hypersurface in $\mathbf{A}^n$ for some irreducible polynomial $f \in \mathbf{C}[x_1,\dots,x_n]$.

Definition. The *homogenization* of $f \in \mathbf{C}[x_1,\dots,x_n]$ with $\deg f = d$ is given by the homogeneous polynomial $f^* = x_n^d f(x_0/x_n,\dots,x_{n-1}/x_n) \in \mathbf{C}[x_0,\dots,x_n]$. The *dehomogenization* of a homogeneous polynomial $f \in \mathbf{C}[x_0,\dots,x_n]$ of degree d is given by the polynomial $f_* = f(x_1,\dots,x_n,1) \in \mathbf{C}[x_1,\dots,x_n]$.

Clearly these two operations are each other's inverses. It can be shown that factoring a polynomial is the same as factoring its homogenization. See for instance Fulton [2008, 2.6, p. 24]. Hence f is irreducible if and only f^* is irreducible. This motivates the following definition.

Definition. The *projective closure* of a hypersurface $Y = Z(f) \subset \mathbf{A}^n$ is the hypersurface given by $\overline{Y} = Z(f^*) \subset \mathbf{P}^n$, where f^* is the homogenization of f.

The projective closure of an affine hypersurface is also called its *completion*. Note that no confusion arises in the notation, because we will never take the Zariski closure of a set that is already closed. Using our favorite embedding we have $\overline{Y} \cap \mathbf{A}^n = Z(f^*) \cap \mathbf{A}^n = Z(f) = Y$. Taking the projective closure adds points at infinity to the variety. More generally, the projective closure $\overline{Y}$ of an affine variety $Y \subset \mathbf{A}^n$ is the zero set of the ideal generated by the elements of $I(Y)$ homogenized. In general it is not true that if $f_1, \ldots, f_r$ generate $I(Y)$, then $f_1^*, \ldots, f_r^*$ generate $I(\overline{Y})$. Instead, one should compute a Gröbner basis for $I(Y)$ and then homogenize each polynomial in the Gröbner basis. In this case we also have $\overline{Y} \cap \mathbf{A}^n = Y$, so an affine variety is an open subset of its projective closure, which means that every affine variety is quasi-projective.

1.3 The Poncelet variety

In this section we define the variety M that is a projective plane model of the set X from the introduction. We compute M explicitly for one pair of conics, and find that this M is an elliptic curve. This motivates our proof strategy.

For the remainder of this thesis, let $C_1 = Z(f_1)$ and $C_2 = Z(f_2)$ be two fixed conics in $\mathbf{A}^2$. First we choose a rational parametrization of C_1, given by $t \mapsto P(t) = (x(t), y(t))$ where x and y are rational functions of (i.e. quotients of polynomials in) $t \in \mathbf{C}$. For example, the parabola $y = x^2$ in $\mathbf{A}^2$ is parametrized by $t \mapsto (t, t^2)$. In general, we can obtain a parametrization of C_1 as follows. Fix a point $P_0 = (x_0, y_0)$ on C_1. Define $P(t)$ to be the second point of intersection with the line of slope t through P_0. In this way, every point on C_1 is uniquely identified by some $t \in \mathbf{C}$, except P_0 and possibly the other point on the vertical line through P_0.

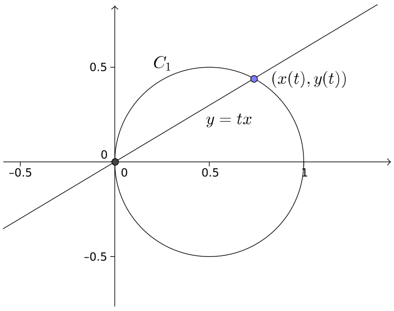


Figure 1.1: Rational parametrization of C_1.

More precisely, the line ℓ of slope t through P_0 is given by $y = t(x - x_0) + y_0$. Substituting this in f_1 yields $f_1(x, t(x-x_0)+y_0) = A(t)x^2 + B(t)x + C(t)$, of which one root is x_0. If $A(t) \neq 0$, then this is a quadratic and the other root is $x(t) = -x_0 - B(t)/A(t)$. For these t, we define $y(t) = t(x(t) - x_0) + y_0$, and then $P(t)$ is the other point of intersection of ℓ with C_1. If we write $f_1 = ay^2 + bxy + cx^2 + r(x, y)$, then $A(t) = at^2 + bt + c$. The zeros of $A(t)$ are precisely the $t \in \mathbf{C}$ where the parametrization is not defined. These are also the poles of the rational functions $x(t)$ and $y(t)$. There can be zero, one or two of these.

Example 1.3.1. Suppose $C_1 = Z(x^2 + y^2 - 1)$, and let $P_0 = (-1,0)$. The line ℓ with slope t through P is given by $y = t(x+1)$. Computing $x(t)$ amounts to finding the solution of $0 = x^2 + t^2(x+1)^2 - 1 = (1+t^2)x^2 + 2t^2x^2 + t^2 - 1$ other than $x_0 = -1$. This is $x(t) = (1-t^2)/(1+t^2)$, and hence $y(t) = t(x(t)+1) = 2t/(1+t^2)$. The poles of these are i and $-i$.

The poles of the parametrization will play a role later on. Equipped with a parametrization of C_1, we now define the Poncelet variety. What does it mean for a line $y = ax + b$ through a point $P(t) \in C_1$ (not on the vertical line through P_0) to be tangent to C_2? Note that we can write $b = y(t) - ax(t)$. The condition for the line ℓ to be tangent to C_2 is exactly that $f_2(x, ax+b) = 0$ has only one solution. This happens if and only if the discriminant of $f_2(x, ax+b) = Q(t,a)x^2 + R(t,a)x + S(t,a)$ is zero. The coefficients can be seen to be functions of t and a by using the expression for b. We define $m(t,a)$ to be the numerator of the discriminant $R(t,a)^2 - 4Q(t,a)S(t,a)$. Hence $m \in \mathbf{C}[t,a]$ is a polynomial.

Assumption. The polynomial $m(t,a)$ is irreducible.

We have not investigated any sufficient conditions for this to be true, but it is the case for many interesting examples. Carrying out the above construction for the most general of conics, we find that $m(t,a)$ always has degree 2 in a and degree at most 4 in t. Among the zeros of m are the (most interesting) pairs (t,a) for which $P(t)$ is a point of C_1, and the line $y = ax + b$ (with b defined in terms of t and a, as above) through $P(t)$ is tangent to C_2. Hence the zero set of m is at least very similar to the set X described in the introduction. The pairs (t,a) play a role similar to the pairs (P,ℓ). Note that because we have taken the denominator of the discriminant, some zeros (t,a) of m may be such that $t \in \mathbf{C}$ does not define a point of C_1, i.e. t is a pole of the parametrization. Also, the vertical tangent lines to C_2 are excluded by construction. The number of such defects is finite, and they will not give us much trouble. We need to make one more assumption about m for the likeness of its zero set to X to be more than superficial.

Assumption. For every $(t,a) \in Z(m)$ there exists at most one other $(t',a) \in Z(m)$ such that $P(t')$ is the other point of C_1 on the line $y = ax + b$.

With these assumptions out of the way, we can give our fundamental definition.

Definition. The *Poncelet variety* $M \subset \mathbf{P}^2$ is the projective closure of $Z(m) \subset \mathbf{A}^2$, where $m \in \mathbf{C}[t,a]$ is defined as above.

The projective closure is taken for the following reason.

