Constructing Cubic Curves with Involutions

Lorenz Halbeisen

Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland

lorenz.halbeisen@math.ethz.ch

Norbert Hungerbühler

Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland

norbert.hungerbuehler@math.ethz.ch

key-words: cubic curve, line involution, ruler constructions, elliptic curve

2020 Mathematics Subject Classification: **51A05** 51A20

Abstract

In 1888, Heinrich Schroeter provided a ruler construction for points on cubic curves based on line involutions. Using Chasles' Theorem and the terminology of elliptic curves, we give a simple proof of Schroeter's construction. In addition, we show how to construct tangents and additional points on the curve using another ruler construction which is also based on line involutions. As applications of Schroeter's construction we provide a new parametrisation of elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and give some configurations with all their points on a cubic curve.

1 Introduction

Heinrich Schroeter gave in [12] a surprisingly simple ruler construction to generate points on a cubic curve. Since he did not provide a formal proof for the construction, we would like to present this here. Schroeter's construction can be interpreted as an iterated construction of line involutions. Thus, we first define the notion of a line involution with cross-ratios, and then we show how one can construct line involutions with ruler only.

For the sake of simplicity, we introduce the following terminology: For two distinct points P and Q in the plane, PQ denotes the line through P and Q, $\overline{PQ}$ denotes the distance between P and Q, and for two distinct lines l_1 and l_2, $l_1 \wedge l_2$ denotes the intersection point of l_1 and l_2. We tacitly assume that the plane is the real projective plane, and therefore, $l_1 \wedge l_2$ is defined for any distinct lines l_1 and l_2. For the cross-ratio of four lines a, b, x, y of a pencil we use the notation $\operatorname{cr}(a, b, x, y)$.

Line involution. Given a pencil. A line involution Λ is a mapping which maps each line l of the pencil to a so-called conjugate line $\bar{l}$ of the pencil, such that the following conditions are satisfied:

- Λ is an involution, *i.e.*, $\Lambda \circ \Lambda$ is the identity, in particular we have $\Lambda(\bar{l}) = l$.
- Given three different pairs of conjugate lines $a, \bar{a}$, $b, \bar{b}$, $c, \bar{c}$, and let l_1, l_2, l_3, l_4 be four lines among $a, \bar{a}, b, \bar{b}, c, \bar{c}$ from three different pairs of conjugate lines, then

$$\operatorname{cr}(l_1, l_2, l_3, l_4) = \operatorname{cr}\left(\bar{l}_1, \bar{l}_2, \bar{l}_3, \bar{l}_4\right).$$

Notice that any line involution is defined by two different pairs of conjugate lines. We shall use the following construction for line involutions (for the correctness of the construction see Chasles [1, Note X, § 34, (28), p. 317]): Given two pairs $a, \bar{a}$ and $b, \bar{b}$ of conjugate lines which meet in P. Suppose, we want to find the conjugate line $\bar{d}$ of a line d from the same pencil. Choose a point $D \neq P$ on d and two lines through D which meet a and b in the points A and B, and $\bar{a}$ and $\bar{b}$ in the points $\bar{A}$ and $\bar{B}$, respectively (see Fig. 1). Let $\bar{D} = A\bar{B} \wedge \bar{A}B$. Then the conjugate line $\bar{d}$ of d with respect to the line involution defined by $a, \bar{a}, b, \bar{b}$ is the line $P\bar{D}$.

Vice-versa, let $A, \bar{A}$ and $B, \bar{B}$ be two pairs of different points and $D = AB \wedge \bar{A}\bar{B}$, $\bar{D} = A\bar{B} \wedge \bar{A}B$. Then, for an arbitrary point $P \notin \{A, \bar{A}, B, \bar{B}, D, \bar{D}\}$, the lines $a = PA, \bar{a} = P\bar{A}$, $b = PB, \bar{b} = P\bar{B}$, and $d = PD, \bar{d} = P\bar{D}$ are conjugate lines.

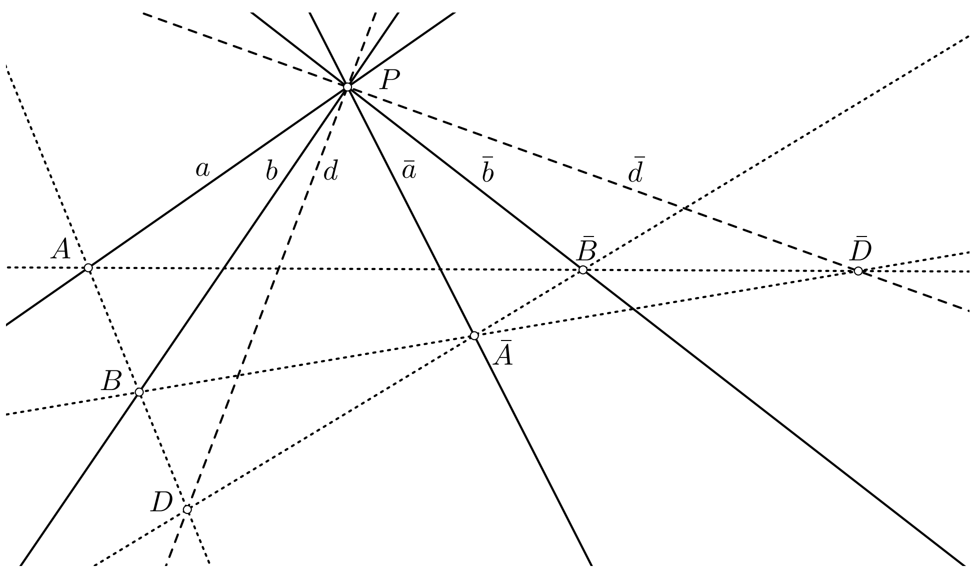

Figure 1: Construction of conjugate lines

Notice that this construction can be carried out using only a ruler.

2 Schroeter's Construction for Cubic Curves

Using the Braikenridge-Maclaurin Theorem, *i.e.*, the converse of Pascal's theorem (see, for example, [2, p. 76]), it is possible to construct an arbitrary number of points on a conic if five of its points are given, using only a ruler. An attempt to find a corresponding ruler construction for cubic curves was made in [9]: Let A, B, C, D, E be five points on a cubic curve. Assume that the points $A\#B$, $C\#D$ and $(A\#B)\#(C\#D)$ are also known (see Figure 2). Then, by Chasles' Theorem (see below), all cubic cuves through the eight points $A, B, C, D, E, A\#B, C\#D$, $(A\#B)\#(C\#D)$ pass through a ninth point X, namely the sixth intersection of the cubic curve with the conic through A, B, C, D, E. It is then shown that X is also the intersection of the conic with the line through E and $(A\#B)\#(C\#D)$, and can therefore be constructed with ruler alone. However the constructions in [9] do not iterate and the authors were not aware of Schroeter's work, which allows to construct an arbitrary number of points on a cubic curve.

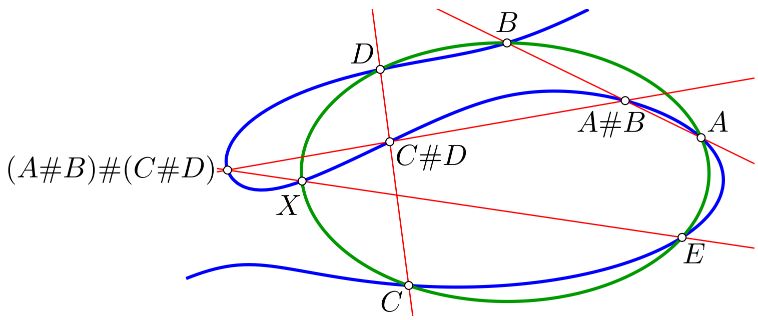

Figure 2: Ruler construction of the point X.

