Master's Thesis

Finding a pointless rational genus one curve with specified automorphism group

Author:
J.H. Dwarshuis

First supervisor:
Prof. dr. J. Top

Second supervisor:
dr. J.S. Müller

Msc Mathematics

July 4, 2020

university of groningen / faculty of science and engineering

Abstract

The aim of this thesis is to find an example of a genus one curve over $\mathbb{Q}$ that has no rational points and contains the dihedral group of order 18 in its automorphism group. Three methods to obtain such a curve are investigated. The first arises from Poncelet sequences with which some new constructions are explored. A much more direct method involves the use of invariant theory, in which one starts with polynomials invariant under the D_9-action and tries to build a genus one curve from those. Finally, a method using twists of elliptic curves is presented. The first and last method were successful, in both an explicit equation of a curve with the desired properties was found.

Contents

1 Introduction

The goal of this thesis is to find an explicit example of a genus one curve X over $\mathbb{Q}$ that has the following two properties:

- The dihedral group of order 18 is contained in the automorphism group of X over $\mathbb{Q}$, i.e. $D_9 \subset \mathrm{Isom}_{\mathbb{Q}}(X)$.
- X has no rational points.

The problem is a follow-up to a master's thesis by M. Roelfszema [5], where this problem is treated for D_n with $n \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$. In all cases but $n = 9$ such curve was found, so this case proved to be hardest. The applied method involved the use of Poncelet figures and this will also be the first method tried here.

Let us study the problem a little closer. Recall that a dihedral group D_n of order $2n$ is defined as

$$D_n = \{< \sigma, \rho > \mid \rho^n = \sigma^2 = id,\ \sigma\rho\sigma = \rho^{-1}\}.$$

It is the group of symmetries of a regular n-gon, which includes rotations and reflections. If the second requirement in the problem is dropped, the problem becomes easy to solve. One can consider an elliptic curve over $\mathbb{Q}$ with a rational point P of order 9. Then taking for σ the multiplication map $[-1]$ and for ρ the translation-by-P map shows that the elliptic curve has the required property. When the curve is not allowed to have rational points, the problem is a lot harder to solve.

In this thesis three methods to tackle this problem are presented. As mentioned the first method deals with Poncelet figures and some possibilities not explored in [5] are considered. In chapter 3 one finds a method involving some invariant theory. The third and last method is about twisting a curves and can be found in chapter 4.

2 Poncelet method

Our first approach to the problem involves the use of Poncelet figures. With the nice construction of these figures, we obtain a genus one curve admitting two involutions. This can be used to construct curves with the required properties, as will become clear in this chapter.

2.1 Poncelet's closure theorem

The main idea of this method arises from Poncelet's closure theorem, which has received quite a lot of attention over the past years. We will repeat the construction in short and mention some important facts concerning its application in the method described in this chapter. This is all done in [5] and [3] and we refer to these for more details. Let $\mathcal{C}$ and $\mathcal{D}$ be distinct irreducible conics in $\mathbb{P}^2$. Let $P_1 \in \mathcal{C}$ be a point and l_1 be a line tangent to $\mathcal{D}$ containing P_1. Now (P_1, l_1) is the first pair and define the next pair as follows. P_2 is the other intersection point of $\mathcal{C}$ with l_1 and l_2 is defined as the tangent line of $\mathcal{D}$ not equal to l_1, such that $P_2 \in l_2$. Repeating this process, one obtains a sequence

$$(P_1, l_1), (P_2, l_2), \ldots, (P_n, l_n), \ldots$$

This is called a Poncelet sequence and the corresponding figure a Poncelet figure. Such a sequence is called periodic of order n if $(P_n, l_n) = (P_1, l_1)$ for some n. Trivial Poncelet sequences occur when either $P_i \in \mathcal{C} \cap \mathcal{D}$ for i or l_j is tangent to both $\mathcal{C}$ and $\mathcal{D}$ for some j. Now Poncelet's closure theorem states the following.

Theorem 1. *Let $\mathcal{C}$ and $\mathcal{D}$ be distinct irreducible conics in $\mathbb{P}^2$. If an initial pair (P_1, l_1) defines a non-trivial Poncelet sequence of order n, then any starting pair (P, l) with $P \in \mathcal{C} \cap l$ and l tangent to $\mathcal{D}$ defines a Poncelet sequence of order n.*

Now define

$$X := \quad \{(P, l) \colon P \in \mathcal{C} \cap l,\ l \text{ tangent to } \mathcal{D}\}$$

which is an algebraic curve in $\mathcal{C} \times \mathcal{D}^\vee$. Here $\mathcal{D}^\vee$ is the 'dual space' of $\mathcal{D}$ and its points correspond to lines in $\mathbb{P}^2$ tangent to $\mathcal{D}$. The curve X has genus one if and only if $\#\mathcal{C} \cap \mathcal{D} = 4$. Also, the following maps define involutions on X: $\sigma \colon (P, l) \mapsto (P, l')$ and $\tau \colon (P, l) \mapsto (P', l)$. Here $\{P, P'\} = C \cap l$ and $\{l, l'\}$ is the set of lines containing P that are tangent to $\mathcal{D}$. In Section 2.3 more will be explained about how to get a construction in which D_9 is contained in the automorphism group of X.

2.2 An example

In this section we present an example of how Poncelet figures can be used to construct a genus one curve admitting two involutions. It is a simple example involving just one parameter and will not result in a curve with the desired properties. It will only serve as an illustration of the method.

Let $\mathcal{C}$ and $\mathcal{D}$ be conics in $\mathbb{P}^2_{\mathbb{Q}}$, in affine equations given by $\mathcal{C}\colon xy = t$ with $t \in \mathbb{Q}\backslash\{0\}$ and $\mathcal{D}\colon x^2 + y^2 = 1$. Let $P = (x, y)$ be a point on $\mathcal{C}$ and $l\colon \eta = a\xi + b$ be a line through $P = (x, y)$, so $y = ax + b$. Then l is tangent to $\mathcal{D}$ if and only if $a^2 - b^2 + 1 = 0$. Hence an affine algebraic model of X in $\mathbb{A}^4$ is described by the points (x, y, a, b) satisfying

$$\begin{cases} xy = t \\ a^2 - b^2 + 1 = 0 \\ y = ax + b. \end{cases} \tag{1}$$

Solving the equations for two variables, one can show that this model is birational over $\mathbb{Q}$ to the curve X given by $Y^2 = x^4 - x^2 + t^2$, with birational correspondence given by $Y = -ax^3 + (a + t)x$. Observe that for $t \neq \pm\frac{1}{2}$, $\#\mathcal{C} \cap \mathcal{D} = 4$ and hence X has genus 1 in this case. It has rational points $(x, Y) = (0, \pm t)$ so X is in fact an elliptic curve (this already shows why this example does not satisfy the desired properties). Sending the point $(0, t)$ to infinity, it is birationally equivalent to the Weierstrass form

$$E\colon \quad V^2 = U^3 - U^2 - 4t^2U + 4t^2,$$

where $U = \frac{2t(Y+t)}{x^2}$ and $V = \frac{4t^2(Y+t)-2tx^2}{x^3}$. So a model of X is given by the elliptic curve E with coordinates

$$U = \frac{2t(-ax^3 + (a + t)x + t)}{x^2}, \qquad V = \frac{4t^2(-ax^3 + (a + t)x + t) - 2tx^2}{x^3}.$$

The inverse transformation is given by

$$x = \frac{2t(U - 1)}{V}, \qquad a = -\frac{(2U^3 - 2tVU - 4U^2 - V^2 + 2tV + 2U)V}{2(U - 1)(4U^2t^2 - 8Ut^2 - V^2 + 4t^2)}.$$

2.2.1 Involutions on the curve

As mentioned, X admits the involutions $\sigma\colon (P, l) \mapsto (P, l')$ and $\tau\colon (P, l) \mapsto (P', l)$. Explicit equations of these involutions on E can be found as follows. In the affine model of X, σ acts geometrically as changing the tangent line l to the other tangent line containing P. So σ acts as

$$(x, y, a, b) \mapsto (x, y, -a - \frac{2t}{1 - x^2}, y + ax + \frac{2tx}{1 - x^2}).$$

Here the image of a follows from combining the equations of (1) into a quadratic equation in a and noting that the sum of its two solutions equals $-B/A$ where A and B are the coefficients of respectively a^2 and a. Plugging this in in $y = ax + b$ gives the image of b. Similarly, τ acts geometrically as changing the intersection point of l with $\mathcal{C}$ and one verifies that τ is given by

$$(x, y, a, b) \mapsto (-x - \frac{b}{a}, -y + b, a, b).$$

Using the coordinate transformations from the affine model of X to the Weierstrass model E and their inverses, the actions of σ and τ on E can now be computed. As the resulting equations are given by huge expressions, they will not be written out here.

2.2.2 Rational points

To understand even better the relation between the geometry in the Poncelet figure and the elliptic curve E, one may consider some of the rational points. The following rational points lie on E (it is by no means an exhaustive list):

$$O,\ (1,0),\ (0,\pm 2t),\ (2t+2,\pm(4t+2)),\ (-2t+2,\pm(4t-2)),\ (4t^2,\pm(8t^3-2t)).$$

Now consider the table below. It shows in columns 2 to 5 the values of x, y, a, b as given by Magma when applying the coordinate transformation on rational points of E. As only an affine model of X is considered, some points are not contained in this model, resulting in ∞-entries in the table. It is still possible, however, to deduce their corresponding point $(P, l) \in \mathbb{P}^2 \times \mathbb{P}^2$ from the action of σ and τ on these points. These are shown in the last two columns. Let us see some examples of how the pair (P, l) can be derived from the

Point on E	x	y	a	b	P	l
$(0:1:0)$	0	∞	∞	∞	$(0:1:0)$	$x=-1$
$(1,0)$	0	∞	∞	∞	$(0:1:0)$	$x=1$
$(2t,0)$	∞	0	0	1	$(1:0:0)$	$y=1$
$(-2t,0)$	∞	0	0	-1	$(1:0:0)$	$y=-1$
$(0,2t)$	-1	$-t$	$\frac{t^2-1}{2t}$	$\frac{-t^2-1}{2t}$	$(-1,-t)$	$y=\frac{t^2-1}{2t}x-\frac{t^2+1}{2t}$
$(0,-2t)$	1	t	∞	∞	$(1,t)$	$x=1$
$(2t+2,4t+2)$	t	1	0	1	$(t,1)$	$y=1$
$(-2t+2,4t-2)$	$-t$	-1	0	-1	$(-t,-1)$	$y=-1$
$(-2t+2,-4t+2)$	t	1	$\frac{2t}{t^2-1}$	$-\frac{t^2+1}{t^2-1}$	$(t,1)$	$y=\frac{2t}{t^2-1}x-\frac{t^2+1}{t^2-1}$
$(2t+2,-4t-2)$	$-t$	-1	$\frac{2t}{t^2-1}$	$\frac{t^2+1}{t^2-1}$	$(-t,-1)$	$y=\frac{2t}{t^2-1}x+\frac{t^2+1}{t^2-1}$
$(4t^2,8t^3-2t)$	1	t	$\frac{t^2-1}{2t}$	$\frac{t^2+1}{2t}$	$(1,t)$	$y=\frac{t^2+1}{t^2-1}x+\frac{t^2+1}{t^2-1}$
$(4t^2,-8t^3+2t)$	-1	$-t$	∞	∞	$(-1,-t)$	$x=-1$

Table 1: Pairs (P, l) corresponding to rational points on E

other points and the involutions. The points $(2t, 0)$ and $(2t+2, 4t+2)$ both correspond to a pair with $l\colon y = 1$ and $\tau(2t, 0) = (2t+2, 4t+2)$. Since this line meets $\mathcal{C}$ in $(t, 1)$ and 'at infinity', $P = (1:0:0)$ is the point corresponding to $(2t, 0)$. Similarly, one deduces that $P = (1:0:0)$, $l\colon y = -1$ comes from $(-2t, 0) \in E$ as $\tau(-2t, 0) = (-2t+2, 4t-2)$. Observe that the line $x = -1$ meets the hyperbola $\mathcal{C}$ in the points $(-1, -t)$ and $(0:1:0)$. Hence $(4t^2, -8t^3+2t) \in E$ corresponds to the pair $P = (-1, -t)$, $l\colon x = -1$ and $\tau(4t^2, -8t^3+2t) = (0:1:0)$ corresponds to $P = (0:1:0)$, $l\colon x = -1$. Finally, as σ acts as swapping the tangent line this implies that $\sigma(0:1:0) = (1, 0)$ corresponds to $P = (0:1:0)$, $l\colon x = 1$.