Example 1.3.2. Let $C_1 = Z(x - \lambda y^2)$ where $\lambda \in \mathbf{C}^*$ is a parameter and $C_2 = Z(y - x^2)$. We parametrize C_1 by $t \mapsto (\lambda t^2, t)$. We compute $f_2(x, ax+b) = ax + b - x^2 = ax + y(t) - ax(t) - x^2 = -x^2 + ax + t - \lambda a t^2$. The discriminant is $m(t,a) = a^2 + 4(t - \lambda a t^2) = a^2 + 4t - 4\lambda a t^2$. The Poncelet variety is then the projective closure of $t = \lambda a t^2 - a^2/4$. Let us make the change of coordinates $\xi = a, \eta = at$. Multiplying the original defining polynomial by a, we obtain $\lambda\eta^2 - \eta = \xi^3/4$. Multiplying by 4λ yields $(2\lambda\eta - 1)^2 = \lambda\xi^3 + 1$. Multiplying by λ^2 gives $(2\lambda^2\eta - \lambda)^2 = (\lambda\xi)^3 + \lambda^2$. Finally, changing coordinates to $Y = 2\lambda^2\eta - \lambda$ and $X = \lambda\xi$, this is $Y^2 = X^3 + \lambda^2$. The reader may recognize this as the equation for an *elliptic curve*. These elliptic curves are properly considered as projective curves, by taking the projective closure. Elliptic curves have a natural group structure (see section 1.10).

This example motivates our proof strategy. We will show that the Poncelet variety M is a curve, and that it can always be transformed into an elliptic curve E (albeit using more complicated transformations). We then use the group structure of E to conclude the theorem.

1.4 Morphisms and rational maps

In this section we define morphisms and rational maps between varieties. Roughly speaking, these are maps that can be defined by polynomials or rational functions. The two maps of the Poncelet variety in the next section that are instrumental to our proof will be of this kind. We also define the function field of a variety, which will allow us to define dimension later on.

Definitions. A function $f : Y \to \mathbf{C}$ on a quasi-affine variety $Y \subset \mathbf{A}^n$ is called *regular at the point* P if there is an open neighborhood U of P such that $f = g/h$ on U for some $g, h \in \mathbf{C}[x_1, \dots, x_n]$, where h does not vanish on U. A function $f : Y \to \mathbf{C}$ on a quasi-projective variety $Y \subset \mathbf{P}^n$ is called *regular at the point* P if there is a neighborhood U of P such that $f = g/h$ on U for some homogeneous polynomials $g, h \in \mathbf{C}[x_0, \dots, x_n]$ of the same degree, where h does not vanish on U. We say that f is *regular on* Y if it is regular at every point of Y.

Regular functions are continuous in the Zariski topology. This follows easily from the fact that the Zariski-closed subsets of $\mathbf{C} = \mathbf{A}^1$ are finite, and the fact that a subset Z of a topological space Y is closed if and only if Y has an open cover of sets U such that $Z \cap U$ is closed in U for each U. Now we can define the category of varieties.

Definition. A *variety* is any affine, quasi-affine, projective, or quasi-projective variety as previously defined. A map $\varphi : X \to Y$ of varieties is called a *morphism* if it is continuous and for every open $U \subset W$ and every regular function f on U we have that $f\varphi$ is regular on $\varphi^{-1}(U)$.

Clearly the composition of two morphisms is a morphism, so we have a category. A morphism of varieties is sometimes called a *regular map*. The identity morphism $Y \to Y$ is denoted id_Y. An *isomorphism* between X and Y is a one-to-one morphism φ of X onto Y such that φ^{-1} is a morphism. An isomorphism $Y \to Y$ is called an *automorphism* of Y. The automorphisms of a variety Y form a group under composition, which we denote by $\mathrm{Aut}(Y)$. We associate a field with every variety.

Definition. If Y is a variety, we define the *function field* $k(Y)$ of Y as follows: an element of $k(Y)$ is an equivalence class of regular functions $U \to \mathbf{C}$, where U is a nonempty open subset of Y, and where two regular functions $f : U \mapsto \mathbf{C}$ and $g : W \mapsto \mathbf{C}$ are equivalent if $f = g$ on $U \cap W$. The elements of $k(Y)$ are called *rational functions* on Y.

If $Y \subset \mathbf{A}^n$ is an affine variety, then $k(Y)$ is isomorphic to the fraction field of the *coordinate ring* $A(Y) = \mathbf{C}[x_1, \dots, x_n]/I(Y)$, which is an integral domain. The fact that $A(Y)$ is an integral domain follows from theorem 1.1.2 (ideals of varieties are prime). If two polynomials $f, g \in \mathbf{C}[x_1, \dots, x_n]$ define the same function $Y \to \mathbf{C}$, then their difference $f - g$ belongs to the ideal $I(Y)$. Hence the elements of $A(Y)$ can be interpreted as polynomial functions $Y \to C$. The function field of a projective variety $Y \subset \mathbf{P}^n$ is isomorphic to the function field of $Y \cap \mathbf{A}^n$ for some embedding of $\mathbf{A}^n$ in $\mathbf{P}^n$ with $Y \cap \mathbf{A}^n \neq \emptyset$. This follows from the fact that a rational function is uniquely determined by its values on a nonempty open set (because nonempty open sets are dense). We will characterize the function field of the Poncelet variety in proposition 1.7.4. Morphisms into affine varieties are characterized by the following lemma.

Lemma 1.4.1. *Let X be any variety, and let $Y \subset \mathbf{A}^n$ be an affine variety. A map $\psi : X \to Y$ is a morphism if and only if $x_i\psi$ is a regular function on X for each i, where the x_i are the coordinate functions on $\mathbf{A}^n$.*

For a proof, see Hartshorne [1977, lemma I.3.6, p. 20]. The next lemma characterizes an important subclass of the morphisms between quasi-projective varieties.

Lemma 1.4.2. *Let $X \subset \mathbf{P}^n$ and $Y \subset \mathbf{P}^m$ be quasi-projective varieties. A map $\varphi : X \to Y$ given by $\varphi([x_0 : \ldots : x_n]) = [\varphi_0([x_0 : \ldots : x_n]) : \ldots : \varphi_m([x_0 : \ldots : x_n])]$, where the $\varphi_i \in \mathbf{C}[x_0, \ldots, x_n]$ are homogeneous of the same degree and don't vanish simultaneously at any point of X, is a morphism.*

These lemmas will help us define maps of the Poncelet variety in the next section. For now, they give a good impression of what morphisms usually look like. The following lemma tells us more about morphisms.

Lemma 1.4.3. *Let $\varphi : X \to Y$ and $\psi : X \to Y$ be two morphisms that agree on an open set $U \subset X$. Then $\varphi = \psi$.*

This is also proven in Hartshorne [1977, lemma I.4.1, p. 24]. The lemma motivates the following definition.

Definition. A *rational map* $\varphi : X \dashrightarrow Y$ is an equivalence class of morphisms $U \to Y$ from an open subset $U \subset X$ to Y, where two morphisms $U_1 \to Y$, $U_2 \to Y$ are equivalent if they agree on $U_1 \cap U_2$. The rational map φ is *dominant* if some (and hence every) $U \to Y$ has its image dense in Y.

The lemma implies that the relation just described is an equivalence relation. In general, a rational map is not a function from X to Y, hence the dashed arrow. The meromorphic functions in complex analysis have a similar status. If $\varphi : X \to Y$ is a rational map defined by a collection of morphisms $U_\alpha \to Y$, then the *domain* of φ is defined to be $\operatorname{dom}\varphi = \bigcup_\alpha U_\alpha$. We say that φ is *defined* at the points of $\operatorname{dom}\varphi$. Composing rational maps in general is problematic, because it may happen that the image of the domain of one does not intersect the domain of another. However, one can compose dominant rational maps, so we can consider the category of varieties and dominant rational maps. An isomorphism in this category is called a birational map:

Definitions. A dominant rational map $X \dashrightarrow Y$ is called *birational* if it has an inverse dominant birational map. In this case we say that X and Y are *birationally equivalent.*

It is clear that two varieties are birationally equivalent if and only if they have isomorphic open subsets. We also have the following result.