Schroeter's ruler construction, described in [12], is based on line involutions:

Schroeter's Construction. *Let $A, \bar{A}$, $B, \bar{B}$, $C, \bar{C}$ be six pairwise distinct points in a plane such that no four points are collinear and the three pairs of points $A, \bar{A}$, $B, \bar{B}$, $C, \bar{C}$ are not the pairs of opposite vertices of the same complete quadrilateral. Now, for any two pairs of points $P, \bar{P}$ and $Q, \bar{Q}$, we define a new pair $S, \bar{S}$ of points by stipulating*

$$S \ := \ PQ \wedge \bar{P}\bar{Q} \qquad \text{and} \qquad \bar{S} \ := \ P\bar{Q} \wedge \bar{P}Q\,.$$

Then all the points constructed in this way lie on a cubic curve.

Points $S, \bar{S}$ which are constructed by Schroeter's construction will be called Schroeter points or pairs of Schroeter points.

Notice first that with Schroeter's construction, we always construct pairs of conjugate lines: For any point $R \notin \{P, \bar{P}, Q, \bar{Q}, S, \bar{S}\}$ the lines $RP, R\bar{P}, RQ, R\bar{Q}, RS, R\bar{S}$ are pairs of conjugate lines with respect to the same line involution. Further notice that if the three pairs of points are opposite vertices of the same complete quadrilateral, then the construction gives us no additional points.

At first glance, it is somewhat surprising that all the points we construct lie on the same cubic curve, which is defined by three pairs of points (recall that a cubic curve is defined by 9 points). The reason is that we have three *pairs* of points and not just 6 points. In fact, if we start with the same 6 points but pairing them differently, we obtain a different cubic curve. It is also not clear whether the construction generates infinitely many points of the curve. Schroeter claims in [12] that this is the case, but, as we will see in the next section, it may happen that the construction gives only a finite number of points.

3 A Proof of Schroeter's Construction

It is very likely that Schroeter discovered his construction based on his earlier work on cubics (see [13, 14]). However, he did not give a rigorous proof of his construction, and the fact that he claimed wrongly that the construction generates always infinitely many points of the curve might indicate that he overlooked something. Below we give a simple proof of Schroeter's construction using Chasles' Theorem (see Chasles [1, Chapitre IV, §8, p. 150]) and the terminology of elliptic curves.

Theorem 1 (Chasles' Theorem)**.** *If a hexagon $ABC\bar{A}\bar{B}\bar{C}$ is inscribed in a cubic curve Γ and the points $AB \wedge \bar{A}\bar{B}$ and $BC \wedge \bar{B}\bar{C}$ are on Γ, then also $C\bar{A} \wedge \bar{C}A$ is on Γ (see Fig. 3).*

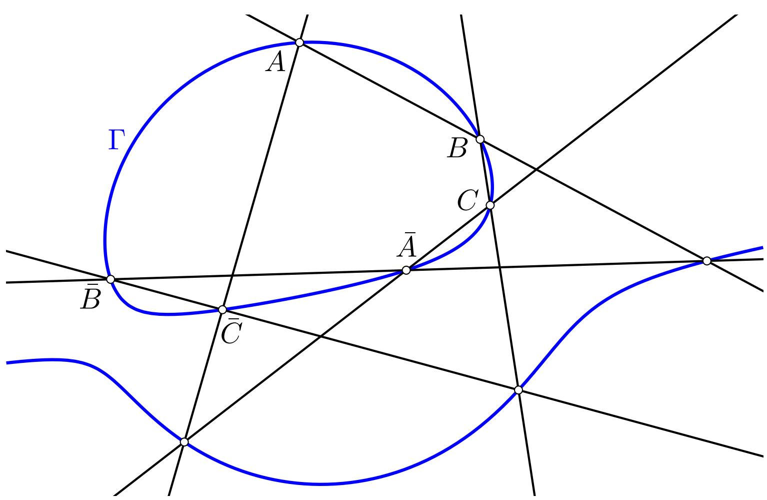

Figure 3: Chasles' Theorem in a Neuberg Cubic Γ.

With Chasles' Theorem we can prove the following

Proposition 2. *Let $A, \bar{A}$, $B, \bar{B}$, $C, \bar{C}$ be six pairwise distinct points in a plane such that no four points are collinear and none of the pairs of points $A, \bar{A}$, $B, \bar{B}$, $C, \bar{C}$ is a* *pair of opposite vertices of the same complete quadrilateral. Furthermore, let*

$$\begin{aligned} D &:= AB \wedge \bar{A}\bar{B}\,, & E &:= BC \wedge \bar{B}\bar{C}\,, & F &:= CA \wedge \bar{C}\bar{A}\,, \\ \bar{D} &:= A\bar{B} \wedge \bar{A}B\,, & \bar{E} &:= B\bar{C} \wedge \bar{B}C\,, & \bar{F} &:= C\bar{A} \wedge \bar{C}A\,, \end{aligned}$$

and assume that the 9 *points* $A, \bar{A}$*,* $B, \bar{B}$*,* $C, \bar{C}$*,* D, E, F *are pairwise distinct and that* Γ *is a cubic curve passing through these* 9 *points. Then* Γ *passes also through* $\bar{D}, \bar{E}, \bar{F}$*.*

Proof. Since the 6 points $A, \bar{A}$, $B, \bar{B}$, $C, \bar{C}$ as well as D and E are on Γ, by Chasles' Theorem we get that also $\bar{F}$ is on Γ. Similarly, since $C, \bar{C}$, $A, \bar{A}$, $B, \bar{B}$, F, D are on Γ, also $\bar{E}$ is on Γ. Finally, since $B, \bar{B}$, $C, \bar{C}$, $A, \bar{A}$, E, F are on Γ, also $\bar{D}$ is on Γ. *q.e.d.*

As an immediate consequence of Proposition 2 we get

Corollary 3. *The unique cubic curve* Γ *passing through the* 9 *points* $A, \bar{A}$*,* $B, \bar{B}$*,* $C, \bar{C}$*,* D, E, F *contains also the* 3 *points* $\bar{D}, \bar{E}, \bar{F}$*.*

In order to show that all the points constructed by Schroeter's construction lie on the same cubic curve, we interpret the construction in the setting of elliptic curves. For this, let Γ be a cubic curve and let $\mathscr{O}$ be a point of inflection of Γ — recall that every cubic curve in the real projective plane has at least one point of inflection. For two points P and Q on Γ let $P \# Q$ be the third intersection point (counting multiplicities) of PQ with Γ, where for $P = Q$, PQ is the tangent on Γ with contact point P. Furthermore, for each point P on Γ, let $-P := \mathscr{O} \# P$. As usual, we define the binary operation $+$ on the points of Γ by stipulating

$$P + Q := -(P \# Q)\ .$$

Notice that $-P + P = \mathscr{O}$ and, since $\mathscr{O}$ is a point of inflection, we have $-\mathscr{O} = \mathscr{O}$. It is well known that the operation $+$ is associative and the structure $(\Gamma, \mathscr{O}, +)$ is an abelian group with neutral element $\mathscr{O}$, which is called an *elliptic curve*.

Now, let Γ be the cubic curve passing through $A, \bar{A}, B, \bar{B}, C, \bar{C}, D, E, F$ and let $\mathscr{O}$ be a point of inflection of Γ. Then, by construction of Γ we have, for example, $A \# B = \bar{A} \# \bar{B}$, or equivalently, $-(A + B) = -\big(\bar{A} + \bar{B}\big)$.