Remark 1. *Viewing E as a curve over the function field $\mathbb{Q}(t)$ one finds with Magma that it has rank 1 and torsion isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In particular it has infinitely many*

rational points. Generators of $E(\mathbb{Q})$ are e.g. $(\pm 2t, 0)$ together with $(0, 2t)$, where the first two generate the torsion subgroup. Note that our approach is rather different: we want to fix t so that E over $\mathbb{Q}$ has a certain property.

2.2.3 Aside: the reducible case

In the case $t = \pm\frac{1}{2}$, the situation is rather different. It is not relevant for our construction, but we mention it for completeness. Since $\#\mathcal{C} \cap \mathcal{D} = 2$, X does not have genus 1 anymore. In fact, X is reducible and hence its (geometric) genus is not even defined. Note that the two intersection points of $\mathcal{C}$ and $\mathcal{D}$ are invariant under both σ and τ because their tangent lines to $\mathcal{C}$ and $\mathcal{D}$ coincide. See Figure 1. An equation for X is given by $Y^2 = x^4 - x^2 + \frac{1}{4} = (x^2 - \frac{1}{2})^2$. Let $C_1 \colon Y = x^2 - \frac{1}{2}$ and $C_2 \colon Y = -x^2 + \frac{1}{2}$ be the two components of X. The involutions act as

$$\sigma \colon (x, Y) \mapsto (x, -Y), \qquad \tau \colon (x, Y) \mapsto \Big(\frac{x^2 - 1}{2Y - x}, \frac{2Yx^3 - 2x^2 + 2Yx - 4Y^2 + 1}{2x(2Y - x)^2}\Big).$$

It is not hard to see that σ maps points of C_1 to C_2 and vice versa. A computation shows that τ does the same. Hence $\sigma\tau$ has the nice property of mapping $C_1 \to C_1, C_2 \to C_2$.

2.2.4 Finding curves with dihedral group in automorphism group

As will soon be discussed, the composition of σ and τ is given by a translation map on E. The computation

$$\sigma\tau(0 : 1 : 0) = \sigma(4t^2 : -8t^3 + 2t : 1) = (0, 2t)$$

shows that in this example $\sigma\tau$ is translation by $(0, 2t)$. Suppose $(0, 2t)$ has order n. Then $\rho := \sigma\tau$ has order n and

$$\sigma\rho\sigma = \tau\sigma = (\sigma\tau)^{-1} = \rho^{-1},$$

so that σ and ρ (and hence σ and τ) generate $D_n \subset \mathrm{Isom}_{\mathbb{Q}}(E)$. We are therefore interested in the order of the point $(0, 2t)$ when fixing $t \in \mathbb{Q}$. As will soon become clear, there is no $t \in \mathbb{Q}$ for which $(0, 2t)$ has order 9 which is another reason this example does not work

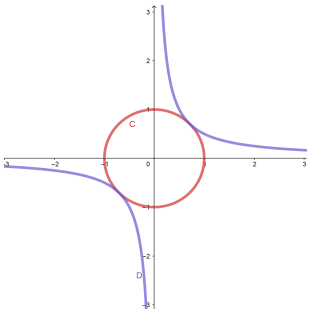

Figure 1: Case $t = 1/2$

for our purposes. For illustration, the possibilities for $(0, 2t)$ to be a torsion point will be explored now.

Observe that $(1, 0)$ is a point of order 2 independent of the choice of t. Therefore, by Mazur's theorem on the rational torsion of an elliptic curve [4], $\text{ord}(0, 2t) = 2, 4, 6$ or 8.

- A point on E has order 2 if and only if its y-coordinate is 0, hence $(0, 2t)$ cannot have order 2.
- $(0, 2t)$ has order 4 if $2 \cdot (0, 2t) = (t^2 + 1, t^3 - t)$ has order 2, which happens when $t^3 - t = 0$. So for $t = \pm 1$, it has order 4.
- The numerator of the y-coordinate of $3 \cdot (0, 2t)$ factors as $2t(3t^2 - 1)(t^2 + 2t - 1)(t^2 - 2t - 1)$ which has no roots in $\mathbb{Q}\backslash\{0\}$. Hence there is no $t \in \mathbb{Q}$ for which $(0, 2t)$ has order 6.
- $4 \cdot (0, 2t)$ has as numerator in its y-coordinate a polynomial of degree 12 in t which has no zeros in $\mathbb{Q}$. So $(0, 2t)$ will never have order 8.

In conclusion, the elliptic curve obtained from this Poncelet construction admits $D_n \subset \text{Isom}_{\mathbb{Q}}(E)$ only for $n = 4$, in which case $t = \pm 1$. For $t = 1$ this curve is $V^2 = U^3 - U^2 - 4U + 4$ and $(0, 2)$ on it has order 4.

2.3 The general setup

In this section some results that are important for our Poncelet method and a general setup will be derived. But first some remarks about notation. For k a field of characteristic 0, the isomorphism group of X is the group of $\bar{k}$-isomorphisms from X to itself. This group is usually denoted $\text{Aut}(X)$ but in this thesis it will be denoted $\text{Isom}(X)$. The subgroup consisting of all isomorphisms that are defined over k is denoted $\text{Isom}_k(X)$. The reason for using 'Isom' instead of 'Aut' is that the notation $\text{Aut}(X)$ might be confusing when X is equipped with a point, making it an elliptic curve. The notation $\text{Aut}(E)$ for E an elliptic curve will be used to denote the $\bar{k}$-isomorphisms from E to E that take O to O. For an elliptic curve E, $\text{Isom}(E) \neq \text{Aut}(E)$ as $\text{Isom}(E)$ contains translation maps $\tau_P \colon E \to E$. The group $\text{Isom}(E)$ is described more fully in the next proposition, which is Prop. X.5.1 in [7].

Proposition 1. *The map*

$$E \times \text{Aut}(E) \to \text{Isom}(E), \qquad (P, \alpha) \mapsto \tau_P \circ \alpha$$

is a bijection of sets. In other words, the group $\text{Isom}(E)$ *can be identified with the set of ordered pairs in* $E \times \text{Aut}(E)$*. In this way the latter set becomes a group with identity element* (O, id) *and group law*

$$(P, \alpha) \cdot (Q, \beta) = (P + \alpha(Q), \alpha \circ \beta).$$

Proof. Let $\phi \in \mathrm{Isom}(E)$. Write $P = \phi(O)$ and $\alpha = \tau_{-P} \circ \phi$. Then $\alpha(O) = O$ and hence $\alpha \in \mathrm{Aut}(E)$. Now the surjectivity of the map follows from writing $\phi = \tau_P \circ (\tau_{-P} \circ \phi)$.
For injectivity, suppose $\tau_P \circ \alpha = \tau_Q \circ \beta$. Then evaluating at O gives $\tau_P(O) = \tau_Q(O)$, so $P = Q$. Then also $\alpha = \beta$ and this shows injectivity of the map.
Finally, for its group structure, note that for every $R \in E$,

$$\alpha \circ \tau_Q(R) = \alpha(Q + R) = \alpha(Q) + \alpha(R) = \tau_{\alpha(Q)} \circ \alpha(R)$$

and hence

$$\tau_P \circ \alpha \circ \tau_Q \circ \beta = \tau_P \circ \tau_{\alpha(Q)} \circ \alpha \circ \beta.$$

Writing $\tau_P \circ \alpha$ as (P, α) and $\tau_Q \circ \beta$ as (Q, β), this calculation shows the desired group law. □

This characterization of $\mathrm{Isom}(E)$ can be used to describe involutions on E.

Lemma 1. *Let k be a field, E/k be an elliptic curve and $\sigma \in \mathrm{Isom}(E)$ an involution. Then σ is of one of the following forms:*

- *$P \mapsto P + Q$ with $Q \in E$ of order 2.*
- *$P \mapsto R - P$ for a fixed $R \in E$.*

Proof. Use the group structure of $\mathrm{Isom}(E)$ as in Proposition 1 and let $\sigma = (P, \alpha)$. From

$$(P + \alpha P, \alpha^2) = (P, \alpha) \cdot (P, \alpha) = (O, id)$$

one obtains that σ has order 2 if and only if $(P, \alpha) \neq (O, id)$, $P + \alpha P = O$ and $\alpha^2 = id$. Since $\mathrm{char}(\mathbb{Q}) = 0$, [7, Thm III.10.1] gives that $\mathrm{Aut}(E)$ is a cyclic group of order $2, 4$ or 6. Therefore, there is only one element of order 2 in $\mathrm{Aut}(E)$ and it is the multiplication by -1 map. So either $\alpha = id$ or $\alpha = [-1]$ which implies that σ is of one of the following two forms:

- $\sigma = (P, id)$ with $2P = O$ and $P \neq O$, i.e. translation over a point of order 2,
- $\sigma = (P, [-1])$ with $P \in E$.

Translating this back with the bijection of Proposition 1 gives the desired result. □

This result can be used to explicitly describe the involutions σ and τ in the example of 2.2. A nice way of doing so is the following. With a computation one shows that the pullback under the involutions of the invariant differential of E is given by $\sigma^*\left(\frac{dU}{V}\right) = -\frac{dU}{V}$ and $\tau^*\left(\frac{dU}{V}\right) = -\frac{dU}{V}$. Since the invariant diffential is invariant under translation (e.g. [7, Prop III.5.1]), it follows from Lemma 1 that σ and τ must be of the form $P \mapsto R - P$ for some $R \in E$. Applying the involutions to O, one finds

$$\sigma \colon P \mapsto (1, 0) - P, \qquad \tau \colon P \mapsto (4t^2, -8t^3 + 2t) - P.$$

The composition $\sigma\tau$ is then the translation-by-$(0, 2t)$ map as mentioned in section 2.2.4.

In general, the composition of two involutions acting in the same way on the invariant differential is always a translation map. Going back to the initial setup (§2.1), $\mathcal{C}$ and $\mathcal{D}$ are conics in $\mathbb{P}^2$ and σ and τ are involutions on the genus one curve X. Fixing a point over k on X, it gets the structure of an elliptic curve E/k. As mentioned in the context for the proof of [5, Thm 3], $\mathcal{C}$ and $\mathcal{D}$ being genus 0 curves implies that σ and τ are respectively of the form $P \mapsto R - P$, $P \mapsto S - P$ for some $R, S \in E$. Therefore, the composition $\sigma\tau$ acts as $P \mapsto (R - S) + P$, i.e. translation by $R - S$. In fact, the closure theorem follows from this observation: if some initial pair (P_1, l_1) defines a non-trivial Poncelet sequence of order n, then $\sigma\tau$ has order n and hence any starting point (P, l) returns to itself after n steps.

Now consider the following construction. Let X be the genus one curve obtained from conics $\mathcal{C}$ and $\mathcal{D}$. Take $P_1 \in X(k)$ with k some extension field of $\mathbb{Q}$ and define $E := (X, P_1)$ with isomorphism $\phi\colon X \to E$ over k. Define $P_2 := \sigma\tau(P_1) \in X$ and suppose that $\phi(P_2) \in E$ has order 9. Then $\sigma\tau$ is translation by a point of order 9 and hence σ and τ generate $D_9 \subset \mathrm{Isom}_{\mathbb{Q}}(X)$. Now if X has no rational points, it has the desired properties. This is the setup we will use and it will be illustrated with an example later in this chapter.