Theorem 1.4.1. *Two varieties X and Y are birationally equivalent if and only if their function fields are isomorphic as extension fields of $k = \mathbf{C}$.*

For a proof, see Hartshorne [1977, corollary I.4.5, p. 26]. From this theorem it is particularly clear that birational equivalence is an equivalence relation. We will show later (in section 1.7) that the Poncelet variety is birational to a nonsingular variety E. In the next section we define two birational maps $\sigma : M \dashrightarrow M$ and $\tau : M \dashrightarrow M$ of the Poncelet variety. For this we use the following easy lemma.

Lemma 1.4.4. *A birational map $Y \dashrightarrow Y$ of an affine variety Y can be uniquely extended to a birational map $\overline{Y} \dashrightarrow \overline{Y}$ of its projective closure.*

Proof. The birational map is represented by an isomorphism φ from an open dense subset $U \subset Y$ to another dense open subset $\varphi(Y)$. Under the standard embedding, both U and $\varphi(U)$ are dense in $\overline{Y}$. Hence φ also represents a birational map $\overline{Y} \to \overline{Y}$. □

We shall call such an induced birational map by the same name as the original. There is no harm in this, as the induced birational map agrees with the original on the affine chart.

1.5 Maps of the Poncelet variety

In this section we introduce two birational maps $\sigma : M \dashrightarrow M$ and $\tau : M \dashrightarrow M$ of the Poncelet variety that correspond to the maps of X from the introduction. We restate the closure theorem in terms of these maps.

Let $P = (x(t), y(t))$ be a point of C_1 and let a be the slope of a tangent line ℓ through P. Let $P' = (x', y')$ be the other point of intersection of ℓ with C_1. We seek t' such that $x(t') = x'$ and $y(t') = y'$. We know that x' is precisely the other root of the quadratic $f_1(x, ax + b) = Q(t, a)x^2 + R(t, a)x + S(t, a)$ besides $x(t)$, where again we have used the fact that $b = y(t) - ax(t)$. Hence $x' = -x(t) - R(t, a)/Q(t, a)$. The corresponding y-coordinate is $y' = ax' + b$. Now we can let t' be the parameter such that $x(t') = x'$ and $y(t') = y'$. For our general parametrization by lines of slope t through a point $P_0 = (x_0, y_0) \in C_1$, this is $t' = (y' - y_0)/(x' - x_0)$. In the case that m is quadratic in t, say $m(t, a) = Q(a)t^2 + R(a)t + S(a)$, we simply have $t' = -t - R(a)/Q(a)$. In any case, this gives a birational map $\sigma : Z(m) \dashrightarrow Z(m)$ defined by $(t, a) \mapsto (t', a)$. The fact that σ is a rational map follows from lemma 1.4.1, and it is birational because it is its own inverse as a rational map.

Let ℓ' be the other tangent line to C_2 through P, with slope a'. Since m is always quadratic in a, say $m(t, a) = Q(t)a^2 + R(t)a + S(t)$, we can simply put $a' = -a - R(t)/Q(t)$. This gives a birational map $\sigma : Z(m) \to Z(m)$ defined by $(t, a) \mapsto (t, a')$.

Definitions. The maps $\sigma : M \dashrightarrow M$ and $\tau : M \dashrightarrow M$ are the birational maps that are uniquely determined (lemma 1.4.4) by the birational maps

$$\sigma(t, a) = (t', a) \qquad \text{and} \qquad \tau(t, a) = (t, a')$$

of $Z(m)$. We call their composition $\eta = \tau\sigma$.

These maps correspond to the maps of X from the introduction. Note that the maps σ and τ have fixed points and are not the identity on M. We will make great use of this later. To be explicit, we restate Poncelet's closure theorem in terms of $\eta : M \dashrightarrow M$.

Theorem 1.5.1 (Poncelet's closure theorem)**.** *If there exists an integer $k > 1$ such that η^k has a fixed point that is not a fixed point of η, then η^k is the identity on M.*

For concreteness, we compute σ and τ for some example.

Example 1.5.2. Let M be the Poncelet variety from example 1.3.2, i.e. M is the projective closure of $t = \lambda a t^2 - a^2/4$. Since $m(t,a) = \lambda a t^2 - t - a^2/4$ is quadratic in both t and a, the maps σ and τ of $Z(m)$ are simply the maps that permute the roots of m. That is, $\sigma(t,a) = (\frac{1}{\lambda a} - t, a)$ and $\tau(t,a) = (t, 4\lambda t^2 - a)$. The coordinate transformation $X = \lambda a$, $Y = 2\lambda^2 at - \lambda$ shows that M is the elliptic curve $Y^2 = X^3 + \lambda^2$. We compute the maps σ and τ in these new coordinates. We use the inverse coordinate transformation $a = X/\lambda$, $t = \frac{Y+\lambda}{2\lambda X}$ to find

$$\sigma(X,Y) = (X,-Y) \qquad \text{and} \qquad \tau(X,Y) = (\left(\frac{Y+\lambda}{X}\right)^2 - X, \left(\frac{Y+\lambda}{X}\right)^3 - Y - 2\lambda).$$

Hence

$$\eta(X,Y) = (\left(\frac{\lambda - Y}{X}\right)^2 - X, \left(\frac{\lambda - Y}{X}\right)^3 + Y - 2\lambda).$$

Using incredible foresight, one might recognize this as the map $P \mapsto P + [0:\lambda:1]$ of the elliptic curve, where the plus sign denotes addition in the elliptic curve group. One can show that that $[0:\lambda:1]$ has order 3 in the elliptic curve group, and hence η^3 is the identity. This proves Poncelet's closure theorem for every pair of conics of the form in example 1.3.2, i.e. $C_1 = Z(x - \lambda y^2)$ and $C_2 = Z(y - x^2)$.

The rest of the thesis is devoted to generalizing the above example. We will show that M is always a curve in the next section. Then we show that M can be transformed into an elliptic curve E. The birational maps σ and τ induce automorphisms of E. We use the structure of $\mathrm{Aut}(E)$ to conclude the theorem.

1.6 Dimension

In this section we define the dimension of affine and projective varieties. We find that the Poncelet variety has dimension 1, so it is a curve.

We will define the dimension of a variety Y in terms of its function field $k(Y)$. For this we first recall some basic facts about field extensions. A field extension K over k is called *algebraic* if each element of K is a root of some non-zero polynomial with coefficients in k. A subset S of K is a *transcendence basis* of K over k if it is algebraically independent over k (the elements do not satisfy any non-trivial polynomial relation with coefficients in k) and K is algebraic over $k(S)$, the field obtained by adjoining the elements of S to k. Any two transcendence bases for a field extension have the same cardinality [Lang, 2005, theorem VIII.1.1, p. 356]. The *transcendence degree* of a field extension K over k is the cardinality of a transcendence basis for K over k.

Definition. The *dimension* of a variety Y, denoted $\dim Y$, is the transcendence degree of its function field $k(Y)$ over the ground field $k = \mathbf{C}$.

In particular, dimension is invariant under birational maps, by theorem 1.4.1. Obviously $\mathbf{A}^n$ has dimension n, as its function field is the field of rational functions in n algebraically independent variables. A variety of dimension 1 is called a *curve*. In particular, $\mathbf{A}^1 = \mathbf{C}$ is a curve, in contrast to the usual interpretation of $\mathbf{C}$ as a plane. Curves in $\mathbf{A}^2$ and $\mathbf{P}^2$ are called *plane curves*.