Lemma 4. *(a) Let* $P, Q, \bar{P}, \bar{Q}$ *be pairwise distinct points on a cubic curve* Γ*. If* $S := PQ \wedge \bar{P}\bar{Q} \in \Gamma$ *and* $\bar{S} := P\bar{Q} \wedge \bar{P}Q \in \Gamma$*, then* $P \# P = \bar{P} \# \bar{P} \in \Gamma$*,* $Q \# Q = \bar{Q} \# \bar{Q} \in \Gamma$*, and* $S \# S = \bar{S} \# \bar{S} \in \Gamma$*.*

(b) Vice versa, if $P' := P \# P = \bar{P} \# \bar{P} \in \Gamma$ *for two points* $P, \bar{P} \in \Gamma$*, then we have for all* $Q \in \Gamma$ *the following: If* $S := P \# Q$ *and* $\bar{Q} = S \# \bar{P}$*, then* $\bar{S} = P\bar{Q} \wedge \bar{P}Q \in \Gamma$ *and* $Q' := Q \# Q = \bar{Q} \# \bar{Q} \in \Gamma$*.*

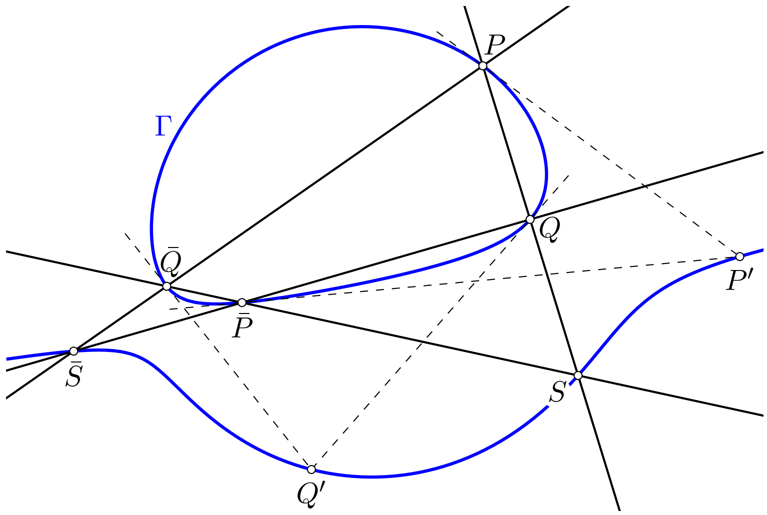

Figure 4: Illustration Lemma 4.

Proof. (a) By assumption we have $P \# Q = \bar{P} \# \bar{Q} = S$ and $P \# \bar{Q} = \bar{P} \# Q = \bar{S}$. With a point $\mathscr{O} \in \Gamma$ of inflection, we get

$$P + Q = \mathscr{O} \# (P \# Q) = \mathscr{O} \# (\bar{P} \# \bar{Q}) = \bar{P} + \bar{Q} \tag{1}$$

and

$$P + \bar{Q} = \mathscr{O} \# (P \# \bar{Q}) = \mathscr{O} \# (\bar{P} \# Q) = \bar{P} + Q. \tag{2}$$

Adding (1) and (2)and subtracting $Q+\bar{Q}$ yields $P+P = \bar{P}+\bar{P}$ and hence $P\#P = \bar{P}\#\bar{P}$. Exchanging left and right hand in (1) and adding (2) gives, upon subtracting $P + \bar{P}$, $Q + Q = \bar{Q} + \bar{Q}$ and hence $Q \# Q = \bar{Q} \# \bar{Q}$. $S \# S = \bar{S} \# \bar{S}$ follows by exchanging the pair $Q, \bar{Q}$ by the pair $S, \bar{S}$.

(b) For the second part, we proceed as follows: By assumption, we have $P\#P = \bar{P}\#\bar{P}$ and therefore $P+P = \mathscr{O}\#(P\#P) = \mathscr{O}\#(\bar{P}\#\bar{P}) = \bar{P}+\bar{P}$. We add S and subtract $P+\bar{P}$ to get $S+P-\bar{P} = S+\bar{P}-P$ or $(\mathscr{O} \# (S \# P)) \# (\mathscr{O} \# \bar{P}) = (\mathscr{O} \# (S \# \bar{P})) \# (\mathscr{O} \# P)$. It follows that $(S \# P) \# \bar{P} = (S \# \bar{P}) \# P$, *i.e.*, $Q \# \bar{P} = \bar{Q} \# P = \bar{S}$. Finally, $Q \# Q = \bar{Q} \# \bar{Q} = Q'$ follows from the first part. *q.e.d.*

For the sake of simplicity we write $2 * P$ for $P + P$. Let $A, \bar{A}$ be a pair of points with $A \# A = \bar{A} \# \bar{A}$ on a cubic curve Γ, and with respect to a given point of inflection $\mathscr{O}$, let $T_A := \bar{A} - A$. Then $A + T_A = \bar{A}$, which implies that

$$2 * \bar{A} = 2 * (A + T_A) = 2 * A + 2 * T_A.$$

Now, by assumption we have $2 * A = 2 * \bar{A}$ and therefore we get that $2 * T_A = \mathscr{O}$. In other words, T_A is a point of order 2.

Now we are ready to prove the following

Theorem 5. *All the points we obtain by Schroeter's construction belong to the same cubic curve.*

Proof. Let $A, \bar{A}, B, \bar{B}, C, \bar{C}$ be six pairwise distinct points in a plane such that no four points are collinear and none of the pairs of conjugate points $A, \bar{A}$, $B, \bar{B}$, $C, \bar{C}$ is a pair of opposite vertices of the same complete quadrilateral. Furthermore, let $D, \bar{D}, E, \bar{E}, F, \bar{F}$ be as in Proposition 2, and let Γ be the cubic curve which passes through all of these 12 points. Finally, let $\mathscr{O}$ a fixed point of inflection of Γ, and let $T_A := \bar{A} - A$, $T_B := \bar{B} - B$, and $T_C := \bar{C} - C$ be three points of order 2. First we show that $T_A = T_B$. Since $A \# B = \bar{A} \# \bar{B}$ we have $-(A + B) = -(A + T_A + B + T_B)$, which implies that $T_A = T_B$. With a similar argument we obtain $T_B = T_C$. Thus, we have $T_A = T_B = T_C =: T$.

We will say that a set M of points is a *good set*, if

(a) all points of M belong to Γ,

(b) the points $A, \bar{A}, B, \bar{B}, C, \bar{C}, D, \bar{D}, E, \bar{E}, F, \bar{F}$ belong to M,

(c) if the pair of points $S, \bar{S}$ belongs to M, then $S = P \# Q = \bar{P} \# \bar{Q}$ and $\bar{S} = P \# \bar{Q} = \bar{P} \# Q$ for two pairs $P, \bar{P}$ and $Q, \bar{Q}$ in M,

(d) for all pairs $P, \bar{P}$ of M, we have $P \# P = \bar{P} \# \bar{P}$, and

(e) for all pairs $P, \bar{P}$ of M, we have $\bar{P} - P = T$.

Observe first, that $\{A, \bar{A}, B, \bar{B}, C, \bar{C}, D, \bar{D}, E, \bar{E}, F, \bar{F}\}$ is a good set. Indeed, (a) and (b) are trivially satisfied. The property (c) is clear for $D, \bar{D}, E, \bar{E}, F, \bar{F}$. For A and $\bar{A}$ we have $A = B \# D = \bar{B} \# \bar{D}$, $\bar{A} = B \# \bar{D} = \bar{B} \# D$, and similarly for the pairs $B, \bar{B}$ and $C, \bar{C}$. The property (d) follows directly from Lemma 4(a). Finally, we have property (e) already for $A, \bar{A}$, $B, \bar{B}$ and $C, \bar{C}$. For D the argument is similar: Let $T_D := \bar{D} - D$. T_D is a point of order 2 and from $B = A \# D = \bar{A} \# \bar{D}$ it follows $A + D = \bar{A} + \bar{D} = A + T + D + T_D$ and hence $T_D = T$. The analogous argument shows that $\bar{E} - E = \bar{F} - F = T$.

Now suppose that M is a good set, and take two pairs $P, \bar{P}$ and $Q, \bar{Q}$ in M. Let $S = PQ \wedge \bar{P}\bar{Q}$ and $\bar{S} = P\bar{Q} \wedge \bar{P}Q$. Then we claim that $M \cup \{S, \bar{S}\}$ is also a good set. We first show that $P \# Q = \bar{P} \# \bar{Q}$ or equivalently that $P + Q = \bar{P} + \bar{Q}$. This is equivalent to $T = \bar{P} - P = Q - \bar{Q} = T$ which is true by property (e) for M and the fact that T is a point of order 2. Then $P \# \bar{Q} = \bar{P} \# Q$ follows from Lemma 4(b). We conclude that the set $M \cup \{S, \bar{S}\}$ has the properties (a) and (c). Property (b) is trivial. For property (d) we need to see that $S \# S = \bar{S} \# \bar{S}$, which follows from Lemma 4(a). For property (e) we define $T_S = \bar{S} - S$. T_S is a point of order 2. From $Q = P \# S = \bar{P} \# \bar{S}$ it follows $P + S = \bar{P} + \bar{S} = P + T + S + T_S$ and hence $T_S = T$. This shows that $M \cup \{S, \bar{S}\}$ has all properties of a good set.