2.4 An observation

In order to search for a curve X with the desired properties, we want to try multiple families of examples. Different families can be constructed by varying the conics $\mathcal{C}$ and $\mathcal{D}$, taking circles, hyperbolas or ellipses. However, we should make sure to try 'new' families. This section makes more precise what is meant by this.

Proposition 2. *All smooth conics in $\mathbb{P}^2$ over $\mathbb{Q}$ with a rational point are equivalent.*

Proof. Let $\mathcal{C}$ be a smooth conic in $\mathbb{P}^2_{\mathbb{Q}}$ with a rational point. By applying a linear transformation we may assume this point is $(0 : 1 : 0)$ and that $\mathcal{C}$ has tangent line $z = 0$ at this point. Write $\mathcal{C}$ as

$$ax^2 + bxy + cy^2 + z(dx + ey + fz) = 0.$$

Now $(0 : 1 : 0) \in \mathcal{C}$ implies $c = 0$. Also $b = 0$, since $\mathcal{C}$ has tangent line $z = 0$. Since $\mathcal{C}$ is a smooth conic, a is not zero and by dividing the equation by a we may assume $a = 1$. Hence the equation reduces to

$$x^2 + z(dx + ey + fz) = 0.$$

The partial derivatives with respect to x and y of this equation evaluated at $(0 : 1 : 0)$ are zero, so the partial derivative to z must not be zero, as $(0 : 1 : 0)$ is a smooth point. This implies e is nonzero. Hence there is a linear transformation fixing x, z and mapping $dx + ey + fz$ to y. Thus $\mathcal{C}$ is equivalent to the conic $x^2 + yz$ and therefore all smooth conics in $\mathbb{P}^2_{\mathbb{Q}}$ with a rational point are. This implies the result. □

Remark 2. *This proposition can be proven with more general theory about quadratic forms. This is done as follows.*

Proof (of Prop. 2). Note that a smooth conic in $\mathbb{P}^2$ over $\mathbb{Q}$ is a non-degenerate quadratic form of rank 3. The following result then follows from combining Theorem 7 and 9 of [6, Ch. 4]: two quadratic forms f and f' over $\mathbb{Q}$ are equivalent if and only if they have the same rank, discriminant, signature (as forms over $\mathbb{R}$) and Hasse-Witt invariants ϵ_p (over $\mathbb{Q}_p$ for all primes p).
Now let $\mathcal{C}$ be a smooth conic with a rational point defined by $F(x, y, z) \in \mathbb{Q}[x, y, z]$. Then $F(x, y, z)$ a nondegenerate quadratic form i.e. F is homogeneous of degree 2 and the determinant of the associated matrix is nonzero. Also $F(a, b, c) = 0$ for some $(a, b, c) \neq (0, 0, 0) \in \mathbb{Q}^3$, so F represents 0. In addition, F has the following properties:

- F has rank 3.
- F is equivalent to $\alpha x^2+\beta y^2+\gamma z^2$, with $\alpha, \beta, \gamma \in \mathbb{Q}\backslash\{0\}$, because every quadratic form has an orthogonal basis [6, Ch.4, Thm. 1']. Hence the matrix associated to F has determinant $\alpha\beta\gamma \neq 0$. Multiplying F by $\alpha\beta\gamma$, which may be done as only the locus of F is relevant, gives that the discriminant of F is equal to $\alpha^4\beta^4\gamma^4 \equiv 1 \in \mathbb{Q}^*/\mathbb{Q}^{*^2}$.
- Since F over $\mathbb{Q}$ represents 0, F over $\mathbb{Q}_p$ represents 0 for all primes p. Now because F over $\mathbb{Q}_p$ has rank 3 and discriminant 1, its Hasse-Witt invariants are given by the Hilbert symbol $(-1, -1)_p$ for all p by [6, Ch. 4, Thm. 6]. Explicitly, $\epsilon_2(F) = -1$ and $\epsilon_p(F) = 1$ for all odd primes p.
- Considering F over $\mathbb{R}$, one finds that its Hasse-Witt invariant is $\epsilon_\infty = (-1, -1)_\infty = -1$, hence F has signature $(1, 2)$.

Since F is the quadratic form corresponding to an arbitrary smooth conic in $\mathbb{P}^2$ over $\mathbb{Q}$ with a rational point, every such conic corresponds to a quadratic form of rank 3, discriminant 1, signature $(1, 2)$ and Hasse-Witt invariants $\epsilon_p = (-1, -1)_p$. This implies the desired result. □

Now consider the situation of Poncelet figures with $\mathcal{C}$ and $\mathcal{D}$ smooth conics defined over $\mathbb{Q}$. Suppose $\mathcal{C}$ has a rational point, then by Proposition 2 there exists a linear transformation $A \in GL_3(\mathbb{Q})$ such that $A \cdot \mathcal{C} = \mathcal{P}$, where $\mathcal{P}$ is the standard parabola defined by $yz = x^2$. Hence the figure defined by $\mathcal{C}$ and $\mathcal{D}$ is equivalent to the figure defined by conics $\mathcal{P}$ and $\mathcal{Q} := A\cdot\mathcal{D}$. Hence figures defined by $\mathcal{P}$ and $B\cdot\mathcal{Q}$, where $B \in \{M \in GL_3(\mathbb{Q}) \quad | \quad M\cdot\mathcal{P} = \mathcal{P}\}$ are all equivalent.

Example 1. *Let $\mathcal{C}$: $yz = x^2$. We want to describe all invertible matrices mapping $\mathcal{C}$ to itself. Taking an element*

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \in GL_3(\mathbb{Q}),$$

we require that

$$(ax+by+cz)^2-(dx+ey+fz)(gx+hy+iz)=const\cdot(x^2-yz).$$

Collecting the left hand side together in x, y and z, the following conditions on the variables can be extracted:

$$\begin{aligned} 2ab-dh-eg&=0\\ 2ac-di-fg&=0\\ b^2-eh&=0\\ c^2-fi&=0\\ 2bc-ei-fh&=-a^2+dg. \end{aligned}$$

Here the last equation corresponds to the relation of the coefficients of yz and x^2. Now matrices in $GL_3(\mathbb{Q})$ satisfying these relations fix the parabola $\mathcal{C}$. Using Maple to solve the system of equations, one obtains two general forms of such matrices:

$$\begin{pmatrix} 1 & 0 & c\\ 2ce & e & c^2e\\ 0 & 0 & 1/e \end{pmatrix},\quad \begin{pmatrix} a & b & g(2a-bg)/4\\ b(2a-bg) & b^2 & a^2-abg+b^2g^2/4\\ g & 1 & g^2/4 \end{pmatrix},$$

with $a,b,c,g\in\mathbb{Q}, e\in\mathbb{Q}\backslash\{0\}$ and $a\neq bg$.
Let another conic be given by $\mathcal{D}\colon x^2+(y-\alpha z)^2=\beta z^2$ with $\alpha\in\mathbb{Q},\beta\in\mathbb{Q}\backslash\{0\}$. Then using the first matrix derived above, one finds that Poncelet figures constructed from

$$\mathcal{C}\colon yz=x^2,\qquad \mathcal{D}'\colon (x-cez)^2+(y/e-2cx+c^2ez-\alpha z)^2=\beta e^2z^2$$

with $\alpha, c\in\mathbb{Q},\beta,e\in\mathbb{Q}\backslash\{0\}$ are equivalent to the Poncelet figure defined by $\mathcal{C}$ and $\mathcal{D}$.

Instead of transforming the first conic to the standard parabola, one may transform it to other conics such as a circle, hyperbola or ellips and apply linear transformations that fix this conic. This gives rise to more equivalent Poncelet constructions. To avoid any equivalences one could use a conic without rational points.

2.5 General equation method

This section deals with an approach slightly different from the Poncelet method. The difference is that the Poncelet construction with the two conics is skipped and instead a general equation is used as starting point. This idea has already been mentioned in [5, §6.1]. The general equation is quadratic in two variables:

$$x^2(ay^2+by+c)+x(dy^2+ey+f)+gy^2+hy+i=0, \tag{2}$$

and its coefficients lie in $\mathbb{Q}$. Involutions on this equation can be obtained by letting them fix either x or y. Define $\sigma\colon (x,y)\mapsto(x,y_2)$ with

$$y_2=-y-\frac{bx^2+ex+h}{ax^2+dx+g}$$

and $\tau\colon (x,y) \mapsto (x_2, y)$ with

$$x_2 = \frac{gy^2 + hy + i}{(ay^2 + by + c)x}.$$

Equation (2) can be written as

$$A(x)y^2 + 2B(x)y + C(x) = 0$$

with

$$A(x) = ax^2 + dx + g, \qquad B(x) = \frac{1}{2}(bx^2 + ex + h), \qquad C(x) = cx^2 + fx + i.$$

The change of variables $\tilde{y} = A(x)y + B(x)$ yields

$$\tilde{y}^2 = (\tfrac{b^2}{4} - ac)x^4 + (\tfrac{be}{2} - af - cd)x^3 + (\tfrac{bh}{2} + \tfrac{e^2}{4} - ai - df - cg)x^2 + (\tfrac{eh}{2} - di - fg)x + \tfrac{h^2}{4} - gi$$

and this defines the genus one curve X.

In order to let X have a point $P \in X$ such that $P \notin X(\mathbb{Q})$, consider equation (2) and let $y = 0$. Then the remaining quadratic equation $cx^2 + fx + i = 0$ has discriminant $f^2 - 4ci$. Now let $c = f = i$, so that $x = \zeta_3$ is a solution, where ζ_3 is a primitive third root of unity. Hence the point $(\zeta_3, 0)$ satisfies (2) and it corresponds to the point P_1 on X given by

$$P_1 = (\zeta_3, A(\zeta_3) \cdot 0 + B(\zeta_3)) = \Big(\zeta_3, \frac{b\zeta_3^2 + e\zeta_3 + h}{2}\Big).$$

Now $E := (X, P_1)$ defines an elliptic curve over $\mathbb{Q}(\sqrt{-3})$. Using the formulas for the involutions σ and τ one obtains

$$\sigma\tau(\zeta_3, 0) = \sigma(\zeta_3^2, 0) = \Big(\zeta_3^2, -\frac{b\zeta_3 + e\zeta_3^2 + h}{a\zeta_3 + d\zeta_3^2 + g}\Big),$$

and P_2 is defined to be its corresponding point on X.

Let $\phi\colon X \to E$ be an isomorphism defined over $\mathbb{Q}(\sqrt{-3})$ for which $\phi(P_1) = O \in E$. As noted, if $\phi(P_2)$ has order 9 on E, it follows that σ and τ generate $D_9 \subset \mathrm{Isom}_{\mathbb{Q}}(X)$ and hence the goal is to find parameters for which this happens. In order to do this, division polynomials of E are used. For odd n, the n-th division polynomial has the property that its roots are the x-coordinates of the points $E[n]\backslash\{O\}$. Now consider the polynomial obtained by dividing the 9-th division polynomial by the 3-rd division polynomial. Evaluating the latter polynomial in the x-coordinate of $\phi(P_2)$ and setting it to zero gives an equation that the parameters need to satisfy so that $\phi(P_2)$ has order 9. As the computation of the 9-th division polynomial is rather involved, further restrictions on the parameters are needed. For example, one may take $a = 1$, $c = f = i$ and $b = e = g = 0$. The code executing this calculation can be found in Appendix A.

Choosing the parameters as above, no rational values for the parameters c, d and h were found. Note that in this case there are 3 free parameters. It was found that in the case $a = 1$, $c = f = i$, 4 free parameters makes the computation of the 9-th division polynomial too heavy for Magma. Other options such as $a = 1$, $c = f = i$ and $b = d = h = 0$ were tried in which case the computations could be performed, but no rationals solutions were found.