Proposition 1.6.1. *A hypersurface in $\mathbf{A}^n$ or $\mathbf{P}^n$ has dimension $n-1$.*

PROOF. Because the function field of a projective variety is the same as the function field of an affine open subset, we can reduce to the affine case. Let $H = Z(f) \subset \mathbf{A}^n$ be a hypersurface, with $f \in \mathbf{C}[x_1,\dots,x_n]$. The coordinate ring of H is $\mathbf{C}[x_1,\dots,x_n]/(f)$, which is generated by the $X_i = x_i + (f)$ satisfying $f(X_1,\dots,X_n) = 0$. Through the canonical embedding of the coordinate ring in its fraction field (i.e. the function field of H), the X_i can be considered elements of $k(H)$. Without loss of generality, suppose that x_n occurs in f in some way. Then $X_1,\dots,X_{n-1}$ are algebraically independent over $\mathbf{C}$. But then $k(H)$ is algebraic over $\mathbf{C}(X_1,\dots,X_{n-1})$, because X_n is a root of $f(X_1,\dots,X_{n-1},X) \in \mathbf{C}[X_1,\dots,X_{n-1}][X]$. This means that the $X_1,\dots,X_{n-1}$ form a transcendence basis of $k(H)$, so H has dimension $n-1$. □

In particular, hypersurfaces in $\mathbf{A}^2$ and $\mathbf{P}^2$ are curves.

Corollary 1.6.2. *The Poncelet variety $M \subset \mathbf{P}^2$ is a curve.*

For a reducible algebraic set Y, we define the dimension of Y to be the maximum of the dimensions of its irreducible components. The next two results will be helpful in the next section.

Proposition 1.6.3. *If Y is a variety and $X \subset Y$ is a proper algebraic subset of Y, then* $\dim X < \dim Y$.

Proposition 1.6.4. *An algebraic set Y of dimension zero is finite.*

PROOF. Because every algebraic set is a finite union of varieties, and the dimension of a projective variety can be computed in terms of the dimension of an affine variety, it suffices to show this for a variety Y in $\mathbf{A}^n$. If $\dim Y = 0$, then $k(Y)$ has transcendence degree zero over $\mathbf{C}$ and hence is algebraic over $\mathbf{C}$. But $\mathbf{C}$ is algebraically closed, so $k(Y) = \mathbf{C}$. From the inclusions $\mathbf{C} \subset A(Y) \subset k(Y) = \mathbf{C}$ we see that $A(Y) = \mathbf{C}$. Hence $I(Y) \subset \mathbf{C}[x_1,\dots,x_n]$ is an ideal such that $\mathbf{C}[x_1,\dots,x_n]/I(Y) = \mathbf{C}$. This means that $I(Y)$ is maximal, so Y is a point. □

For the remainder of this thesis we concern ourselves with the rich theory of curves. We define singularities on curves, the genus of a curve, and then we single out the curves of genus 1 with a rational point on them, called *elliptic curves.*

1.7 Singularities

In this section we define singularities that curves may have. We show that a curve has only finitely many singular points, and we describe a method to find these points. We see that every curve is birational to a nonsingular curve. In particular, the Poncelet variety has a nonsingular model. We show that the birational maps defined on the Poncelet variety induce automorphisms of its nonsingular model. We restate the closure theorem in terms of these automorphisms.

It will turn out that singularities can be analyzed locally, so we treat the affine case first and reduce the projective case to it later. For the rest of this section, let $C = Z(f) \subset \mathbf{A}^2$ be a curve. We borrow a definition from differential geometry.

Definitions. A point $P = (a_1,\dots,a_n) \in C$ is *nonsingular* if the partial derivatives $\partial f/\partial x_i$ don't vanish simultaneously at P. In this case the line $\sum_i f_{x_i}(P)(x_i - a_i) = 0$ is called the *tangent line* to C at P. A point that isn't nonsingular is called *singular,* or a *singularity.* The set of singular points of C is denoted $\operatorname{Sing} C$. A curve without singular points is called a *nonsingular curve.*

More generally, a point on a variety $Y \subset \mathbf{A}^n$ is said to be nonsingular if the Jacobian matrix of the generators of $I(Y)$ has rank $n - \dim Y$. From the definition it should be clear that a nonsingular curve is also a complex manifold. It is entirely possible to apply the theory of complex manifolds to nonsingular varieties, but we do not pursue this. Nonsingularity may also be defined algebraically and more intrinsically in terms of local rings, but we shall find the Jacobian criterion to be most practical for our purposes. The following theorem is fundamental.

Proposition 1.7.1. Sing$C$ *is a finite set.*

PROOF. If Sing$C = C$, then the functions $\partial f/\partial x_i$ are zero on C, and hence $\partial f/\partial x_i \in I(C)$ for each i. But $I(C)$ is the principal ideal generated by f, and $\deg(\partial f/\partial x_i) < \deg f$ for each i, so we must have $\partial f/\partial x_i = 0$ for each i. This is a contradiction, and hence Sing$C$ is a proper subset of C. Certainly Sing$C$ is closed, so it has dimension zero by proposition 1.6.3, and hence Sing$C$ is finite by proposition 1.6.4. □

Now that we know the number of singularities is finite, we begin to investigate them. This is particularly doable case of a planar curve.

Definitions. Write $f = f_0 + \ldots + f_d$, where f_i is homogeneous of degree i. The *multiplicity* of $P = (0,0)$ on C, denoted $\mu_P(C)$, is the least r such that $f_r \neq 0$. We can write $f_r = \prod L_i^{r_i}$, where the $L_i = \alpha_i x + \beta_i y$ are distinct lines. The L_i are called the *tangent lines* to C at P and r_i is the *multiplicity* of the tangent L_i. If C has $\mu_P(C)$ distinct tangents at P, then P is called an *ordinary* singularity.

The hypothesis $n = 2$ is used in the factorization of f_r. The homogeneous polynomial in two variables $f_r(x, y)$ can be factored into a product of lines by first writing $f_r = y^k g$ where y doesn't divide g, dehomogenizing and factoring in $\mathbf{C}[x]$ like $f_{r*} = g_* = c\prod(x - \xi_i)$, and then homogenizing to obtain $f_r = cy^k \prod(x - \xi_i y)$. These definitions can be extended to a point $P \neq (0,0)$ by performing the appropriate translation. For projective curves, we define a point to be singular if it is singular in an affine chart. Equivalently, a point P of a projective curve $Z(f) \subset \mathbf{P}^n$ is nonsingular if the partial derivatives $\partial f/\partial x_i$ don't vanish simultaneously at P. The Poncelet variety $M \subset \mathbf{P}^2$ may be singular.