It follows that all points we obtain by Schroeter's construction belong to the same curve Γ. *q.e.d.*

The above proof shows that the Schroeter points have the following additional properties

- If $P, \bar{P}$ is a pair of Schroeter points on Γ, then the tangents in P and $\bar{P}$ meet on Γ.
- With respect to a chosen point $\mathscr{O}$ of inflection, we have that $\bar{P} - P = T$ is a point of order 2 on Γ which is the same for all Schroeter pairs $P, \bar{P}$.

The following result shows that we can construct the tangent to Γ in each Schroeter point by a line involution (hence with ruler alone).

Proposition 6. *Let Γ be the cubic from Proposition 2. Assume that $S, \bar{S}$, $P, \bar{P}$, $Q, \bar{Q}$ are three of the pairs $A, \bar{A}$, $B, \bar{B}$, $C, \bar{C}$, $D, \bar{D}$, $E, \bar{E}$, $F, \bar{F}$ or of the pairs which are constructed by Schroeter's construction, such that SP, SQ, $S\bar{P}$, $S\bar{Q}$ are four distinct lines. Let $s = S\bar{S}$ and $\bar{s}$ its conjugate line with respect to the involution given by the lines SP, SQ, $S\bar{P}$, $S\bar{Q}$. Then $\bar{s}$ is tangent to Γ in S (see Fig. 5).*

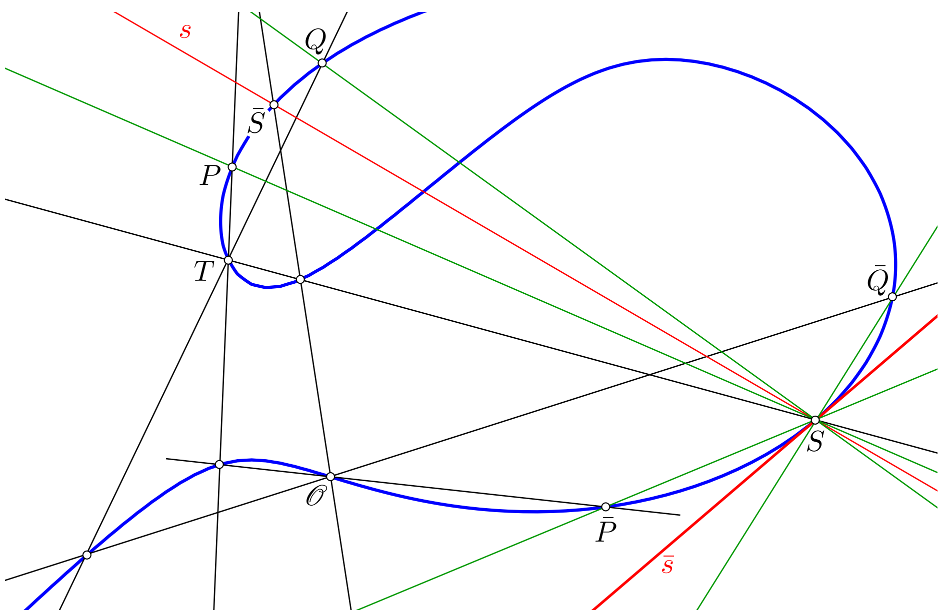

Figure 5: Thin black lines: $\bar{P} = T + P, \bar{Q} = T + Q, \bar{S} = T + S$. The red lines $s = S\bar{S}$ and the thick tangent $\bar{s}$ in S are conjugate lines with respect to the line involution given by the green lines $SP, S\bar{P}, SQ, S\bar{Q}$.

Before we can prove Proposition 6, we have to recall a few facts about cubic curves. It is well-known that every cubic curve can be transformed into Weierstrass Normal

Form

$$\Gamma_{a,b}:\ y^2 = x^3 + ax^2 + bx$$

with $a, b, c \in \mathbb{R}$. In the real projective plane, $\mathscr{O} = (0, 1, 0)$ is a point inflection of $\Gamma_{a,b}$ and $T_{a,b} = (0, 0, 1)$ is a point of order 2 of $\Gamma_{a,b}$, where $\mathscr{O}$ is the neutral element of the elliptic curve $\Gamma_{a,b}$. If A is a point on $\Gamma_{a,b}$, then we call the point $\bar{A} := T + A$ the *conjugate of* A. Since $T + T = \mathscr{O}$, we have

$$\bar{\bar{A}} = T + \bar{A} = T + T + A = \mathscr{O} + A = A\,.$$

Recall that $A \# B := -(A + B)$. In particular, if $C = A \# A$, then the line through C and A is tangent to $\Gamma_{a,b}$ with contact point A.

The following result gives a connection between conjugate points and tangents.

Fact 7. *If $A, \bar{A}, B$ are three points on $\Gamma_{a,b}$ which lie on a straight line, then $A \# A = \bar{B}$.*

Proof. If $A, \bar{A}, B$ are three points on $\Gamma_{a,b}$ on a straight line, then $A + \bar{A} = -B$. Thus, $A + T + A = T + A + A = -B$, which implies

$$A + A = T + (T + A + A) = T + (-B) = (-T) + (-B) = -(T + B) = -\bar{B}\,,$$

and therefore, the line $A\bar{B}$ is tangent to $\Gamma_{a,b}$ with contact point A, *i.e.*, $A \# A = \bar{B}$.

q.e.d.

In homogeneous coordinates, the curve $y^2 = x^3 + ax^2 + bx$ becomes

$$\Gamma:\ Y^2 Z = X^3 + aX^2 Z + bXZ^2\,.$$

Assume now that $\tilde{A} = \big(r_0, r_1, 1\big)$ is a point on the cubic Γ, where $r_0, r_1 \in \mathbb{R} \setminus \{0\}$. Then the point $(1, 1, 1)$ is on the curve

$$r_1^2 Y^2 Z = r_0^3 X^3 + ar_0^2 X^2 Z + br_0 XZ^2\,.$$

Now, by exchanging X and Z (*i.e.*, $(X, Y, Z) \mapsto (Z, Y, X)$), de-homogenising with respect to the third coordinate (*i.e.*, $(Z, Y, X) \mapsto (\frac{Z}{X}, \frac{Y}{X}, 1)$), and multiplying with $\frac{1}{r_1^2}$, we obtain that the point $A = (1, 1)$ is on the curve

$$\Gamma_{\alpha,\beta,\gamma}:\ y^2 x = \alpha + \beta x + \gamma x^2\,,$$

where

$$\alpha = \frac{r_0^3}{r_1^2}\,, \qquad \beta = a \cdot \frac{r_0^2}{r_1^2}\,, \qquad \gamma = b \cdot \frac{r_0}{r_1^2}\,.$$

Notice that since $A = (1, 1)$ is on $\Gamma_{\alpha,\beta,\gamma}$, we have $\alpha + \beta + \gamma = 1$.

The next result gives a connection between line involutions and conjugate points.

Lemma 8. *Let $A = (x_0, y_0)$ be an arbitrary but fixed point on $\Gamma_{\alpha,\beta,\gamma}$. For every point P on $\Gamma_{\alpha,\beta,\gamma}$ which is different from A and $\bar{A}$, let $g := AP$ and $\bar{g} := A\bar{P}$. Then the mapping $I_A : g \mapsto \bar{g}$ is a line involution.*

Proof. It is enough to show that there exists a point ζ_0 (called the center of the involution) on the line $h : x = 0$, such that the product of the distances between ζ_0 and the intersections of g and $\bar{g}$ with h is constant.