Another option is to take $g = h = i$, so that $(0, \zeta_3)$ lies on the general equation corresponding to $P_1 := (0, \frac{\sqrt{-3}}{2}g) \in X$. Now let σ be as above and $\tau\colon (x, y) \mapsto (x_2, y)$ with $x_2 = -x - \frac{dy^2+ey+f}{ay^2+by+c}$, then

$$\tau\sigma(0, \zeta_3) = -\frac{d\zeta_3 + e\zeta_3^2 + f}{a\zeta_3 + b\zeta_3^2 + c}.$$

Let P_2 be its corresponding point on X, so that $P_2 = \tau\sigma(P_1)$. Then proceeding as before, $E := (X, P_1)$ is an elliptic curve over $\mathbb{Q}(\sqrt{-3})$ and let $\phi\colon X \to E$ be an isomorphism sending P_1 to $O \in E$. Taking in addition $a = 1$, $e = f = 0$, the image of P_2 is given by

$$\phi(P_2) = \Big(-\frac{4}{9}d^2, \frac{4g}{9}(2d - c - bd + (bd - c)\sqrt{-3})\Big).$$

As this is a rather simple expression, it gives more hope for a solution. However, it turns out that taking 4 parameters still makes the computations too heavy. Fixing in addition one of b, c, d or g makes it possible to do the calculations, but no rational solutions were found.

2.6 A solution

Having failed to find an example of the desired curve by means of a general equation, we return to our initial approach with Poncelet figures. As suggested in §2.4, we start with a conic that has no rational points so that the Poncelet figure is definitely not equivalent to figures exhibited by others. So let $\mathcal{C}$ be the conic defined by $x^2 + y^2 = d$ with $d \in \mathbb{Z}$ such that either $d < 0$ or there exists a prime $p \equiv 3 \bmod 4$ such that $\mathrm{ord}_p(d)$ is odd (see e.g. [1, Thm 3.13]). Let $\mathcal{D}$ be the simple parabola with affine equation $y = (x - \alpha)^2 + \beta$. Lines $y = ax + b$ are tangent to $\mathcal{D}$ if and only if $a^2 + 4a\alpha - 4\beta + 4b = 0$, so an affine model for X is the points (x, y, a, b) with

$$\begin{cases} x^2 + y^2 = d \\ y = ax + b \\ a^2 + 4a\alpha - 4\beta + 4b = 0. \end{cases}$$

Rewriting and solving the equations, one obtains

$$X\colon \quad B^2 = -\frac{1}{16}a^4 - \frac{\alpha}{2}a^3 + (-\alpha^2 + \frac{1}{2}\beta + d)a^2 + 2\alpha\beta a - \beta^2 + d, \tag{3}$$

where the birational equivalence is given by $B = (a^2+1)x - a^3/4 - \alpha a^2 + \beta a$ and the inverse by $x = \frac{4B+a^3+4\alpha a^2-4\beta a}{4a^2+4}$. Formulas for the involutions σ and τ acting on this equation are easily found. The first is given by $\sigma\colon (a, B) \mapsto (a_2, B_2)$, where

$$a_2 = -a - 4\alpha + 4x_2, \qquad B_2 = (a_2^2+1)x_2 - a_2^3/4 - \alpha a_2^2 + \beta a_2,$$

with $x_2 = \frac{4B+a^3+4\alpha a^2-4\beta a}{4a^2+4}$. Note that since τ fixes a, it follows from the equation of X that it maps B to $-B$. So $\tau\colon (a, B) \mapsto (a, -B)$.

Observe that the point $P_1 = (1 : i/4 : 0)$ lies on X. Then P_2 defined as the image of P_1 under $\sigma\tau$ is given by: $P_2 = (-i : -\alpha + i\beta + i/4 : 1)$. Let E be the elliptic curve over $\mathbb{Q}(i)$ defined by (X, P_1) and $\phi\colon X \to E$ be the corresponding isomorphism. Then E is given by

$$E\colon \quad y^2 + 8\alpha xy + 128\alpha dy = x^3 + (32d + 16\beta)x^2 + (256d^2 + 256\beta d + 64d)x.$$

Using 3-rd and 9-th division polynomial of E and evaluating those at the x-coordinate of $\phi(P_2)$ gives a relation of the parameters α, β and d. A point search in Magma gives among others rational triple $(\alpha, \beta, d) = (-1/3, -5/4, 16/9)$. The curve X corresponding to this triple is

$$X\colon \quad y^2 = -9x^4 + 24x^3 + 150x^2 + 120x + 31.$$

This curve has no points over $\mathbb{Q}_2$ and hence no points over $\mathbb{Q}$. So this curve has the desired properties! Note that for the given value of d, conic $\mathcal{C}$ *does* have rational points. So it turns out that the assumption of $\mathcal{C}$ having no rational points is not a necessary requirement. A minimal model for the corresponding elliptic curve is

$$E\colon \quad y^2 = x^3 - 219x - 1654,$$

and the point $P_2 = (-35, 192i) \in E$ has indeed order 9. Note that this elliptic curve is in fact defined over $\mathbb{Q}$. Since we used a $\mathbb{Q}(i)$-point to define E this is not expected in general.

To show that the curve X has no $\mathbb{Q}_2$-rational points, one reasons as follows. First consider points at infinity. Let $\eta = \frac{y}{x^2}, \zeta = \frac{1}{x}$, then the curve is given by

$$\eta^2 = -9 + 24\zeta + 150\zeta^2 + 120\zeta^3 + 31\zeta^4.$$

The points at infinity satisfy $\zeta = 0$, hence $\eta^2 = -9$. Since -9 is not a square in $\mathbb{Q}_2$, the points at infinity are not $\mathbb{Q}_2$-rational. For the remaining points, one may write $x = 2^n \cdot u$ with $u \in \mathbb{Z}_2^*$. Therefore, X has points in $\mathbb{Q}_2$ if and only if

$$-9 \cdot 2^{4n}u^4 + 24 \cdot 2^{3n}u^3 + 150 \cdot 2^{2n}u^2 + 120 \cdot 2^n u + 31 \tag{4}$$

is a square in $\mathbb{Q}_2$. Now distinguish three cases.

- $n < 0$. Writing (4) as $2^{4n} \cdot f$, one has $f \equiv 3 \cdot u^4 \bmod 4$. Since $2^{4n}u^4$ is a square in $\mathbb{Q}_2$ and 3 is not, there are no $\mathbb{Q}_2$-rational solutions.

- $n > 0$. In this case $x \in \mathbb{Z}_2$, so $x \equiv 0 \bmod 2$. Then (4) modulo 4 is equivalent to 3, so there are no solutions over $\mathbb{Q}_2$.
- $n = 0$. This means $x \in \mathbb{Z}_2^*$. Then equation 4 is equivalent to 2 modulo 16 which is not a square in $\mathbb{Q}_2$.

Therefore X has no $\mathbb{Q}_2$-rational points.

3 Invariant theory method

To solve the problem of finding a curve with the desired properties, we now study a method that is completely different from the Poncelet constructions of Chapter 2. The general idea of the approach in this chapter is the following. Start out with polynomials that are invariant under some action of the dihedral group D_9. This can be done using invariant theory. Then try to construct a genus one curve over $\mathbb{Q}$ from those polynomials, which will then contain D_9 in its automorphism group. Succeeding in this, one only needs to make sure the curve has no rational points.

First we will describe the action of D_n on polynomials that we will use. Identify an n-dimensional vector space over $\mathbb{Q}$ with $\sum_{j=1}^{n} \mathbb{Q}x_j$. Viewing the coordinates $x_1, x_2, \ldots, x_n$ as vertices on a regular n-gon, we can describe the action of D_n on this vector space as follows. Firstly, there is a rotation map of order n sending x_j to x_{j+1} (and x_n to x_1). Secondly, the reflection is the reflection of the vertices of the n-gon by the line through x_1. So this switches pairs x_2, x_n and x_3, x_{n-1} and so on. Now the group generated by these two actions defines the action D_n on the polynomial ring $\mathbb{Q}[x_1, \ldots, x_n]$. The following example illustrates our approach.

Example 2. *Consider the dihedral group D_3 ($= S_3$) of order 6, which is the group of all permutations of a three-element set. The (homogeneous) polynomials invariant under the D_3-action for the first 3 degrees are linear combinations of*

- *deg 1:* $x_1 + x_2 + x_3$,
- *deg 2:* $x_1^2 + x_2^2 + x_3^2,\ (x_1 + x_2 + x_3)^2$,
- *deg 3:* $x_1^3 + x_2^3 + x_3^3,\ (x_1 + x_2 + x_3)^3,\ (x_1^2 + x_2^2 + x_3^2)(x_1 + x_2 + x_3)$.

Now (the zero set of) a linear combination F of these polynomials of the same degree over $\mathbb{Q}$ defines a curve in $\mathbb{P}^2$ that is invariant under D_3. If F is non-singular of degree 3, it has genus 1 by the genus-degree formula. For example

$$F: \quad x_1^3 + x_2^3 + x_3^3 + \lambda(x_1^2 + x_2^2 + x_3^2)(x_1 + x_2 + x_3)$$

with $\lambda \in \mathbb{Q}$ defines such a curve. However, it does have rational points such as $(1 : -1 : 0)$.

This example motivates the search for all invariant polynomials under the action of the dihedral group. A useful tool for this is the Molien series. This is a power series $M(t) = \sum_d n_d t^d$, where n_d is the number of linearly independent homogeneous polynomials of degree d that are invariant for the associated group G. Molien's theorem [2, Thm. 8.1.1] states that this series is given by

$$M(t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - t[g])},$$

where $[g]$ is a linear representation of $g \in G$ on a finite-dimensional vector space.

Denote the elements of the polynomial ring $\mathbb{Q}[x_1, \ldots, x_n]$ of degree d by $\mathbb{Q}[x_1, \ldots, x_n]_d$ and its elements invariant under D_n by $\mathbb{Q}[x_1, \ldots, x_n]^{D_n}$. To get a full description of $\mathbb{Q}[x_1, \ldots, x_n]^{D_n}$, generators for it should be found. It follows from Hilbert's finiteness theorem [2, Thm. 5.0.11] that $\mathbb{Q}[x_1, \ldots, x_n]^{D_n}$ is finitely generated. Slightly better is Noether's bound [2, Thm. 5.1.1], which applied to this case says that $\mathbb{Q}[x_1, \ldots, x_n]^{D_n}$ is generated by polynomials of degree at most the number of elements of D_n.

3.1 A degree 5 example

As the complexity of computations quickly increases for larger dihedral groups, we present our attempts of creating a genus one curve with $D_5 \subset \mathrm{Isom}_{\mathbb{Q}}(X)$ and $X(\mathbb{Q}) = \emptyset$ in this section. We denote by σ the rotation map of order 5 and by τ the reflection map of order 2. The group D_5 is generated by σ and τ and it has the four conjugacy classes $\{id\}, \{\sigma, \sigma^4\}, \{\sigma^2, \sigma^3\}, \{\tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \tau\sigma^4\}$. Since $\det(I - t[g])$ is constant on a conjugacy class, this can be used to compute the Molien series. Computing this determinant for each conjugacy class yields

$$M(t) = \frac{1}{10}\left(\frac{1}{(1-t)^5} + \frac{2}{1-t^5} + \frac{2}{1-t^5} + \frac{5}{-(t-1)^3(t+1)^2}\right)$$

and writing this out as a series expansion one obtains

$$M(t) = 1 + t + 3t^2 + 5t^3 + 10t^4 + 16t^5 + O(t^6).$$

Hence $\mathbb{Q}[x_1, \ldots x_5]_1^{D_5}$ has one linearly independent element, $\mathbb{Q}[x_1, \ldots x_5]_2^{D_5}$ has three etc. Up to degree 3, (nonunique) generators of $\mathbb{Q}[x_1, \ldots x_5]_d^{D_5}$ are given in the table below.

Deg 1	Deg 2	Deg 3
$p_1 := \sum_{i=1}^{5} x_i$	$p_2 := \sum_{i=1}^{5} x_i^2$	$p_3 := \sum_{i=1}^{5} x_i^3$
	$q_2 := \sum_{i=1}^{5}\sum_{j>i}^{5} x_i x_j$	$q_3 := \sum_{i=1}^{4} x_i^2 x_{i+1} + x_1^2 x_5 + \sum_{i=1}^{4} x_i x_{i+1}^2 + x_1 x_5^2$
	$r_2 := \sum_{i=1}^{4} x_i x_{i+1} + x_1 x_5$	$r_3 := \sum_{i=1}^{5}\sum_{j\neq i}^{5} x_i x_j^2$
		$s_3 := x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_1x_4x_5 + x_1x_2x_5$
		$t_3 := \sum_{i=1}^{5}\sum_{j>i}^{5}\sum_{k>j}^{5} x_i x_j x_k$

Table 2: Generators of $\mathbb{Q}[x_1, \ldots x_5]_d^{D_5}$ for $d = 1, 2, 3$.