Example 1.7.2. Let $C_1 = Z(x^2 + y^2 - 1)$ be the unit circle and $C_2 = Z(3x^2 - 4y^2 - 12)$ a hyperbola. Parametrize C_1 by $x(t) = (1 - t^2)/(1 + t^2)$ and $y(t) = 2t/(1 + t^2)$. Our general construction from section 1.3 yields $m(t, a) = 3t^4 - 3a^2t^4 - 10a^2t^2 + 4at^3 - 3a^2 - 4at + 10t^2 + 3$. Hence $M = Z(m^*) \subset \mathbf{P}^2$, and we let t, a, s be homogeneous coordinates in $\mathbf{P}^2$. First we check for singularities in the affine chart $s \neq 0$. This amounts to solving the system of polynomial equations $m(t, a) = \frac{\partial m}{\partial t}(t, a) = \frac{\partial m}{\partial a}(t, a) = 0$. To do this we use the standard method of computing a Gröbner basis for the ideal of $\mathbf{C}[t, a]$ generated by $m(t, a)$, $\frac{\partial m}{\partial t}(t, a)$, and $\frac{\partial m}{\partial a}(t, a)$ in lexicographic order and solving the system of equations obtained by equating the elements of the basis to zero successively. The Gröbner basis turns out to be $t - a$, $a^2 + 1$. Hence the singular points in the affine chart $s \neq 0$ are (i, i) and $(-i, -i)$. Next we check for singularities in the affine chart $a \neq 0$. For this we compute a Gröbner basis for the ideal of $\mathbf{C}[t, s]$ generated by $m^*(t, 1, s)$ and its derivatives with respect to t and s. This yields the singularities $(0, 0)$, $(1, i)$ and $(1, -i)$ in the affine chart $a \neq 0$. However, these last two points $[1 : 1 : i] = [-i : -i : 1]$ and $[1 : 1 : -i] = [i : i : 1]$ were already found in the previous chart. Next we check for singularities in the affine chart $t \neq 0$. For this we compute a Gröbner basis for the ideal of $\mathbf{C}[a, s]$ generated by $m^*(1, a, s)$ and its derivatives with respect to a and s. This basis is $a+s^2$, $s(s^2+1)$. Hence the singular points are $(0,0)$, $(1,i)$ and $(1,-i)$ in the affine chart $t \neq 0$. Again, these last two points were already found in the first chart. In summary, the singular points of M are $[i:i:1]$, $[-i:-i:1]$, $[0:1:0]$ and $[1:0:0]$. We investigate the nature of the singular point $[0:1:0]$, which already has coordinates $(0,0)$ in the affine chart $a \neq 0$. We have $m^*(t,1,s) = 3s^6+10s^4t^2+3s^2t^4-4s^4t+4s^2t^3-3s^4-10s^2t^2-3t^4$. The term of lowest homogeneous degree is $m_4 = -3s^4-10s^2t^2-3t^4$, and hence $[0:1:0]$ is a singularity of multiplicity four. Since $m_4(t,1)$ has four distinct roots, the singularity is ordinary. Similarly, the other three points can be found to be ordinary of multiplicity 2.

The singularities of the Poncelet variety will play a role in section 1.9, where we compute the genus of the Poncelet variety. We have the following theorem about projective curves.

Theorem 1.7.3. *For every projective curve $C \subset \mathbf{P}^n$ there exists an m and a nonsingular curve $C' \subset \mathbf{P}^m$ such that C is birational to C'.*

This is theorem 7.5.3 in Fulton [2008]. The nonsingular curve C' in theorem 1.7.3 is called a *nonsingular model* or *desingularization* or *normalization* of the original curve C (or its function field). In particular, the Poncelet variety M has a nonsingular model which we call E. Note that a nonsingular model of a plane curve need not (and in fact cannot in some cases) be planar. In example 1.3.2 the Poncelet variety was already nonsingular, so $E = M$. We can give a useful description of the nonsingular model of the Poncelet variety.

Proposition 1.7.4. *The function field of the Poncelet variety M can be written $\mathbf{C}(t,z)$ where $z^2 = h(t)$, h is without square factor and $\deg h \leq 4$. There exists a nonsingular model of M such that $z^2 = h(t)$ in an affine chart.*

Proof. Let $m(t,a) = m_2a^2+m_1a+m_0 = 0$ with $m_i \in \mathbf{C}[t]$. We have $(2m_2a+m_1)^2+(4m_2m_0-m_1^2) = 0$. Introduce $y = 2m_2a+m_1$ and $m_1^2-4m_2m_0 = g^2h$ with $g,h \in \mathbf{C}[t]$ and h without square factor. Then we have $y^2 = g^2h$, and by introducing $z = y/g$ we obtain the equation $z^2 = h(t)$. Clearly $\mathbf{C}(t,a) = \mathbf{C}(t,z)$. The fact that h has degree at most 4 is derived as follows. Suppose $x(t) = A/B$ and $y(t) = C/D$ for some $A,B,C,D \in \mathbf{C}[t]$ with $\gcd(A,B) = \gcd(C,D) = 1$. Put $E = \gcd(B,D)$ and write $x(t) = A'/E$ and $y(t) = C'/E$ for $A',C' \in \mathbf{C}[t]$. Then $b = y(t)-ax(t) = F/E$ where $F = C'-aA'$. Let $f_2 = b_{00}+b_{01}x+b_{02}x^2+b_{11}xy+b_{10}y+b_{20}y^2$. Then $f_2(x,ax+b) = m(t,a)/E^2$ and $\gcd(m,E) = 1$. By writing out $m(t,a)$ in terms of F and E, we find that m_1 has E as a factor and m_0 has E^2 as a factor. Hence $m_1^2-4m_2m_0$ has E^2 as a factor. What remains after factoring out E^2 has degree at most 2 in E, and hence degree at most 4 in t. For the proof that there exists a nonsingular model of M such that $z^2 = h(t)$ in an affine chart, see Silverman [2009, example II.2.5.1, p. 22]. □

Note that the proof above is constructive. Given the equation $m(t,a) = 0$ of a Poncelet variety, we can compute $h(t)$ to obtain the simple description $z^2 = h(t)$ of its function field.

Example 1.7.5. Let $M \subset \mathbf{P}^2$ be the Poncelet variety from example 1.7.2, defined by $m(t,a) = -(3t^4+10t^2+3)a^2+4(t^3-t)a+3t^4+10t^2+3$. Write $m(t,a) = m_2a^2+m_1a+m_0$ with $m_i \in \mathbf{C}[t]$. Then $m_1^2-4m_2m_0 = 4(t^2+1)^2(9t^4+46t^2+9)$, and hence $h(t) = 9t^4+46t^2+9$. Thus the function field of M can be written $\mathbf{C}(t,z)$ where $z^2 = 9t^4+46t^2+9$.

Note that a rational map from a curve induces a rational map of its nonsingular model. A fundamental result about smooth projective curves is that rational maps are defined at every point.

Proposition 1.7.6. *A rational map $C \dashrightarrow Y$ from a smooth projective curve C to a projective variety Y is a morphism $C \to Y$.*

For a proof, see Silverman [2009, II.2.1, p. 19].

Corollary 1.7.7. *A birational map $C \dashrightarrow C'$ between smooth projective curves C and C' is an isomorphism $C \to C'$.*

It follows from corollary 1.7.7 that the nonsingular model of theorem 1.7.3 is unique up to isomorphism. Since birational maps of M induce birational maps of E, the induced maps $\sigma : E \to E$ and $\tau : E \to E$ are automorphisms of E. To be explicit, we restate Poncelet's closure theorem for the last time in terms of $\eta : E \to E$.

Theorem 1.7.8 (Poncelet's closure theorem)**.** *If there exists an integer $k > 1$ such that η^k has a fixed point which is not a fixed point of η, then $\eta^k = \mathrm{id}_E$.*

In fact we shall see that the induced map $\eta : E \to E$ itself has no fixed points, even if $\eta : M \dashrightarrow M$ does. This was already the case in example 1.5.2.

1.8 Divisors on curves

In this section we define divisors on nonsingular curves. This will allow us to define the genus of a curve in the next section.

Throughout this section C will denote a nonsingular projective curve. We give a brief overview of the theory of divisors that we will be needing.

Definition. The *divisor group* $\mathrm{Div}(C)$ is the free abelian group on the points of C.

An element of $\mathrm{Div}(C)$ is a formal finite sum of points $D = \sum_n d_n P_n$ (with $d_n \in \mathbf{Z}$), called a *divisor*. More generally, *Weil divisors* are formal sums of codimension 1 subvarieties, but we will only be interested in the case of curves, in which the codimension 1 subvarieties are just the individual points of C. The *degree* of a divisor, denoted $\deg D$, is the sum of its coefficients $\sum_n d_n$. We write $\sum n_P P \geq \sum m_P P$ if each $n_P \geq m_P$. The divisors of degree 0 form a subgroup, which we denote by $\mathrm{Div}^0(C)$. For any nonzero rational function $f \in k(C)$, we define the *divisor of f*, denoted $\mathrm{div}(f)$, to be $\sum_{P \in C} \mathrm{ord}_P(f) P$. Here, $\mathrm{ord}_P(f)$ equals k if P is a zero of order $k > 0$, -k if P is a pole of order $k > 0$, and zero otherwise. If $\mathrm{ord}_P(f) = -1$ then P is called a *simple pole* of f. Since f has only a finite number of poles and zeros, $\mathrm{div}(f)$ is a well-defined divisor. The divisor of a function is also called a *principal divisor*, and the subgroup of principal divisors is denoted $\mathrm{Prin}(C)$. From the relations $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$ and $\mathrm{div}(1/f) = -\mathrm{div}(f)$ it is clear that this is indeed a subgroup. Two divisors D and D' are said to be *linearly equivalent* if they differ by a pricipal divisor, i.e. $D' - D \in \mathrm{Prin}(C)$, in which case we write $D' \equiv D$. This is an equivalence relation. It can be shown that $\mathrm{Prin}(C) \subset \mathrm{Div}^0(C)$, i.e. $\deg(\mathrm{div}(f)) = 0$ for nonzero $f \in k(C)$.