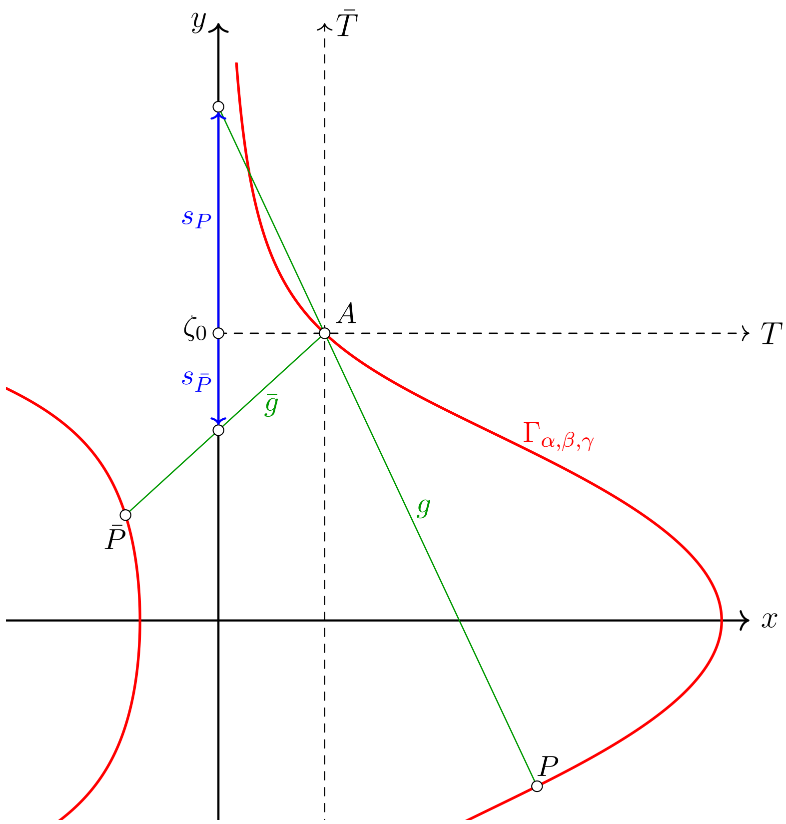

Figure 6: Line involution.

Since $\bar{T} = T + T = \mathscr{O}$, with respect to T we have $g : y = y_0$ and $\bar{g} : x = x_0$, which implies that $\zeta_0 = (0, y_0)$. Now, let $P = (x_1, y_1)$ be a point on $\Gamma_{\alpha,\beta,\gamma}$ which is different from $A, \bar{A}, T, \mathscr{O}$, and let $g := AP$ and $\bar{g} := A\bar{P}$. Since $\bar{P} = \left(\frac{\alpha}{\gamma x_1}, -y_1\right)$, the slopes λ_P and $\lambda_{\bar{P}}$ of g and $\bar{g}$, respectively, are

$$\lambda_P = \frac{y_1 - y_0}{x_1 - x_0} \qquad \text{and} \qquad \lambda_{\bar{P}} = \frac{-y_1 - y_0}{\frac{\alpha}{\gamma x_1} - x_0}\,.$$

Thus, the distances s_P and $s_{\bar{P}}$ between ζ_0 and the intersections of g and $\bar{g}$ with h, respectively, are

$$s_P = -\frac{x_0(y_1 - y_0)}{x_1 - x_0} \qquad \text{and} \qquad s_{\bar{P}} = \frac{x_0(y_1 + y_0) \cdot \gamma x_1}{\alpha - \gamma x_1 x_0}\,.$$

Now,

$$s_P \cdot s_{\bar{P}} = -\frac{x_0^2(y_1-y_0)(y_1+y_0)\gamma x_1}{(x_1-x_0)(\alpha-\gamma x_0 x_1)} = -\frac{x_0^2(y_1^2-y_0^2)\gamma x_1}{(x_1-x_0)(\alpha-\gamma x_0 x_1)},$$

and using the fact that for $i \in \{0,1\}$, $y_i^2 = \frac{\alpha}{x_i} + \beta + \gamma x_i$, we obtain

$$s_P \cdot s_{\bar{P}} = \gamma \cdot x_0,$$

which is independent of the particular point $P = (x_1, y_1)$. *q.e.d.*

Since line involutions are invariant under projective transformations, as a consequence of Lemma 8 we obtain the following

Fact 9. *Let Γ be the cubic from Proposition 2 with two pairs of Schroeter points $P, \bar{P} = T + P$, $Q, \bar{Q} = T + Q$, and let R be a point on Γ such that $RP, R\bar{P}, RQ, R\bar{Q}$ are four different lines. Let S be a further point on Γ and $\bar{S} = T + S$. Then the lines $s = RS$ and $\bar{s} = R\bar{S}$ are conjugate lines with respect to the line involution given by the lines $RP, R\bar{P}, RQ, R\bar{Q}$ (see Fig. 7).*

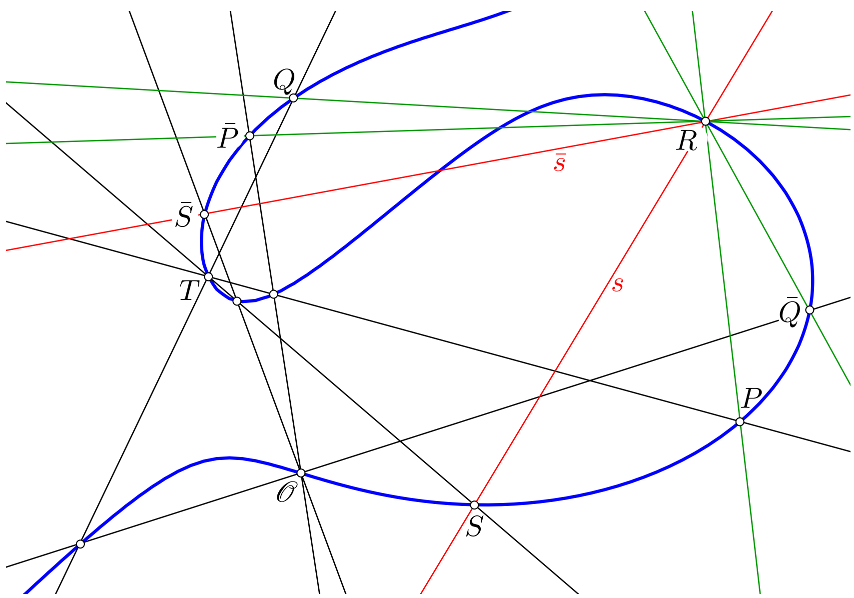

Figure 7: Thin black lines: $\bar{P} = T + P$, $\bar{Q} = T + Q$, $\bar{S} = T + S$. The red lines $s = RS$ and $\bar{s} = R\bar{S}$ are conjugate lines with respect to the line involution given by the green lines $RP, R\bar{P}, RQ, R\bar{Q}$.

Now we are ready to prove Proposition 6.

Proof of Proposition 6. First notice that S and $\bar{S}$ are distinct, since otherwise, $\bar{S} = T + S = S$, which implies that $T = S - S = \mathscr{O}$.

Assume that the line s intersects Γ in a point U which is different from S and $\bar{S}$. Then $\bar{U} := T + U$ belongs to $\bar{s}$. If the line $\bar{s}$ intersects Γ in a point V which is different from $\bar{U}$, then, with respect to the involution given by the lines $\bar{U}S$, $\bar{U}P$, $\bar{U}\bar{S}$, $\bar{U}\bar{P}$, the point $\bar{V}$ belongs to s. Hence, $\bar{V} = \bar{S}$, which shows that $\bar{s}$ is tangent to Γ in S.