Now in order to find generators of $\mathbb{Q}[x_1, \ldots, x_5]^{D_5}$ one may start with the ideal (p_1) and repeatedly add generators of $\mathbb{Q}[x_1, \ldots x_5]_d^{D_5}$ for $d \geq 2$ without adding superfluous ones. Note that $q_2 \in (p_1, p_2)$. Adding r_2 and p_3 as well, one can show that (p_1, p_2, r_2, p_3) contains

q_3, r_3, s_3 and t_3. It is possible to find all the generators in this way, since by the Noether's degree bound the generators have degree at most 10. However, since there are 111 linearly independent invariant polynomials of degree 10, this is tedious work and will not be done.

The next step is to search for polynomials that define a genus one curve. Since the polynomials define points in $\mathbb{P}^4$, the zero set of 3 polynomials in general defines a curve. For simplicity, fix the first equation to be p_1. So the goal is to find polynomials f_1, f_2 defining sets in $\mathbb{P}^4$ such that $C\colon Z(p_1, f_1, f_2)$ defines a genus one curve. Note that equivalently one may try to find polynomials f_1', f_2' defining sets in $\mathbb{P}^3$ such that $Z(f_1', f_2')$ is a genus one curve, where f_i' is obtained from f_i by elimination one of its coordinates with p_1 for $i = 1, 2$. The arithmetic genus of the latter curve is given by

$$g = 1 + \frac{1}{2} d_1 d_2 (d_1 + d_2 - 4),$$

where d_1 and d_2 are the degrees of f_1' and f_2' respectively. Now since $\deg(f_i) = \deg(f_i') = d_i$ for $i = 1, 2$, this can be used to find polynomials f_1 and f_2. Observe that $d_i \geq 2$ for $i = 1, 2$, because p_1 is the only generator of $\mathbb{Q}[x_1, \ldots, x_5]_1^{D_5}$.

Taking $d_1 = d_2 = 2$ results in a curve with arithmetic genus 1. However, C defines a singular curve for any choice of f_1, f_2 (provided that $Z(p_1, f_1, f_2)$ defines a curve at all) in this case. Hence at least one of f_1, f_2 has degree more than 2. This leads to a curve with arithmetic genus bigger than 1 so it should have singularities. For each singularity, the genus drops with the quantity $r(r-1)/2$, where r is the order of vanishing of the singular point. Let us characterize the singularities on $C\colon Z(p_1, f_1, f_2)$. Note that since points of C are invariant under D_5, singular points of C occur in orbits. More concretely, if P is a singular point on C, $\sigma(P), \ldots, \sigma^4(P)$ are singular and the image under τ of each of these as well. So in general a singularity implies the existence of 9 more singularities. Hence, it is useful to consider points that are invariant under σ or τ.

- Points invariant under σ are $(1 : \zeta_5 : \zeta_5^2 : \zeta_5^3 : \zeta_5^4)$ with ζ_5 a fifth root of unity. Since points of C lie in the zero set of p_1, only the four points with $\zeta_5 \neq 1$ have this property.

- Points invariant under τ are of the form $(1 : a : b : b : a), (0 : a : b : b : a)$ or $(0 : a : b : -b : -a)$ with $a, b \in \overline{\mathbb{Q}}$ and they lie in $Z(p_1)$ if the sum of their coordinates is zero. Note that points invariant under $\tau\sigma, \ldots, \tau\sigma^4$ satisfy the same condition but with shifted coordinates.

Observe that no points of C are invariant under both σ and τ. Hence points invariant under σ come in pairs and points invariant under τ come in 5-tuples. This makes life rather difficult, since for example taking $d_1 = 2$ and $d_2 = 3$ gives an arithmetic genus of 4, which cannot be reduced to 1 with singularities.

Searching for appropriate polynomials of larger degree, a genus one curve was found in the case $d_1 = 2$ and $d_2 = 5$. It is given by $Z(p_1, p_2 + 2r_2, p_5 - 5q_5)$, where $p_5 := \sum_{i=1}^{5} x_i^2$ and

$$q_5 := x_1^2x_2^3 + x_2^2x_3^3 + x_3^2x_4^3 + x_4^2x_5^3 + x_5^2x_1^3 + x_2^2x_1^3 + x_3^2x_2^3 + x_4^2x_3^3 + x_5^2x_4^3 + x_1^2x_5^3.$$

The curve has singular points $(1 : -1 : 0 : 0 : 0), (0 : 1 : -1 : 0 : 0), (0 : 0 : 1 : -1 : 0), (0 : 0 : 0 : 1 : -1)$ and $(1 : 0 : 0 : 0 : -1)$ all with order of vanishing equal to 3. It has, however, many (nonsingular) rational points so it does not satisfy all desired properties.

In conclusion, we find that in the D_5 case it is rather difficult to find curves of genus 1 with this method. Even if we succeed it is not guaranteed that is has no rational points. As the complexity of the problem only increases for larger dihedral groups, the method has not been tried for the D_9-group.

4 Twisting method

In this section we present a third method for solving the problem of this thesis. Starting with an elliptic curve $E/\mathbb{Q}$ containing D_9 in its automorphism group over a quadratic extension of $\mathbb{Q}$, the hope is to find a quadratic twist X of E over $\mathbb{Q}$ such that X has no rational points and such that the automorphisms in D_9 yield automorphisms on X defined over $\mathbb{Q}$. The method is explained in more detail below. Along the way, conditions for arriving at the desired setup are developed.

Let k be a field. Remember that a twist of X/k is a smooth curve X'/k such that X and X' are isomorphic over $\bar{k}$. For our purposes a quadratic twist over the rationals is needed. For $d \in \mathbb{Q}\backslash\mathbb{Q}^2$, a quadratic twist of X over $\mathbb{Q}$ is a curve $X'/\mathbb{Q}$ isomorphic to X over $\mathbb{Q}(\sqrt{d})$. It is called a nontrivial quadratic twist if moreover X is not isomorphic to E over $\mathbb{Q}$. Start with an elliptic curve $E/\mathbb{Q}$ and consider its function field $\mathbb{Q}(E)$. From now

on, let $d \in \mathbb{Q}\backslash\mathbb{Q}^2$. Then $\mathbb{Q}(E) \subset \mathbb{Q}(\sqrt{d}, E)$ is a field extension of degree 2. Now let σ be an involution on E and define $\tilde{\sigma}$ to be the induced map of σ on $\mathbb{Q}(\sqrt{d}, E)$ composed with the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. The curve X of our interest has function field given by

$$\mathbb{Q}(X) = \mathbb{Q}(\sqrt{d}, E)^{<\tilde{\sigma}>},$$

where $\mathbb{Q}(\sqrt{d}, E)^{<\tilde{\sigma}>}$ are the elements of $\mathbb{Q}(\sqrt{d}, E)$ that are invariant under $\tilde{\sigma}$. Since $\tilde{\sigma}$ is an involution on $\mathbb{Q}(\sqrt{d}, E)$ it follows that $\mathrm{Gal}(\mathbb{Q}(\sqrt{d}, E)/\mathbb{Q}(\sqrt{d}, E)^{<\tilde{\sigma}>})$ has two elements and hence that

$$\mathbb{Q}(\sqrt{d}, E)^{<\tilde{\sigma}>} \subset \mathbb{Q}(\sqrt{d}, E)$$

is a field extension of degree 2. Since the element $\sqrt{d} \notin \mathbb{Q}(X)$ has minimal polynomial of degree 2 over $\mathbb{Q}(X)$, it follows that $\mathbb{Q}(\sqrt{d}, X) = \mathbb{Q}(\sqrt{d}, E)$. Therefore, $X \cong E$ over $\mathbb{Q}(\sqrt{d})$, so X is a quadratic twist of E. The following example illustrates this theoretic method and its implications.

4.1 An example

Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = x^3 + ax^2 + bx$, so that $(0, 0) \in E$. Let σ be the involution on E given by

$$(x, y) \mapsto (0, 0) - (x, y) = (b/x, by/x^2).$$

Now let $d \in \mathbb{Q}\backslash\mathbb{Q}^2$ and define $\tilde{\sigma}$ on $\mathbb{Q}(\sqrt{d}, E)$ as

$$\tilde{\sigma} : \begin{cases} x \mapsto b/x \\ y \mapsto by/x^2 \\ \sqrt{d} \mapsto -\sqrt{d}. \end{cases}$$

So restricted to $\mathbb{Q}(E)$ $\tilde{\sigma}$ acts as σ and restricted to $\mathbb{Q}(\sqrt{d})$ it acts as the nontrivial automorphism in $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$.

In order to find the curve X, one needs to find the elements of $\mathbb{Q}(\sqrt{d}, E)$ that are invariant under $\tilde{\sigma}$. It is easy to see that the element $\eta := x + b/x$ has this property. To find the other invariants, one can consider $\mathbb{Q}(\sqrt{d}, E)$ as a vector space over $\mathbb{Q}(\eta)$ and take $\{1, x, \sqrt{d}, x\sqrt{d}, y, xy, y\sqrt{d}, xy\sqrt{d}\}$ as its basis. Computing the action of $\tilde{\sigma}$ on these basis vectors, one finds, apart from η, the invariants $\xi := \sqrt{d}(x - b/x), \rho := y/x$ and $\chi = \sqrt{d}(y - by/x^2)$. Note that

$$\eta = \frac{x^3 + bx}{x^2} = \frac{y^2 - ax^2}{x^2} = \rho^2 - a,$$

so $\eta \in \mathbb{Q}(\rho)$, i.e. η is a rational function of ρ. Also $\chi = \xi \cdot \rho$ and hence ξ and ρ generate the set of invariants. It is not hard to see that ξ and ρ cannot be written as a rational function of the other and therefore $\mathbb{Q}(\sqrt{d}, E)^{<\tilde{\sigma}>} = \mathbb{Q}(\xi, \rho)$.

The next step is finding the curve X for which $\mathbb{Q}(X) = \mathbb{Q}(\sqrt{d}, E)^{<\tilde{\sigma}>}$. A minimal polynomial of x over $\mathbb{Q}(\rho)$ is $Y^2 + (a - \rho^2)Y + b$ and since $\mathbb{Q}(\rho) \neq \mathbb{Q}(\rho, x)$ (e.g. σ fixes ρ but not x), $\mathbb{Q}(\rho) \subset \mathbb{Q}(\rho, x)$ is a degree 2 extension. One gets the following chain of inclusions where all extensions are of degree 2:

$$\mathbb{Q}(\rho) \subset \mathbb{Q}(\rho, x) \subset \mathbb{Q}(\sqrt{d}, \rho, x).$$

Note that $\mathbb{Q}(\sqrt{d}, \rho, x) = \mathbb{Q}(\sqrt{d}, x, y) = \mathbb{Q}(\sqrt{d}, E)$. As remarked in the introduction of this chapter, $\mathbb{Q}(\sqrt{d}, E)^{<\tilde{\sigma}>} \subset \mathbb{Q}(\sqrt{d}, E)$ is a degree 2 extension and hence $\mathbb{Q}(\rho) \subset \mathbb{Q}(\sqrt{d}, E)^{<\tilde{\sigma}>}$ has degree 2. The element $\xi \in \mathbb{Q}(\sqrt{d}, E)^{<\tilde{\sigma}>}$ has minimal polynomial

$$m_\xi(Y) = Y^2 - d\rho^4 + 2ad\rho^2 - a^2d + 4bd$$

and hence this defines the function field of X. So we found an equation for X for $a, b \in \mathbb{Q}, d \in \mathbb{Q}\backslash\mathbb{Q}^2$ and since X is isomorphic to E over $\mathbb{Q}(\sqrt{d})$ it has genus 1.