Definition. The *divisor class group* of C is $\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Prin}(C)$, which is also called its *Picard group*. The *degree-0 part of the divisor class group* of C is $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Prin}(C)$.

If a rational function $f \in k(C)$ has a pole of order at most n at the point $P \in C$ and a zero at the point $Q \in C$, then we can write this neatly as $\operatorname{div}(f) \geq Q - nP$. Hence inequalities with divisors are useful for describing poles and/or zeros of functions.

Definition. To a divisor $D \in \operatorname{Div}(C)$ we associate the set of functions

$$L(D) = \left\{f \in k(C) : \operatorname{div}(f) \geq -D\right\} \cup \{0\}.$$

Thus a rational function f belongs to $L(D)$ if $f = 0$ or $\operatorname{ord}_P(f) \geq -n_P$ for all $P \in C$.

Theorem 1.8.1. *$L(D)$ is a finite-dimensional linear space over* $\mathbf{C}$.

We denote the dimension of $L(D)$ by $l(D)$. These spaces are sometimes called *Riemann–Roch spaces*, for their role in the *Riemann–Roch theorem*. Bases for these linear spaces can be computed using computer algebra systems such as MAGMA or SAGE.

1.9 The genus of a curve

In this section we define the genus of a curve. We will find that the Poncelet variety has genus 1 and contains a rational point, which leads us to the next section on elliptic curves.

There are many ways to define the genus of a curve, and most definitions agree on certain classes of curves. We give a definition in terms of divisors. Throughout this section, let C be a projective curve that is nonsingular unless stated otherwise.

Theorem 1.9.1. *There is an integer g such that $l(D) \geq \deg(D) + 1 - g$ for all divisors D. The smallest such g is called the* genus *of C. The genus is a nonnegative integer.*

For a proof, see Fulton [2008, p. 101]. This result is sometimes called *Riemann's theorem*. By definition the genus depends only on the function field, so two birationally equivalent curves have the same genus. Consequently, we can define the genus of a singular curve to be the genus of its nonsingular model (see theorem 1.7.3). We also say that g is the genus of the function field. The following corollary will be useful in the next section.

Corollary 1.9.2. *If $l(D_0) = \deg(D_0) + 1 - g$ and $D \equiv D' \geq D_0$, then $l(D) = \deg(D) + 1 - g$.*

Proof. Let $s(D) = \deg D + 1 - l(D)$ for every divisor D. Theorem 1.9.1 states that g is the smallest nonnegative integer such that $s(D) \leq g$ for all divisors D. We want to show that $s(D_0) = g$ implies $s(D) = g$ for $D \equiv D' \geq D_0$. It suffices to show that $s(D) = s(D')$ and $D' \geq D_0$ implies $s(D') \geq s(D_0)$. These are in fact proven on the way to proving Riemann's theorem, but since we have omitted that proof we show the first of these for fun. Suppose that $D' = D - \operatorname{div}(g)$. Define $\psi : L(D) \to L(D')$ by setting $\psi(f) = fg$. Then ψ is an isomorphism of linear spaces since $\operatorname{div}(f) \geq -D$ if and only if $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g) \geq -D + \operatorname{div}(g) = -D'$, and hence $l(D) = l(D')$. Because $\deg(\operatorname{div}(f)) = 0$ for nonzero $f \in k(C)$ and degree is additive, we also have $\deg D = \deg D'$. This means $s(D) = s(D')$. □

The next theorem is helpful in calculating the genus of a (possibly singular) projective plane curve.

Theorem 1.9.3. *Let C be a projective plane curve of degree d with only ordinary singularities. Then the genus of C is given by the formula*

$$g = \frac{1}{2}(d-1)(d-2) - \sum_{P \in C} \frac{\mu_P(\mu_P - 1)}{2}.$$

The formula in theorem 1.9.3 is one instance of a genus-degree formula. Since $\mathbf{P}^1$ is birational to the nonsingular plane curve $Z(f) \subset \mathbf{P}^2$ where $f(x,y,z) = z$ has degree 1, $\mathbf{P}^1$ has genus zero. We apply theorem 1.9.3 to an example.

Example 1.9.4. In example 1.7.2 we found that the Poncelet variety $M \subset \mathbf{P}^2$ given by $m(t,a) = 3t^4 - 3a^2t^4 - 10a^2t^2 + 4at^3 - 3a^2 - 4at + 10t^2 + 3$ had four ordinary singularities. Namely $[0:1:0]$ has multiplicity 4, and the three points $[i:i:1]$, $[-i:-i:1]$, and $[1:0:0]$ all have multiplicity 2. The homogeneous defining polynomial of M, being the homogenization of m, has degree six. By the genus-degree formula, we have $g(M) = 10 - 6 - 1 - 1 - 1 = 1$.

In fact we can compute the genus of the Poncelet variety M in full generality. For this we use the characterization of the function field of M (and hence E) described in proposition 1.7.4.

Proposition 1.9.5. *A nonsingular projective curve with function field $\mathbf{C}(x,y)$, where $y^2 = h(x)$, $h(x)$ is without square factor and has degree d, has genus $[(d-1)/2]$.*

Here, $[r]$ denotes the integer part of $r \in \mathbf{Q}$. The proof is an exercise in Silverman [2009, exercise II.2.14, p. 40]. Since we found in proposition 1.7.4 that $d \leq 4$, the Poncelet variety has genus at most 1. From now on we shall assume that our E has genus 1, which is the most nontrivial case. Note that we can arrange for E to contain a point with rational coordinates. This leads us to the next section.

1.10 Elliptic curves

In this section we define elliptic curves and equip them with a natural group structure. We show that every elliptic curve is isomorphic to one given by a Weierstrass equation.

Definition. An *elliptic curve* over the field $k \subset \mathbf{C}$ is a projective curve of genus 1 defined over k with a given point O that has coordinates in k.

The point O is also called the *base point* of the elliptic curve. Recall that for a curve to be defined over k means that its defining polynomial has coefficients in k. Because we have taken $\mathbf{C}$ as our base field, k must have characteristic zero, and in particular k is infinite. Elliptic curves can also be defined over finite fields, but we shall have no use for this. For the rest of this section, let E be an elliptic curve over k with base point O. There is a natural group structure on E, which we proceed to describe.

Theorem 1.10.1. *There is a one-to-one correspondence between E and $\operatorname{Pic}^0(E)$ given by $P \mapsto P - O$.*

Recall that $\mathrm{Pic}^0(E)$ is the degree-0 part of the divisor class group of E. Hence this yields a group law on E by pulling back the group operations via the bijection. The reader is perhaps more familiar with elliptic curves given by *Weierstrass equations* such as $y^2 = x^3 + ax + b$, where $a, b \in k$. Note that these are always nonsingular. On these curves, a group law is usually defined by declaring that any three points on the curve are collinear. That is, for $P, Q, R \in E$ on the same line, we have $P + Q + R = O$. The sum of two points P and Q is then given in coordinates by rational functions of the coordinates of P and Q. It can be shown that our group law agrees with this one in the case of a Weierstrass curve. In fact, every elliptic curve is isomorphic to one given by a Weierstrass equation. We proceed to show this.