Now, assume that the line s intersects Γ just in S and $\bar{S}$. Then, the line s is tangent to Γ either in S or in $\bar{S}$. We just consider the former case, the latter case is handled similarly. Let P_n (for $n \in \mathbb{N}$) be a sequence of points on Γ which are different from S and which converges to S, *i.e.*, $\lim_{n\to\infty} P_n = S$. Since for each $n \in \mathbb{N}$ we have $\bar{P}_n = T + P_n$ (where $\bar{P}_n := T + P$), by continuity of addition we have $\lim_{n\to\infty} \bar{P}_n = \bar{S}$. For each $n \in N$ let $t_n := P_n S$. Then, for each $n \in \mathbb{N}$, $\bar{t}_n = \bar{P}_n S$. Since s is tangent to Γ in S, by continuity, on the one hand we have $\lim_{n\to\infty} t_n = s$, and on the other hand we have $\lim_{n\to\infty} \bar{t}_n = s$, which implies that $\bar{s} = s$ and shows that $\bar{s}$ is tangent to Γ in S. *q.e.d.*

As a corollary of Proposition 6 and Lemma 4(a) we obtain the following:

Corollary 10. *Let Γ be the cubic from Proposition 2. Then we have:*

(a) In each Schroeter point it is possible to construct the tangent by a line involution, i.e., with a ruler construction.

(b) In addition to the Schroeter points on Γ one can construct for each Schroeter pair $P, \bar{P}$ the point $P \# P = \bar{P} \# \bar{P} \in \Gamma$ by ruler alone: These are the intersection points of the tangents in P and in $\bar{P}$.

Fig. 8 shows a sample of Schroeter points and of intersection points of the corresponding tangents.

A priori it might be possible that Schroeter's construction does not yield *all* cubic curves. However, the next theorem says that in fact all cubic curves carry Schroeter's construction.

Theorem 11. *Let Γ be a non-singular cubic curve. Let A, B, C be three different arbitrary points on Γ. Then, there are points $\bar{A}, \bar{B}, \bar{C}$ on Γ such that $D = AB \wedge \bar{A}\bar{B}$, $E = BC \wedge \bar{B}\bar{C}$, $F = CA \wedge \bar{C}\bar{A}$ are points on Γ and so do all the points given by Schroeter's construction.*

Proof. Choose $\bar{A}$ such that $A \# A = \bar{A} \# \bar{A}$ and $\bar{B} := \bar{A} \# (A \# B)$. In particular, we have $A \# B = \bar{A} \# \bar{B}$, and, by Lemma 4, $A \# \bar{B} = \bar{A} \# B$ and $B \# B = \bar{B} \# \bar{B}$. Let $\bar{C} := \bar{B} \# (B \# C)$. In particular, we have $B \# C = \bar{B} \# \bar{C}$, and, by Lemma 4, $B \# \bar{C} = \bar{B} \# C$ and $C \# C = \bar{C} \# \bar{C}$. It follows from Chasles' Theorem 1 that $A \# \bar{C} = \bar{A} \# C$. From the above, we obtain by applying Proposition 2 with C and $\bar{C}$ exchanged, that $A \# C = \bar{A} \# \bar{C}$. Hence all points constructed from these points by Schroeter's construction lie on Γ. *q.e.d.*

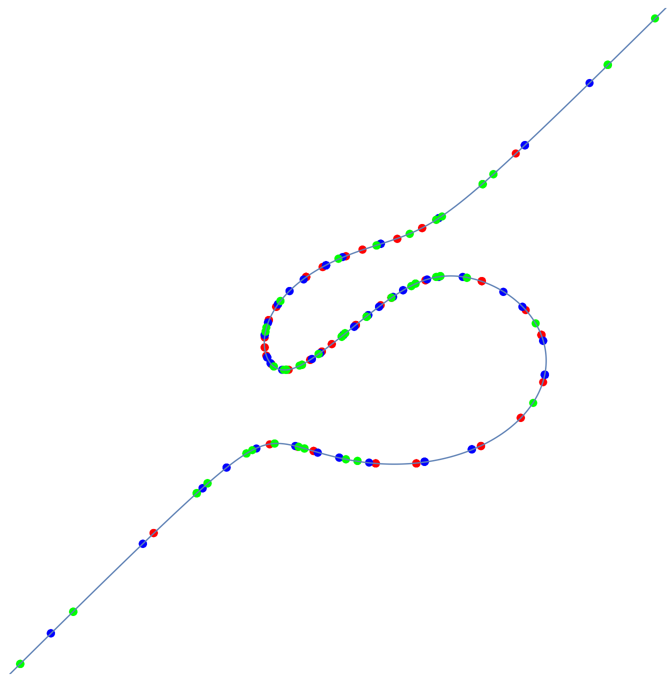

Figure 8: Schroeter pairs P (red), $\bar{P}$ (blue), and intersection points $P\#P = \bar{P}\#\bar{P}$ of the corresponding tangents (green).

Remarks. Let Γ_0 be the cubic curve passing through $A, \bar{A}$, $B, \bar{B}$, $C, \bar{C}$, D, E, F, let $\mathscr{O}$ be a point of inflection of Γ_0, and let $E_0 = (\Gamma_0, \mathscr{O}, +)$ be the corresponding elliptic curve.

(1) If C_n is a cyclic group of order n, then there is a point on Γ_0 of order n (with respect to E_0). This implies that if we choose the six starting points in a finite subgroup of E_0, then Schroeter's construction "closes" after finitely many steps and we end up with just finitely many points. However, if our 6 starting points are all rational and we obtain more than 16 points with Schroeter's construction, then, by Mazur's Theorem, we obtain infinitely many rational points on the cubic curve Γ_0.

(2) If the elliptic curve E_0 has three points of order 2, then one of them, say T, has the property that for any point P on Γ_0 we have $\bar{P} = P + T$. In particular, we have $\bar{T} = T + T = \mathscr{O}$. Furthermore, for the other two points of order 2, say S_1 and S_2, we have $S_1 = S_2 + T$ and $S_2 = S_1 + T$, *i.e.*, $S_1 = \bar{S}_2$.

(3) If we choose another point of inflection $\mathscr{O}'$ on the cubic curve Γ_0, we obtain a different elliptic curve E_0'. In particular, we obtain different inverses of the constructed points, even though the constructed points are exactly the same (see Fig. 9).

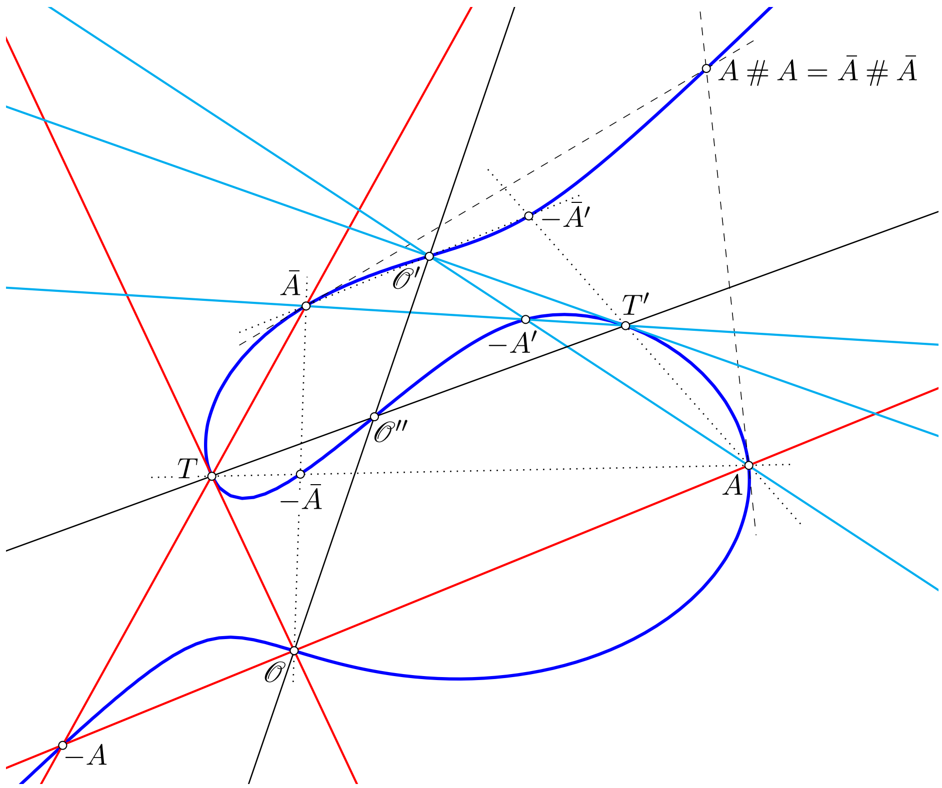

Figure 9: $A, \bar{A}$ is a Schroeter pair, in particular $A \# A = \bar{A} \# \bar{A}$. With respect to $\mathscr{O}$, we get the points $-A, -\bar{A}$, and the point $T = \bar{A} - A = A - \bar{A}$ of order 2. With respect to $\mathscr{O}'$, we get the points $-A', -\bar{A}'$, and the point $T' = \bar{A} - A' = A - \bar{A}'$ of order 2. The three points $\mathscr{O}, \mathscr{O}', \mathscr{O}''$ of inflection are collinear. The lines TT' and $\mathscr{O}\mathscr{O}'$ meet in $\mathscr{O}''$.