In the next section we will see that this example cannot result in a curve X with the desired properties. The reason is that $(0, 0) \in E$ used to define σ has order 2 and therefore E cannot have a point of order 9 over $\mathbb{Q}(\sqrt{d})$.

4.2 Conditions on the setup

The example in the previous section shows that we can find a twist X of some initial elliptic curve E. Since the goal is to find a very specific curve, this section deals with the conditions on the setup that arise from the desired properties of X.

One condition on X is that it must contain the dihedral group of order 18 in its automorphism group over $\mathbb{Q}$. In particular there is a $\beta \in \mathrm{Isom}_{\mathbb{Q}}(X)$, with $\mathrm{ord}(\beta) = 9$. Since

$X \cong E$ over $\mathbb{Q}(\sqrt{d})$, a necessary condition on E thus is that there is an $\alpha \in \mathrm{Isom}(E)$ with $\mathrm{ord}(\alpha) = 9$. The map α can have only one form as is shown in the next Lemma.

Lemma 2. *Let $E/\mathbb{Q}$ be an elliptic curve and let $\alpha \in \mathrm{Isom}(E)$ have order 9. Then α is the translation-by-Q map with $\mathrm{ord}(Q) = 9$.*

Proof. It follows from Proposition 1 that α can be uniquely written as $\alpha = \tau_Q \circ \phi$, where τ_Q is the translation-by-Q map and $\phi \in \mathrm{Aut}(E)$. Because of [7, Prop. 10.1, Ch. 3], $\mathrm{Aut}(E)$ is a cyclic group with $2, 4$ or 6 elements depending on the j-invariant of E. If one shows that in all cases α has order 9 implies $\phi = id$ and Q has order 9, the result follows.

- $j(E) \neq 0, 1728$. Then E has two automorphisms given by id and $[-1]$. If $\phi = [-1]$, $\alpha^2 = \tau_Q \circ [-1] \circ \tau_Q \circ [-1] = \tau_{Q-Q} \circ ([-1])^2 = id$. So α has order 2 in this case. Therefore, α having order 9 implies $\phi = id$ and $\alpha = \tau_P$ with Q of order 9.

- $j(E) = 1728$. Now E has four automorphisms and they are given by id, $[-1]$, $[i]$ and $[-i]$. Suppose $\phi = [i]$, then $\alpha^2 = \tau_Q \circ [i] \circ \tau_Q \circ [i] = \tau_{Q+[i]Q} \circ [-1]$. Therefore $\alpha^4 = \tau_{Q+[i]Q} \circ [-1] \circ \tau_{Q+[i]Q} \circ [-1] = \tau_{Q+[i]Q-[i]Q-Q} \circ ([-1])^2 = id$. Similarly, one shows that $\alpha^4 = id$ in case $\phi = [-i]$. We conclude that ϕ must be the identity map and Q has order 9.

- $j(E) = 0$. In this case $\mathrm{Aut}(E)$ has 6 elements given by the multiplication by sixth roots of unity. Suppose $\phi = [\zeta_6]$, then $\alpha^2 = \tau_Q \circ [\zeta_6] \circ \tau_Q \circ [\zeta_6] = \tau_{Q+[\zeta_6]Q} \circ ([\zeta_6])^2$ and $\alpha^3 = \tau_{Q+[\zeta_6]Q} \circ ([\zeta^6])^2 \circ \tau_Q \circ [\zeta_6] = \tau_{Q+[\zeta_6]Q+[\zeta_6]^2Q} \circ [-1]$. Hence $\alpha^6 = \tau_{Q+[\zeta_6]Q+[\zeta_6]^2Q} \circ [-1] \circ \tau_{Q+[\zeta_6]Q+[\zeta_6]^2Q} \circ [-1] = id$. Similarly, one can show that $\alpha^3 = id$ if $\phi = ([\zeta^6])^2$ and $\phi = ([\zeta^6])^4$, and $\alpha^6 = id$ if $\phi = ([\zeta^6])^5$. Therefore, ϕ must be id and $\mathrm{ord}(Q) = 9$.

□

From Lemma 2 it follows that E should have a point Q of order 9 so that the translation-by-Q map, denoted by τ_Q, has order 9 on E. Now consider the following commutative diagram in which $\psi \colon E \to X$ is an isomorphism over $\mathbb{Q}(\sqrt{d})$

$$\begin{array}{ccc} E & \xrightarrow{\psi} & X \\ \downarrow{\scriptstyle \tau_Q} & & \downarrow{\scriptstyle \tau'} \\ E & \xrightarrow{\psi} & X \end{array}$$

The map $\tau' := \psi \tau_Q \psi^{-1} \colon X \to X$ should be defined over $\mathbb{Q}$. If also $\sigma' := \psi \sigma \psi^{-1} \colon X \to X$ is defined over $\mathbb{Q}$, then σ' and τ' generate $D_9 \subset \mathrm{Isom}_{\mathbb{Q}}(X)$. We shall return to this matter later in this section. First conditions on when σ' and τ' are defined over $\mathbb{Q}$ are presented.

Proposition 3. *Let E be an elliptic curve, $\tau_Q \colon E \to E$ be the translation map by $Q \in E(\overline{\mathbb{Q}})$ and σ be an involution on E defined by $P \mapsto R - P$, with $R \in E(\overline{\mathbb{Q}})$. Let X be a quadratic twist of E such that $\mathbb{Q}(X) = \mathbb{Q}(\sqrt{d}, E)^{<\tilde{\sigma}>}$. Let γ be the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ and its action on a point $P \in E(\mathbb{Q}(\sqrt{d}))$ is denoted by P^γ. Then*

1. *σ' is defined over $\mathbb{Q}$ if and only if $R \in E(\mathbb{Q})$.*

2. *τ' is defined over $\mathbb{Q}$ if and only if $Q \in E(\mathbb{Q}(\sqrt{d}))$ and $Q^\gamma = -Q$.*

Proof. Since X is a twist of E, it is given by a Galois 1-cocycle, i.e. an element of the cohomology group $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Isom}(E))$. We claim that this 1-cocycle ξ is the homomorphism

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\text{res}} \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \longrightarrow \mathrm{Isom}(E)$$

where the second arrow sends γ to involution σ. This homomorphism corresponds to (see e.g. [7, Thm X.2.2c]) the twist with function field $\mathcal{F}$, where $\mathcal{F}$ is the field of invariants of $\overline{\mathbb{Q}}(E)$ under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ twisted by ξ. Hence $\mathcal{F}$ consists of functions $f \in \overline{\mathbb{Q}}(E)$ for which $f = f^\delta \xi_\delta$ for all $\delta \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Now for automorphisms that act trivially on $\mathbb{Q}(\sqrt{d})$ this implies $f = f^\delta$ and for the automorphisms that restrict to γ on $\mathbb{Q}(\sqrt{d})$ this implies $f = \sigma^\#(f^\delta)$, where $\sigma^\#$ is the involution on $\mathbb{Q}(E)$ induced by σ. Hence, $\mathcal{F} = \mathbb{Q}(\sqrt{d}, E)^{<\tilde{\sigma}>} = \mathbb{Q}(X)$, proving the claim.

Since X is a twist of E it follows that ([7, Thm X.2.2] again) there is an isomorphism $\psi\colon E \to X$ over $\mathbb{Q}(\sqrt{d})$ such that $\xi = \psi^{-1}\psi^\gamma$. Therefore, ψ can be chosen such that for all $\delta \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ one has

$$\psi^\delta = \begin{cases} \psi & \text{if } \delta \text{ fixes } \sqrt{d}, \\ \psi\sigma & \text{else.} \end{cases}$$

Now for the first assertion, note that σ' being defined over $\mathbb{Q}$ is equivalent to saying that for all $\delta \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and all $P \in X(\overline{\mathbb{Q}})$ it holds that $\sigma'(P)^\delta = \sigma'(P^\delta)$. Writing this out, it is equivalent to claiming

$$\psi^\delta \sigma^\delta (\psi^\delta)^{-1} \delta = \psi\sigma\psi^{-1}\delta. \tag{5}$$

Elements $\delta \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that fix $\sqrt{d}$ satisfy $\psi^\delta = \psi$. Hence such automorphisms are defined over $\mathbb{Q}$ if and only if $\sigma^\delta = \sigma$. For automorphisms that do not fix $\sqrt{d}$ one has $\psi^\delta = \psi\sigma$, and hence equation 5 becomes $\psi\sigma\sigma^\delta\sigma^{-1}\psi^{-1}\delta = \psi\sigma\psi^{-1}\delta$. Since $\sigma^2 = id$, this reduces to the question if $\sigma^\delta = \sigma$. Therefore, σ' is defined over $\mathbb{Q}$ if and only if $\sigma^\delta = \sigma$ for all $\delta \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, i.e. if and only if σ is defined over $\mathbb{Q}$. Since σ is given by $P \mapsto R - P$, this is equivalent to $R \in E(\mathbb{Q})$.

Similarly, τ' is defined over $\mathbb{Q}$ if and only if for all $\delta \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and all $P \in X(\overline{\mathbb{Q}})$ it holds that $\tau'(P)^\delta = \tau'(P^\delta)$. This can be rewritten as

$$\psi^\delta \tau_{Q^\delta} (\psi^\delta)^{-1} \delta = \psi\tau_Q\psi^{-1}\delta. \tag{6}$$

In the case $\delta \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ fixes $\sqrt{d}$, this reduces to the question if $\tau_{Q^\delta} = \tau_Q$. This holds if and only if $Q^\delta = Q$, and requiring this for all automorphisms fixing $\sqrt{d}$ is equivalent to asking $Q \in E(\mathbb{Q}(\sqrt{d}))$. If δ does not fix $\sqrt{d}$, equation 6 may be rewritten as $\psi\sigma\tau_{Q^\delta}\sigma^{-1}\psi^{-1}\delta = \psi\tau_Q\psi^{-1}\delta$ or after canceling terms as $\sigma\tau_{Q^\delta}\sigma = \tau_Q$. Now plugging in any point of E in this equation, this is equivalent to the question whether Q equals $-Q^\delta$. Since γ is the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$, this holds for all δ not fixing $\sqrt{d}$ if and only if $Q^\gamma = -Q$. This proves the second assertion. □

We have derived a setup in which the twist X of E admits two maps σ' and τ' defined over $\mathbb{Q}$. In fact, under these conditions X contains the dihedral group of order 18 in its automorphism group over $\mathbb{Q}$.

Lemma 3. *Let E be an elliptic curve, $\sigma\colon P \mapsto R-P$ be an involution on E, s.t. $R \in E(\mathbb{Q})$. Let τ_Q be translation by $Q \in E(\mathbb{Q}(\sqrt{d}))$ with $Q = -Q^\gamma$ and ord$(Q) = 9$. Let X be a quadratic twist of E such that $\mathbb{Q}(X) = \mathbb{Q}(\sqrt{d}, E)^{<\tilde{\sigma}>}$. Then $D_9 \subset \mathrm{Aut}_{\mathbb{Q}}(X)$ and it is generated by σ' and τ'.*

Proof. Note that σ, τ are automorphisms over $\mathbb{Q}$ on E with $\mathrm{ord}(\sigma) = 2$, $\mathrm{ord}(\tau) = 9$ and

$$\begin{aligned}\sigma\tau\sigma(x,y) &= \sigma\tau(P-(x,y)) = \sigma(P+Q-(x,y))\\ &= P-(P+Q-(x,y)) = (x,y)-Q = \tau^{-1}(x,y).\end{aligned}$$

Therefore, σ and τ generate $D_9 \subset \mathrm{Aut}_{\mathbb{Q}}(E)$. From Proposition 3 it follows that σ' and τ' are defined over $\mathbb{Q}$. Furthermore, $\mathrm{ord}(\sigma') = 2$, $\mathrm{ord}(\tau') = 9$ and

$$\begin{aligned}\sigma'\tau'\sigma' &= (\psi^{-1}\sigma\psi)(\psi^{-1}\tau\psi)(\psi^{-1}\sigma\psi)\\ &= \psi^{-1}(\sigma\tau\sigma)\psi = \psi^{-1}\tau^{-1}\psi = (\psi^{-1}\tau\psi)^{-1} = \tau'^{-1}.\end{aligned}$$

Hence $< \sigma', \tau' >= D_9 \subset \mathrm{Aut}_{\mathbb{Q}}(X)$ as desired. □

The other condition on X is that it must not have rational points. So the question arises which points of $E(\overline{\mathbb{Q}})$ will lead to a rational point on X after the twisting procedure. This is done in the next Lemma.