Lemma 1.10.1. *For $P \in E$, $D = nP$ with $n > 0$, we have $l(D) = \deg(D) = n$.*

PROOF. If D satisfies $l(D) = \deg(D) = n$, and D' is a divisor such that $D' \geq D$, then we have $l(D') = \deg(D')$ by corollary 1.9.2. Since $nP \geq (n-1)P \geq \ldots \geq P$ as divisors, it is enough to show that $\ell(P) = 1$. Clearly $l(P) > 0$, since $k \subset L(P)$. On the other hand, $l(P) > 1$ would imply that there exists $f \in k(E)$ such that f has a simple pole at P, and no other poles. But this would imply that the map $f : E \to \mathbf{P}^1$ is an isomorphism, which contradicts the fact that $\mathbf{P}^1$ has genus zero. Thus $l(P) = 1$. □

Theorem 1.10.2. *The elliptic curve E is isomorphic to an elliptic curve given by*

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

in $\mathbf{P}^2$ with $a_i \in k$ and base point $[0:1:0]$.

PROOF. By lemma 1.10.1, we can choose functions $x, y \in k(E)$ such that $\{1, x\}$ is a basis for $L(2O)$ and $\{1, x, y\}$ is a basis for $L(3O)$. Note that x must have a pole of exact order 2 at O, and similarly y must have a pole of exact order 3 at O. Now we observe that $L(6O)$ has dimension 6, but it contains the seven functions $1, x, y, x^2, xy, y^2, x^3$. It follows that there is a linear relation

$$A_1 + A_2 x + A_3 y + A_4 x^2 + A_5 xy + A_6 y^2 + A_7 x^3 = 0,$$

where we may take the $A_i \in k$. Note that $A_6 A_7 \neq 0$, since otherwise every term would have a pole at O of different order, and so all of the A_j's would vanish. Replacing x and y by $-A_6 A_7 x$ and $A_6 A_7^2 y$ respectively and dividing by $A_6^3 A_7^4$, we obtain an equation in the desired form. This gives a map $\psi : E \to \mathbf{P}^2$ sending $P \neq O$ to $[x(P) : y(P) : 1]$ and sending O to $[0:1:0]$, whose image is the curve with that equation. It can be shown that ψ is an isomorphism. See for instance Silverman [2009, theorem III.3.1, p. 59]. □

The bases for the linear spaces in the proof above can in fact be computed using computer algebra systems such as SAGE, Singular and MAGMA.

Corollary 1.10.3. *The elliptic curve E is isomorphic to an elliptic curve given by*

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

in $\mathbf{P}^2$ with $a, b \in k$ and base point $[0:1:0]$.

This is proved by making two more changes of coordinates, which are possible because the characteristic of our base field is not 2 or 3.

1.11 Morphisms of elliptic curves

In this section we investigate the automorphism group $\mathrm{Aut}(E)$ of an elliptic curve. We find that it is a semidirect product of the automorphism group $\mathrm{Aut}(E,O)$ of the elliptic curve group and the group of translations with respect to the group operation. We use this fact to conclude the closure theorem.

Throughout this section we assume that E has a Weierstrass model $y^2 = x^3 + ax + b$. From corollary 1.10.3 and the fact that isomorphic varieties have isomorphic automorphism groups it follows that this is no restriction.

Proposition 1.11.1. *The maps of an elliptic curve given by negation $P \mapsto -P$ and translation $P \mapsto P+Q$ are morphisms.*

This follows from the fact that the group law on the cubic is given in coordinates by rational functions. A translation $P \mapsto P+Q$ is also denoted $\tau_Q : E \to E$. We denote the group of translations of E by T_E. We say that a point $Q \in E$ is a *k-torsion* point if τ_Q has finite order k in T_E. Since elliptic curves have a distinguished base point, it is natural to single out the maps that respect this property.

Definition. Let E_1 and E_2 be elliptic curves with base points O_1 and O_2. An *isogeny* from E_1 to E_2 is a morphism $\varphi : E_1 \to E_2$ satisfying $\varphi(O_1) = O_2$.

With these morphisms we obtain the category of elliptic curves. It might seem more natural to focus on those isogenies that are group homomorphisms, but the following theorem shows that this is unnecessary.

Theorem 1.11.2. *An isogeny is a homomorphism.*

The set of invertible isogenies of an elliptic curve E form a group called the *automorphism group* of E, and we denote it by $\mathrm{Aut}(E,O)$. The following theorem characterizes this group.

Theorem 1.11.3. *Let E be an elliptic curve. Then its automorphism group $Aut(E,O)$ is $\mathbf{Z}/n\mathbf{Z}$, where n is one of 2, 4, and 6.*

For a proof of this, see Silverman [2009, theorem III.10.1, p. 103]. Because the groups from the theorem have only one element of order 2, we have the following corollary.

Corollary 1.11.4. *The only involution in* $\mathrm{Aut}(E,O)$ *is* $[-1]$.

We will make great use of this fact later.

Proposition 1.11.5. *An automorphism $\varphi \in \mathrm{Aut}(E)$ can be written $\varphi = \tau_Q\phi$, the composition of an isogeny ϕ and a translation τ_Q, and this representation is unique.*

PROOF. Put $\phi(P) = \varphi(P) - \varphi(0)$ and $Q = \varphi(0)$. For uniqueness (if it isn't obvious), suppose that $\varphi(P) = \phi(P) + Q = \phi'(P) + Q'$. Then $Q' = \varphi(O) = Q$ and $\phi'(P) = \varphi(P) - Q = \phi(P)$. □

This proposition helps us show that T_E is a normal subgroup of $\mathrm{Aut}(E)$. Indeed, if $\varphi = \tau_Q\phi$ is an automorphism, then it is an easy computation that $\varphi\tau_R\varphi^{-1} = \tau_{\phi(R)}$. Hence the proposition shows that $\mathrm{Aut}(E) = T_E \rtimes \mathrm{Aut}(E,O)$, the semidirect product of T_E and $\mathrm{Aut}(E,O)$.

Corollary 1.11.6. *An involution $\varphi \in \operatorname{Aut}(E)$ is either a translation by a 2-torsion point, or $\varphi(P) = Q - P$ for some $Q \in E$.*

Proof. Write $\varphi = \tau_Q \phi$. Then $\varphi^2 = \tau_Q \phi \tau_Q \phi$, and since $\phi \tau_Q = \tau_{\phi(Q)} \phi$, we have $\varphi^2 = \tau_{Q+\phi(Q)} \phi^2$. In particular $\varphi^2(O) = Q + \phi(Q)$, and since φ is an involution we must have $\phi(Q) = -Q$, so in fact $\varphi^2 = \phi^2 = \mathrm{id}_E$. This means that $\phi \in \operatorname{Aut}(E, 0)$ is an element of order ≤ 2, so (by corollary 1.11.4) we have either $\phi = \mathrm{id}$ or $\phi = [-1]$. If $\phi = [-1]$, any $Q \in E$ will do. If $\phi = \mathrm{id}$, then $Q \in E$ must be a 2-torsion point. □

Finally, we are ready to prove Poncelet's closure theorem as we stated it at the end of section 1.7.