Example. Let $A, \bar{A}, B, \bar{B}, C, \bar{C}$ be six different starting points for Schroeter's construction such that no three points are co-linear. By a projective transformation, we can move $A \mapsto (0,0,1)$, $\bar{A} \mapsto (0,1,0)$, $B \mapsto (1,0,0)$, $\bar{B} \mapsto (1,1,1)$, $C \mapsto (C_x, C_y, 1)$, $\bar{C} \mapsto (\bar{C}_x, \bar{C}_y, 1)$. Then, the corresponding cubic curve Γ we obtain by Schroeter's construction is given by the following equation:

$$\begin{aligned}\Gamma: \quad & xy^2 - x^2y + x^2\, C_y\bar{C}_y + y^2\left(C_x\bar{C}_x - C_x - \bar{C}_x\right) \\ & + xy\left(C_x + \bar{C}_x - C_y\bar{C}_x - C_x\bar{C}_y\right) - x\, C_y\bar{C}_y + y\left(C_y\bar{C}_x + C_x\bar{C}_y - C_x\bar{C}_x\right) = 0\end{aligned}$$

4 Elliptic Curves with Torsion Group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

As a first application of Schroeter's construction we provide a new parametrisation of elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. This parametrisation was the nucleus of the characterisation of elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and positive rank given in [5]. For other new parametrisations – which are different to the parametrisations given by Kubert [7] and Rabarison [11] – of elliptic curves with torsion group $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, and $\mathbb{Z}/14\mathbb{Z}$ obtained by Schroeter's construction see [6].

Let $\Gamma_{a,b}:\ y^2 = x^3 + ax^2 + bx$ be a regular curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ over $\mathbb{Q}$. In homogeneous coordinates, the curve $\Gamma_{a,b}$ becomes

$$\Gamma:\ Y^2Z = X^3 + aX^2Z + bXZ^2\,.$$

Assume now that $\tilde{A} = \left(\frac{n_0}{m_0}, \frac{n_1}{m_1}, 1\right)$ is a rational point on the cubic Γ, where n_0, m_0, n_1, m_1 are integers and $n_0 \neq 0 \neq n_1$. Then the point $(1,1,1)$ is on the curve

$$\tfrac{n_1^2}{m_1^2}Y^2Z = \tfrac{n_0^3}{m_0^3}X^3 + a\tfrac{n_0^2}{m_0^2}X^2Z + b\tfrac{n_0}{m_0}XZ^2\,.$$

Now, by exchanging X and Z (*i.e.*, $(X,Y,Z) \mapsto (Z,Y,X)$), de-homogenising with respect to the third coordinate (*i.e.*, $(Z,Y,X) \mapsto (\frac{Z}{X}, \frac{Y}{X}, 1)$), and multiplying with $\frac{m_1^2}{n_1^2}$, we obtain that the point $A = (1,1)$ is on the curve

$$\Gamma_{\alpha,\beta,\gamma}:\ y^2x = \alpha + \beta x + \gamma x^2\,,$$

where

$$\alpha = \frac{n_0^3 \cdot m_1^2}{m_0^3 \cdot n_1^2}\,, \qquad \beta = a \cdot \frac{n_0^2 \cdot m_1^2}{m_0^2 \cdot n_1^2}\,, \qquad \gamma = b \cdot \frac{n_0 \cdot m_1^2}{m_0 \cdot n_1^2}\,.$$

Notice that since $A = (1,1)$ is on $\Gamma_{\alpha,\beta,\gamma}$, we have $\alpha + \beta + \gamma = 1$, and recall that if $\tilde{A} = \tilde{B} + \tilde{B}$ for some rational point $\tilde{B}$ on Γ, then n_0 and m_0 are perfect squares.

In homogeneous coordinates, the neutral element of $\Gamma_{\alpha,\beta,\gamma}$ is $\mathscr{O} = (0,1,0)$ and the image under Φ of the point $(0,0,1)$ on $\Gamma_{a,b}$ is $T = (1,0,0)$. With respect to the curve $\Gamma_{\alpha,\beta,\gamma}$, we can compute the conjugate of a point by the following

Fact 12. *Let $P = (x_1, y_1)$ be a point on $\Gamma_{\alpha,\beta,\gamma}$. Then*

$$\bar{P} = \left(\frac{\alpha}{\gamma x_1}, -y_1\right).$$

Proof. Let $P = (x_1, y_1)$ be a point on $\Gamma_{\alpha,\beta,\gamma}$. Then

$$y_1^2 = \frac{\alpha}{x_1} + \beta + \gamma x_1\,,$$

which implies that x_1 is a root of

$$x^2\gamma + x(\beta - y_1^2) + \alpha = \frac{(x - x_1)(x \cdot \gamma x_1 - \alpha)}{x_1}\,.$$

The other root is $\frac{\alpha}{\gamma x_1}$, and hence, $\left(\frac{\alpha}{\gamma x_1}, y_1\right)$ is a point on $\Gamma_{\alpha,\beta,\gamma}$. Now, since $\bar{P} = T + P$ and $T = (1, 0, 0)$, we have $\bar{P} = (x_2, -y_1)$, and therefore, $\bar{P} = \left(\frac{\alpha}{\gamma x_1}, -y_1\right)$. *q.e.d.*

Let $\tilde{A}$ be a rational point on $\Gamma_{a,b}$ of order 4, and let $\tilde{B}$ be such that $\tilde{B} + \tilde{B} = \tilde{A}$. Furthermore, let $\tilde{C} = \tilde{A} + \tilde{B}$, let $\tilde{T} = (0, 0)$, and let $\tilde{S}$ be another rational point of order 2. Finally, for a point $\tilde{P}$ on $\Gamma_{a,b}$, define $\tilde{P}_1 := \tilde{S} + \tilde{P}$. Now, there is a rational projective transformation Φ which maps the point $\tilde{A}$ to the point $A = (1, 1)$ and the curve $\Gamma_{a,b}$ to the curve $\Gamma_{\alpha,\beta,\gamma}$. Notice that since $\tilde{B} + \tilde{B} = \tilde{A}$, α is a square, say $\alpha = \left(\frac{p}{q}\right)^2$ for some $\frac{p}{q} \in \mathbb{Q}$.

Let $T := \Phi(\tilde{T})$, $B := \Phi(\tilde{B})$, $C := \Phi(\tilde{C})$, and $S := \Phi(\tilde{S})$. Then, for $A, -A, \bar{A}, \ldots$ we obtain the following correspondence between these points on $\Gamma_{\alpha,\beta,\gamma}$ and the elements of the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$:

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,4)$	$(0,5)$	$(0,6)$	$(0,7)$
$\Gamma_{\alpha,\beta,\gamma}$	$\mathscr{O}$	B	A	C	T	$\bar{B}$	$\bar{A}$	$\bar{C}$
$\Gamma_{\alpha,\beta,\gamma}$	S	B_1	A_1	C_1	$\bar{S}$	$\bar{B}_1$	$\bar{A}_1$	$\bar{C}_1$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$	$(1,5)$	$(1,6)$	$(1,7)$

Let us now compute γ.