Lemma 4. *Let E be an elliptic curve, σ be an involution on E. Let X be a quadratic twist of E such that $\mathbb{Q}(X) = \mathbb{Q}(\sqrt{d}, E)^{<\tilde{\sigma}>}$. Let $P \in E(\overline{\mathbb{Q}})$ be a point and let $\psi\colon E \xrightarrow{\sim} X$ be an isomorphism over $\mathbb{Q}(\sqrt{d})$. Then $\psi(P) \in X(\mathbb{Q})$ if and only if $P \in E(\mathbb{Q}(\sqrt{d}))$ and $\sigma(P) = P^\gamma$. Here γ is the generator of Gal$(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$.*

Proof. Since $X \cong E$ over $\mathbb{Q}(\sqrt{d})$, it holds that $X(\mathbb{Q}(\sqrt{d})) \cong E(\mathbb{Q}(\sqrt{d}))$. Therefore, points $P \in E(\mathbb{Q}(\sqrt{d}))$ satisfy $\psi(P) \in X(\mathbb{Q}(\sqrt{d}))$ and only those P can possibly have $\psi(P) \in X(\mathbb{Q})$. It remains to show that for $P \in E(\mathbb{Q}(\sqrt{d}))$ it holds that, $\psi(P) \in X(\mathbb{Q})$ if and only if $\sigma(P) = P^\gamma$. As noted in the proof of Proposition 3, ψ can be chosen so that $\psi^{-1}\psi^\gamma = \sigma$. Now since $\sigma^\gamma = \sigma$, it follows that

$$\sigma(P)^\gamma = \sigma(P^\gamma) = \psi^{-1}\psi^\gamma(P^\gamma) = \psi^{-1}(\psi(P))^\gamma.$$

This is equal to $\psi^{-1}\psi(P) = P$ if and only if $\psi(P) \in X(\mathbb{Q})$ and hence the result follows from acting by γ on both sides of the equation. □

This condition may help to build a setup so that X does not have rational points. In the example of section 4.1, we find that points $P \in E(\mathbb{Q}(\sqrt{d}))$ satisfying $(0,0) - P = P^\gamma$ give

rise to a rational point on X. Writing $P = (k + l\sqrt{d}, m + n\sqrt{d})$ with $k, l, m, n \in \mathbb{Q}$, then P comes from $X(\mathbb{Q})$ if and only if

$$\Big(\frac{b}{k + l\sqrt{d}}, \frac{m + n\sqrt{d}}{(k + l\sqrt{d})^2}\Big) = (k - l\sqrt{d}, m - n\sqrt{d}).$$

So taking $b \neq k^2 - dl^2$ with $k, l \in \mathbb{Q}$ makes sure this does not happen.

Before stating the exact conditions on the elliptic curve E, we need to make one more observation.

Lemma 5. *Let $E/\mathbb{Q}$ be an elliptic curve with points $O \neq P \in E(\mathbb{Q})$ and $Q \in E(\mathbb{Q}(\sqrt{d}))$ of order 9 such that $Q^\gamma = -Q$. Then P is a point of infinite order.*

Proof. Since $\mathrm{char}(\mathbb{Q}) \neq 2$, E may be written in Weierstrass form as $y^2 = x^3 + a_2x^2 + a_4x + a_6$. Suppose $P \neq O$ in $E(\mathbb{Q})$ has finite order. Because $Q \in E(\mathbb{Q}(\sqrt{d}))$ has order 9, it follows from [8, Thm 1] that the torsion subgroup $E(\mathbb{Q}(\sqrt{d}))$ is cyclic of order 9 or 18. Suppose it is cyclic of order 9. Then $P \in E(\mathbb{Q})$ is a multiple of Q, so $P = nQ$ for some positive integer n. Then $P = P^\gamma = (nQ)^\gamma = -nQ$, so $2nQ = O$. This implies that 9 divides n and hence that $P = O$. This contradicts our assumption, so we conclude that $E(\mathbb{Q}(\sqrt{d}))$ is cyclic of order 18. Therefore, there exists a point over $E(\mathbb{Q}(\sqrt{d}))$ of order 2 and there is only one such point as the cyclic group contains one point of order 2. Denoting this point by T, we must therefore have that $T = T^\gamma$, so T is a rational point on E. Hence $T = (a, 0)$ with $a \in \mathbb{Q}$. Now consider the quadratic twist $E^{(d)}$ of E given by $E^{(d)}\colon y^2 = x^3 + da_2x^2 + d^2a_4x + d^3a_6$ and the map $\phi\colon E \to E^{(d)}$, $(x, y) \mapsto (dx, d\sqrt{d}y)$. Then $E^{(d)}$ contains the points $\phi(T) = (ad, 0) \in E^{(d)}(\mathbb{Q})$ and $\phi(Q)$. Note that on E the property $Q^\gamma = -Q$ is equivalent to $Q = (b, c\sqrt{d})$ for some $b, c \in \mathbb{Q}$. Hence $\phi(Q) = (bd, cd^2) \in E^{(d)}(\mathbb{Q})$ and it has order 9. But this contradicts Mazur's result [4] on the possible torsion of an elliptic curve over $\mathbb{Q}$, hence P cannot have finite order.

□

We can now formulate the exact setup under which the quadratic twist X of E has the desired properties. The goal is to find an elliptic curve $E/\mathbb{Q}$ with

- $Q \in E(\mathbb{Q}(\sqrt{d}))$ of order 9 such that $Q^\gamma = -Q$,
- $R \in E(\mathbb{Q})$ of infinite order,
- no points $P \in E(\mathbb{Q}(\sqrt{d}))$ satisfying $P + P^\gamma = R$.

An approach for this problem is considering the quadratic twist $E^{(d)}$ of E. Note that an equivalent goal is to find $E^{(d)}$ with

- $\widetilde{Q} \in E^{(d)}(\mathbb{Q})$ of order 9,
- $\widetilde{R} \in E^{(d)}(\mathbb{Q}(\sqrt{d}))$ of infinite order,

- no points $P \in E^{(d)}(\mathbb{Q}(\sqrt{d}))$ satisfying $P + P^\gamma = \widetilde{R}$,

since on the quadratic twist E of $E^{(d)}$ it automatically holds that $Q^\gamma = -Q$. This observation allows us to start with an elliptic curve that is known to have a rational point of order 9, which can be found in the LMFDB.

4.3 Construction of a twist

In this section we present a curve with the desired properties that was found with the approach described in this chapter. The corresponding code can be found in appendix B. As mentioned at the end of section 4.2, we may start with an elliptic curve $E^{(d)}$, with $\widetilde{Q} \in E(\mathbb{Q})$ of order 9 and $\widetilde{R} \in E^{(d)}(\mathbb{Q}(\sqrt{d}))$ of infinite order. Also, we did not need the condition of having no points $P \in E(\mathbb{Q}(\sqrt{d}))$ satisfying $P + P^\gamma = \widetilde{R}$ because a twist without rational points was quickly found.

Consider the elliptic curve $E^{(d)}\colon y^2 + xy + y = x^3 - x^2 - 14x + 29$ which has a point $\widetilde{Q} := (9, 19)$ of order 9. Let $d = 13$, then one has $\widetilde{R} := (0, \frac{-1\pm\sqrt{13}}{2}) \in E(\mathbb{Q}(\sqrt{13}))$. Taking the quadratic twist $E = E^{(d)(13)}$ gives

$$E\colon y^2 = x^3 - \frac{39}{4}x^2 - \frac{4563}{2}x + \frac{257049}{4},$$

with $R = (0, \frac{507}{2}) \in E(\mathbb{Q})$ of infinite order and $Q = (117, 247\sqrt{13})$ of order 9 satisfying $Q^\gamma = -Q$. Now let the involution σ be given by $(x, y) \mapsto (0, \frac{507}{2}) + (x, -y)$. For finding the invariants of $\mathbb{Q}(\sqrt{13}, E)$ under $\tilde{\sigma}$, Lemma 2.1 in [3] is a useful result. Applied to this problem it states that $\mathbb{Q}(E)^{<\sigma>} = \mathbb{Q}(\eta)$, where η is any non-constant function in the $\mathbb{Q}$-vector space $L(O + (0, \frac{507}{2}))$. To find such η, note that the function $1/x$ has divisor $2O - (0, \frac{507}{2}) - (0, -\frac{507}{2})$. Since the function $y + 507/2$ has a pole of order 3 in O, no other poles and a zero at $(0, -\frac{507}{2})$, it follows that

$$\eta := \frac{2y + 507}{2x}$$

is a non-constant function in $L(O + (0, \frac{507}{2}))$. So for this η, $\mathbb{Q}(E)^{<\sigma>} = \mathbb{Q}(\eta)$.
Since σ has order 2, it holds that $[\mathbb{Q}(E)\colon \mathbb{Q}(\eta)] = 2$. Hence every element of $\mathbb{Q}(E)$ not invariant under σ has a minimal polynomial of degree 2 over $\mathbb{Q}(\eta)$. The minimal polynomial of $x \in \mathbb{Q}(E)$ is given by $Y^2 - (\eta^2 + 39/4)Y + 507\eta - 4563/2$. Completing the square one obtains $\xi := x - \eta^2/2 - 39/8$ as generator of $\mathbb{Q}(E)$ over $\mathbb{Q}(\eta)$, and $\sigma(\xi) = -\xi$. Hence $\mathbb{Q}(\sqrt{13}, E) = \mathbb{Q}(\sqrt{13}, \eta, \xi)$ and $\tilde{\sigma}(\eta) = \eta, \tilde{\sigma}(\xi) = -\xi$ and $\tilde{\sigma}(\sqrt{13}) = -\sqrt{13}$. A basis of $\mathbb{Q}(\eta, \xi, \sqrt{13})$ as vector space over $\mathbb{Q}(\eta)$ is given by $1, \xi, \sqrt{13}, \xi\sqrt{13}$. Therefore, the invariants are given by

$$\mathbb{Q}(\sqrt{13}, E)^{<\tilde{\sigma}>} = \mathbb{Q}(\eta, \xi\sqrt{13}).$$

All successive extensions are of degree 2 in the following chain:

$$\mathbb{Q}(\eta) \subset \mathbb{Q}(\sqrt{13}, E)^{<\tilde{\sigma}>} \subset \mathbb{Q}(\sqrt{13}, E)$$

and $\mathbb{Q}(X) = \mathbb{Q}(\sqrt{13}, E)^{<\tilde{\sigma}>}$. The minimal polynomial of $\xi\sqrt{13}$ over $\mathbb{Q}(\eta)$ is given by $m(Y) = Y^2 - 13/4\eta^4 - 507/8\eta^2 + 6591\eta - 1917981/64$. Since $\mathbb{Q}(X) = \mathbb{Q}(\eta)[Y]/(m(Y))$,

$$Y^2 = \frac{13}{4}\eta^4 + \frac{507}{8}\eta^2 - 6591\eta + \frac{1917981}{64}$$

is an equation defining X. One can check that $X(\mathbb{Q}_{13}) = \emptyset$ so it has no rational points either. By construction, $< \sigma', \tau' >= D_9 \subset \mathrm{Isom}_{\mathbb{Q}}(X)$, so this curve has exactly the properties we were looking for.

4.4 Twisting and Poncelet

We have seen that the desired curves X can be constructed with both a Poncelet figure and a method involving twists. One might wonder what happens if we try to twist a Poncelet figure. This approach has been mentioned in [5, §6.2] and the example given there will be worked out in this section.