Theorem 1.11.7 (Poncelet's closure theorem)**.** *If there exists an integer $k > 1$ such that η^k has a fixed point which is not a fixed point of η, then $\eta^k = \mathrm{id}_E$.*

Proof. We know that $\sigma, \tau \in \operatorname{Aut}(E)$ are involutions of E. Hence by corollary 1.11.6 either $\sigma(P) = Q - P$ for some $Q \in E$ or $\sigma = \tau_Q$ for a 2-torsion point Q. But σ has fixed points and isn't the identity on E, so the latter possibility is excluded. Analogously, $\tau(P) = R - P$ for some $R \in E$. Hence $\eta(P) = \tau\sigma(P) = R - (Q - P) = P + (Q - R)$, a translation by the point $Q - R \in E$. Since $\sigma \neq \tau$, we must have $Q \neq R$ and hence $Q - R \neq O$. Note that η itself has no fixed points, as we remarked at the end of section 1.7. If η^k has a fixed point for some $k > 1$, then $Q - R$ is a k-torsion point and hence $\eta^k = \mathrm{id}_E$. □

1.12 Concluding remarks

In this chapter we constructed the Poncelet variety M, a projective plane model of the set X described in the introduction. We showed that M is birational to a nonsingular elliptic curve E, and we used the group structure of $\operatorname{Aut}(E)$ to conclude the theorem. It is also possible to show that X is itself a variety (using a more general definition of a variety), and this is the approach taken by Griffiths and Harris [1977]. Our proof is more algebraic in the sense that we used the group structure of $\operatorname{Aut}(E)$. Griffiths and Harris also proved a Poncelet-type theorem for quadrics in $\mathbf{A}^3$ in the same paper. Quadrics in $\mathbf{A}^3$ are zero sets of quadratic polynomials in $\mathbf{C}[x, y, z]$. Since this proof also involves an elliptic curve, perhaps it is possible to give a proof in a similarly explicit way as was done for Poncelet's closure theorem in this chapter.

There are some more interesting facts related to the closure theorem. There is an explicit condition due to Cayley for the existence of a closed Poncelet traverse which involves determinants [Griffiths and Harris, 1978]. One can also look at the theorem for conics with rational coefficients. In this case it is known that only Poncelet traverses with $3, 4, 5, 6, 7, 8, 9, 10$ or 12 vertices can exist. A first bound was given by Malyshev [2008], which also included $14, 16, 18, 20$ and 24 as possibilities. This was improved by Los [2013] to exclude these possibilities, by examining the torsion subgroup of an elliptic curve defined over $\mathbf{Q}$. There is also a connection between Poncelet's closure theorem and dynamical billiards in ellipses, which we investigate in the next chapter.

Chapter 2

A connection with dynamical billiards

In this chapter we give a brief introduction to dynamical billiards in ellipses and we derive a result involving Poncelet's closure theorem. We ask two interesting and difficult questions about the connection between Poncelet's closure theorem and dynamical billiards in ellipses.

Let C_1 be an ellipse in $\mathbf{A}^2$ (a circle is also an ellipse). We call the interior of C_1 the *billiard table*. Define a flow on the billiard table by letting a particle move freely with unit velocity in the interior, with elastic reflections at the boundary. That is, *the angle of incidence equals the angle of reflection*, where angles are measured with respect to the normal to C_1 at the point of contact.

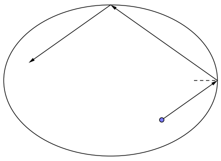


Figure 2.1: Billiards in an ellipse.

We now describe all possible trajectories. If the trajectory passes through a focus of the ellipse, then the consecutive line segments pass alternately through the two foci of C_1. When the trajectory moves along the minor axis of C_1, it reverses direction upon each contact with C_1. In all other cases we have the following:

Theorem 2.1. *The lines containing the segments of a billiard trajectory in C_1 are all tangent to another ellipse or a hyperbola C_2 confocal with C_1.*

We omit the proof, which can be found in Pecker [2012, theorem 2]. From now on, by billiard trajectories we shall mean the kind in theorem 2.1, excluding the two simple cases described before it. The conic C_2 in theorem 2.1 is called a *caustic* of the trajectories. The proof of theorem 2.1 in fact shows that the caustic is completely determined by a *single* segment of a billard trajectory. We say that a billiard trajectory is *k-periodic* if it makes contact with C_1 at exactly $k > 1$ distinct points. Clearly Poncelet's closure theorem applies to the conics C_1 and C_2:

Corollary 2.2. *If one billiard trajectory in C_1 is k-periodic, then every billiard trajectory in C_1 is k-periodic.*

The k-periodic billiard trajectories in corollary 2.2 correspond to Poncelet traverses that close in $k+1$ steps. Hence the pairs of conics that satisfy the conclusion of Poncelet's closure theorem are divided into two classes: those that arise from billiards in an ellipse, and the rest. This raises at least two questions. Can an arbitrary Poncelet pair (C_1, C_2) be transformed into a billiards pair (C_1', C_2') by, say, a coordinate transformation? Does this divide the Poncelet varieties into two classes, or can an ordinary Poncelet pair give rise to the same Poncelet variety as a billiards pair? These are interesting and difficult questions that the author has not yet been able to answer, and which may be the subject of further research.

Bibliography

William Fulton. Algebraic Curves: An Introduction to Algebraic Geometry. Free online LaTeX edition, 2008.

Philip Griffiths and Joseph Harris. A Poncelet theorem in space. *Commentarii Mathematici Helvetici*, 52:145–160, 1977.

Philip Griffiths and Joseph Harris. On Cayley's explicit solution to Poncelet's porism. *L'Enseignement Mathematique*, 24:31–40, 1978.

Robin Hartshorne. *Algebraic Geometry*. Springer, 1977.

Serge Lang. *Algebra*. Springer, revised 3rd edition, 2005.

Johan Los. Ponceletfiguren over Q. Bachelor's thesis, University of Groningen, 2013.

Vladimir Aleksandrovich Malyshev. Poncelet problem for rational conics. *St. Petersburg Mathematical Journal*, 19(4):597–601, 2008.

Daniel Pecker. Poncelet's theorem and Billiard knots. *Geometriae Dedicata*, 161(1): 323–333, 2012.

Jean-Victor Poncelet. *Traité des propriétés projectives des figures*. Bachelier, 1822.

Igor Shafarevich. *Basic Algebraic Geometry*. Springer-Verlag, 2nd edition, 1994.

Joseph Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2nd edition, 2009.

Glossary of Notations

$\mathbf{A}^n$	Affine n-space,	1
$\mathrm{Aut}(E,O)$	Automorphism group of the elliptic curve E,	18
$\mathrm{Aut}(Y)$	Automorphism group of the variety Y,	7
$A(Y)$	Coordinate ring of an affine variety Y,	7
$\mathbf{C}$	The complex numbers,	1
$\mathbf{C}^*$	Units of $\mathbf{C}$,	3
$\mathbf{C}[x_1,\dots,x_n]$	Polynomial ring in n variables over $\mathbf{C}$,	1
$\mathrm{Div}(C)$	Group of divisors on the curve C,	14
$\mathrm{dom}\,\varphi$	Domain of the rational function φ,	8
f^*	Homogenization of the polynomial f,	4
f_*	Dehomogenization of the homogenous polynomial f,	4
$I(Y)$	Ideal of the algebraic set Y,	2, 4
id_Y	The identity morphism $Y \to Y$,	7
$k(Y)$	Function field of the variety Y,	7
$L(D)$	Riemann-Roch space of the divisor D,	15
$l(D)$	Dimension of the Riemann-Roch space $L(D)$,	15
μ_P	Multiplicity of the singular point P on a curve,	12
$\mathrm{ord}_P(f)$	Order of the rational function f at P,	14
$\mathbf{P}^n$	Projective n-space,	3
$\mathrm{Pic}(C)$	Picard group of the curve C,	14
$\mathrm{Pic}^0(C)$	Degree-0 part of the Picard group of C,	14
$\mathrm{Sing}\,C$	Singular points of the curve C,	11
τ_Q	Translation by Q on an elliptic curve,	18
T_E	Group of translations of the elliptic curve E,	18
$\overline{Y}$	Projective closure of the affine variety Y,	5
$Z(T)$	Zero set of the polynomials in T,	1

Index