Consider the conics $\mathcal{C}\colon x^2 + y^2 = 1$ and $\mathcal{D}\colon x^2 + xy + y^2 = \frac{3}{8}$ in $\mathbb{P}^2$. This defines a Poncelet figure of order 4, for example the square with vertices $(\pm\frac{1}{2}\sqrt{2}, \pm\frac{1}{2}\sqrt{2})$ provides such a figure. Let $X/\mathbb{Q}$ be the corresponding curve; since $\mathcal{C} \cap \mathcal{D}$ consists of four distinct points, X has genus 1. Let $P = (p, q)$ be a point on $\mathcal{C}$. Lines $l\colon y = rx + s$ that are tangent to $\mathcal{D}$ satisfy $2s^2 = r^2 + r + 1$. Hence the curve X satisfies $\mathbb{Q}(X) = \mathbb{Q}(p, q, r, s)$ where

$$\begin{cases} 1 = p^2 + q^2 \\ q = rp + s \\ 2s^2 = r^2 + r + 1. \end{cases}$$

This system of equations is birationally equivalent over $\mathbb{Q}$ to

$$X\colon \quad y^2 = 5x^4 - 16x^3 + 10x^2 + 16x + 5,$$

with correspondence given by $x = \frac{1-q}{p}$ and $y = \frac{2A(x)\cdot r + 2B(x)}{x^2+1}$, with

$$A(x) = -x^4 + 6x^2 - 1 \qquad B(x) = -\frac{1}{2}x^4 + 4x^3 - x^2 - 4x - \frac{1}{2}.$$

Note that $\mathcal{C}$ and $\mathcal{D}$ are symmetric around the origin. This induces an involution on X given by $\mu\colon\ (p, q, r, s) \mapsto (-p, -q, r, -s)$. To compute the induced map of μ on the function field of X, note that $(1 - q)(1 + q) = p^2$ and hence $\frac{1-q}{p} \cdot \frac{1+q}{p} = 1$. This means the inverse of x is given by $\frac{1+q}{p}$ and we thus find $\mu(x) = \mu(\frac{1-q}{p}) = \frac{1+q}{-p} = -1/x$. Then it follows that $\mu(y) = \frac{2A(-1/x)\cdot r + 2B(-1/x)}{(-1/x)^2+1} = y/x^2$. As before, define $\tilde{\mu}$ to be the map acting on $\mathbb{Q}(\sqrt{d}, X)$ as

$$\begin{aligned} \tilde{\mu}\colon \quad x &\mapsto -1/x \\ y &\mapsto y/x^2 \\ \sqrt{d} &\mapsto -\sqrt{d}. \end{aligned}$$

As noted in the introduction of this chapter, the curve $X^{(d)}$ for which $\mathbb{Q}(X^{(d)}) = \mathbb{Q}(\sqrt{d}, X)^{<\tilde{\mu}>}$ is a quadratic twist of X, which justifies the notation. To find this twist, start with $\mathbb{Q}(\sqrt{d}, X) = \mathbb{Q}(p, q, r, s, \sqrt{d})$. Consider the chain of inclusions

$$\mathbb{Q}(r) \subset \mathbb{Q}(r, s) \subset \mathbb{Q}(r, s, p) \subset \mathbb{Q}(r, s, p, \sqrt{d}) = \mathbb{Q}(\sqrt{d})(X),$$

where all inclusions are of degree 2. For the first inclusion this follows from μ mapping $s \mapsto -s$ and for the second from $0 = p^2 + q^2 - 1 = p^2 + (rp + s)^2$, i.e. p has minimal polynomial of degree 2 over $\mathbb{Q}(r, s)$. From the chain it follows that a basis of $\mathbb{Q}(\sqrt{d})(X)$ as vector space over $\mathbb{Q}(r)$ is given by $1, s, p, sp, \sqrt{d}, s\sqrt{d}, p\sqrt{d}, sp\sqrt{d}$. As $\tilde{\mu}$ maps r to itself and $p, q, s, \sqrt{d}$ to minus itself, a basis of the subspace of invariants is given by $1, sp, s\sqrt{d}, p\sqrt{d}$. Now because $sp = (s\sqrt{d})(p\sqrt{d})/d$, the field of invariants is $\mathbb{Q}(r, s\sqrt{d}, p\sqrt{d})$ so this is the function field of the twist $X^{(d)}$. Comparing this to the equations defining X, we find that $X^{(d)}$ comes from the same conics scaled by a factor $\sqrt{d}$! That is, starting from $\mathcal{C}_2 \colon x^2 + y^2 = d$ and $\mathcal{D}_2 \colon x^2 + xy + y^2 = \frac{3}{8}d$ results in a Poncelet figure of order 4 with corresponding genus one curve $X^{(d)}$. Explicitly, this curve is given by $X^{(d)} \colon\ y^2 = 5d^2x^4 - 16d^2x^3 + 10d^2x^2 + 16d^2x + 5d^2$.

5 Conclusion

The aim of the thesis was to find an explicit example of a genus one curve over $\mathbb{Q}$ such that it has no rational points and it has a D_9 group structure in its automorphism group. The Poncelet method was tried first. An observation about equivalence of conics motivated a setup with one conic not necessarily having a rational point. Starting from a circle and a simple parabola, a curve with the desired properties was found this way. A hybrid method starting from a general equation did not give a solution. Secondly the invariant theory method was tried but it turned out to be not suitable as the computations became involved even for simpler cases. The last method about twists of elliptic curves resulted in a nice setup and an example of a curve satisfying the conditions was quickly found. Finally, we explained a relation between scaling certain Poncelet figures and twists of the corresponding genus one curve.

A Code general equation method

This appendix provides the Magma code that was used for the computations in the general equation method. The computations are done for the case $a = 1$, $c = f = i$ and $b = e = g = 0$. The first lines define the curve X, points $P_1, P_2 \in X$ and $E = (X, P_1)$.

```
K<w>:=QuadraticField(-3);
F<c>:=FunctionField(K);
FF<d>:=FunctionField(F);
FFF<h>:=FunctionField(FF);
P<x>:=PolynomialRing(FFF);
D:=BaseChange(HyperellipticCurve((-c)*x^4+(-c-c*d)*x^3+(-c-c*d)*x
   ^2+(-c*d)*x+(h^2)/4), FFF);
P1:=D![(-1+w)/2, h/2];
E,phi:= EllipticCurve(D, P1);
E;
P2:=D![(-1-w)/2, -h/2];
phi(P2);
```

Having found an equation for E, its 9-th and 3-rd division polynomial can be computed. The polynomials are evaluated at the x-coordinate of $\phi(P_2)$. Dividing the results leads to a huge expression in c, d and h, hence it is stored in a separate file.

```
Q<w>:=QuadraticField(-3);
A3<c,d,h>:=AffineSpace(Q,3);
K<c,d,h>:=FunctionField(A3);
PK<T>:=PolynomialRing(K);
E:=EllipticCurve([((2*w - 2)*h^2 + (4*w*c*d + (-2*w - 6)*c))/h^2,
   ((2*w + 2)*h^4 + ((-4*w - 4)*c*d + (-4*w + 20)*c)*h^2 + (-24*c
   ^2*d^2 + (-24*w + 24)*c^2*d + (12*w + 12)*c^2))/h^4, ((8*c*d +
   (16*w - 8)*c)*h^4 + ((-32*w + 48)*c^2*d^2 + (104*w + 72)*c^2*d +
    (-8*w - 120)*c^2)*h^2 + (-48*w*c^3*d^3 + (72*w + 216)*c^3*d^2 +
    (72*w - 216)*c^3*d - 48*w*c^3))/h^6, (((-8*w + 8)*c*d + (16*w +
    32)*c)*h^6 + ((-16*w - 32)*c^2*d^2 + (-32*w + 32)*c^2*d + (-16*
   w + 64)*c^2)*h^4 + ((48*w + 48)*c^3*d^3 + (48*w - 432)*c^3*d^2 +
    (-336*w + 144)*c^3*d + (96*w + 192)*c^3)*h^2 + (144*c^4*d^4 +
   (288*w - 288)*c^4*d^3 + (-432*w - 432)*c^4*d^2 + 576*c^4*d +
   (72*w - 72)*c^4))/h^8,0]);
pol9:=PK!DivisionPolynomial(E,9);
pol3:=PK!DivisionPolynomial(E,3);
ev9:=Evaluate(pol9,(((2*w + 6)*c*d + (4*w - 12)*c)*h^2 + (12*c^2*d
   ^2 + (12*w - 12)*c^2*d + (-6*w - 6)*c^2))/h^4);
ev3:=Evaluate(pol3,(((2*w + 6)*c*d + (4*w - 12)*c)*h^2 + (12*c^2*d
   ^2 + (12*w - 12)*c^2*d + (-6*w - 6)*c^2))/h^4);
good:=ev9/ev3;
SetLogFile("good.txt");
```

Note that the calculation can be somewhat simplified by getting rid of the denominators in E, using the change of variables $x = h^4x$, $y = h^6y$. To search for rational triples (c, d, h) satisfying the equation 'good', a point search is applied.

```
1 A3<c,d,h>:=AffineSpace(Rationals(),3);
2 good:=[paste];
3 V:=Scheme(A3,good);
4 PointSearch(V,500);
```

No rationals triples were found with this calculation.

B Code twisting method solution

The magma code used to obtain a solution via the twisting method (§ 4.3) is provided in this section. The non-constant function η in $L(O + (0, \frac{507}{2}))$ was computed as follows.

```
Q:=Rationals();
E:=EllipticCurve([0,-39/4,0,-4563/2,257049/4]);
F<x,y>:=FunctionField(E);
D1:=Divisor(E![0,1,0])+Divisor(E![0,-507/2]);
V,b:=RiemannRochSpace(D1);
Dimension(V);
b(V.1);
b(V.2);
```

For the computation of the minimal polynomial of $\xi\sqrt{13}$, first the function field $\mathbb{Q}(\sqrt{13}, E)$ is constructed by adding x and $\sqrt{13}$ to $\mathbb{Q}(\eta)$.

```
Q:=Rationals();
Qe<e>:=FunctionField(Q);
PQe<Y>:=PolynomialRing(Qe);
Qex<x>:=ext<Qe | Y^2-(e^2+39/4)*Y+507*e-4563/2>;
PQex<Z>:=PolynomialRing(Qex);
Qexw<w>:=ext<Qex | Z^2-13>;
xi:=x-e^2/2-39/8;
MinimalPolynomial(xi*w,Qe);
```

To show that the resulting genus one curve has no rational points, the following code is used. In the last line, 'false' is returned.

```
Q:=Rationals();
P<e>:=PolynomialRing(Q);
C:=GenusOneModel(HyperellipticCurve(13*e^4 + 1014*e^2 - 210912*e +
   1917981));
IsLocallySoluble(C,2);
IsLocallySoluble(C,3);
IsLocallySoluble(C,5);
IsLocallySoluble(C,7);
IsLocallySoluble(C,11);
IsLocallySoluble(C,13);
```

References

[1] J. Bhaskar. Sum of two squares. https://www.math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Bhaskar.pdf, 2008.

[2] D. G. J. Draisma. Invariant theory with applications. https://www.win.tue.nl/~jdraisma/teaching/invtheory0910/lecturenotes12.pdf, 2009.

[3] J. Los, T. Mepschen, and J. Top. Rational Poncelet. *Int. J. Number Theory*, 14:2641–2655, 2018.

[4] B. Mazur. Modular curves and the Eisenstein ideal. *Publ. Math. Inst. Hautes Études Sci.*, 47:33–186, 1977.

[5] M. Roelfszema. Finite groups of automorphisms on genus one curves without rational points. http://fse.studenttheses.ub.rug.nl/17862/, 2018.

[6] J.-P. Serre. *A Course in Arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Springer Verlag, New York, 1973.

[7] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer Verlag, Berlin, 2009.

[8] A. Sutherland. Torsion subgroups of elliptic curves over number fields. http://www-math.mit.edu/~drew/MazursTheoremSubsequentResults.pdf, 2012.