Lemma 13. *$\gamma = \alpha$.*

Proof. First, notice that $\bar{A} = -A$, and since $A = (1, 1)$ we have $\bar{A} = (\frac{\alpha}{\gamma}, -1)$. Thus, $\frac{\alpha}{\gamma} = 1$ which implies $\alpha = \gamma$. *q.e.d.*

By considering the points S and $\bar{S}$, we obtain the following result.

Lemma 14. *If $\alpha = \left(\frac{p}{q}\right)^2$ for $\frac{p}{q} \in \mathbb{Q}$, then there are $r, s \in \mathbb{N}$ with $(r, s) = 1$ such that*

$$p = \pm rs \quad \textit{and} \quad q = \pm(r^2 + s^2)\,.$$

Proof. Let $\alpha = \gamma = u^2$ and $u = \frac{p}{q}$. Since the y-coordinate of the points S and $\bar{S}$ equals 0, for $S = (x, 0)$ we have $u^2 + (1 - 2u^2)x + u^2x^2 = 0$. Hence,

$$x = \frac{2u^2 - 1 \pm \sqrt{1 - 4u^2}}{2u^2}\,,$$

and since $x \in \mathbb{Q}$, we have $1 - 4u^2 = \square$. Thus,

$$1 - \frac{4p^2}{q^2} = \frac{q^2 - 4p^2}{q^2} = \square\,,$$

which implies $q^2 - 4p^2 = q^2 - (2p)^2 = \square$. Since $(p, q) = 1$, there are some $r, s \in \mathbb{N}$ with $(r, s) = 1$ such that $p = \pm rs$ and $q = \pm(r^2 + s^2)$. *q.e.d.*

Using the fact that $B \# B = -A$, we can show the following result.

Lemma 15. *For $p = \pm rs$ and $q = \pm(r^2 + s^2)$ we find $m, n \in \mathbb{N}$ such that $r = 2mn$ and $s = m^2 - n^2$.*

Proof. First notice that $B \# B = -A$ and that $-\bar{A} = A = (1, 1)$. Let $B = (x_2, y_2)$. Then, since $\alpha = \gamma$, $\bar{B} = (\frac{1}{x_2}, -y_2)$. Since $B \# B = -A$, the points $B, \bar{B}, A$ are collinear, which implies that

$$y_2 = -\frac{x_2 + 1}{x_2 - 1}.$$

Now, since B is on the curve, we have

$$y_2^2 x_2 = \alpha + (1 - 2\alpha) x_2 + \alpha x_2^2,$$

and for $\alpha = \frac{r^2 s^2}{(r^2 + s^2)}$ we obtain

$$x_2 = \frac{\pm r^2 + rs \pm s^2 \pm (r - s)\sqrt{r^2 + s^2}}{rs}.$$

So, since $x_2 \in \mathbb{Q}$, we have $r^2 + s^2 = \square$, which implies that there are $m, n \in \mathbb{N}$ with $(m, n) = 1$ such that $r = 2mn$ and $s = m^2 - n^2$. *q.e.d.*

Now, we are ready to give a parametrisation of elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

Theorem 16. *Let $\frac{m}{n} \neq 1$ be a positive rational in lowest terms and let*

$$a_1 = (2mn)^4 + (m^2 - n^2)^4, \qquad b_1 = (2mn)^4 \cdot (m^2 - n^2)^4.$$

Then the curve

$$\Gamma_{a_1,b_1} : y^2 = x^3 + a_1 x^2 + b_1 x$$

is an elliptic curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Conversely, if $\Gamma_{a,b}$ is a regular elliptic curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, then there exists a positive rational $\frac{m}{n}$ such that $\Gamma_{a,b}$ is isomorphic to Γ_{a_1,b_1}.

Proof. By construction, for any relatively prime positive integers m and n, the corresponding elliptic curve Γ_{a_1,b_1} has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

On the other hand, if $\Gamma_{a,b}$ is an elliptic curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, then we find a rational point $\tilde{A}$ on $\Gamma_{a,b}$ of order 4, and by construction we find relatively prime positive integers m and n such that $\Gamma_{a,b}$ is isomorphic to the curve Γ_{a_1,b_1}. *q.e.d.*

As a last remark we would like to mention that for any positive integers m and n we have $(m^2-n^2)^2+(2mn)^2=\square$, *i.e.*, for $k=m^2-n^2$ and $l=2mn$, (k,l) is a so-called pythagorean pair. Now, in [5] it is shown that the corresponding elliptic curve Γ_{a_1,b_1} has positive rank over $\mathbb{Q}$ if and only if there exists a pythagorean pair (r,s) such that $(k^2\cdot r,\, l^2\cdot s)$ is a pythagorean pair.

5 Configurations on Elliptic Curves

In the complex projective plane, a generic elliptic curve has nine inflection points, located in groups of three on a total of 12 lines. The nine inflection points and 12 lines form the so-called Hesse configuration $(9_4, 12_3)$: See Figure 10.

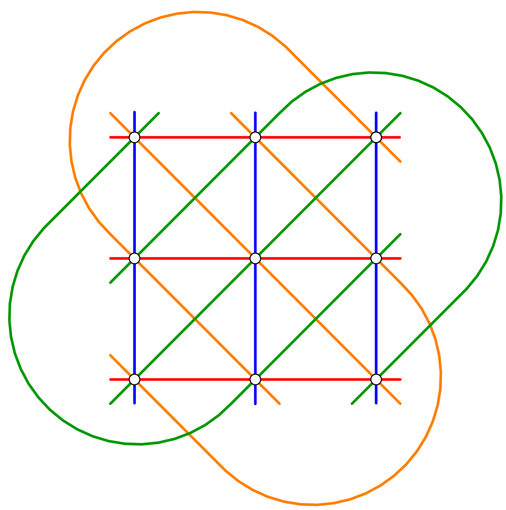

Figure 10: The Hesse configuration $(9_4, 12_3)$: A model of a finite affine plane.

Recall that a $(p_\lambda,\, \ell_\pi)$ configuration consists of p points and ℓ lines in the real (or complex) projective plane arranged in such a way that each of the p points is incident to λ lines, while each of the ℓ-lines is incident to π points. As usual, we write (n_k) for a configuration of the type (n_k, n_k) (see [4] as a main reference for configurations). Schroeter gave in [12] a proof that (n_3) configurations can be realized in the real projective plane for $n \geq 9$. His construction relies on properties of point sets on cubic curves. Moreover, since all steps in his construction can be carried out with ruler alone, the corresponding configurations can also be geometrically realized in the rational plane.

As an application of Schroeter's construction we provide now a few configurations whose points belong to an elliptic curve.

To warm up, assume that $A, \bar{A},\ B, \bar{B},\ C, \bar{C}$ are six pairwise distinct points in the real projective plane such that the three pairs of points $A, \bar{A},\ B, \bar{B},\ C, \bar{C}$ are the pairs of opposite vertices of the same complete quadrilateral. In other words, assume that A, B, C; $\bar{B}, \bar{A}, C$; $A, \bar{B}, \bar{C}$; and $B, \bar{A}, \bar{C}$ are collinear. Then the six points $A, \bar{A}$, $B, \bar{B}$, $C, \bar{C}$ together with the four lines AC, $\bar{A}C$, $A\bar{C}$, $\bar{A}\bar{C}$ is a $(6_2, 4_3)$ configuration. This configuration we find on every elliptic curve Γ_6 which contains the torsion subgroup $\mathbb{Z}/6\mathbb{Z}$. The following table and Figure 11 shows how we can assign the six points $A, \bar{A}$, $B, \bar{B}$, $C, \bar{C}$ to the elements of the group $\mathbb{Z}/6\mathbb{Z}$:

$\mathbb{Z}/6\mathbb{Z}$	0	1	2	3	4	5
Γ_6	$\bar{C} = \mathscr{O}$	A	B	$C = T$	$\bar{A}$	$\bar{B}$

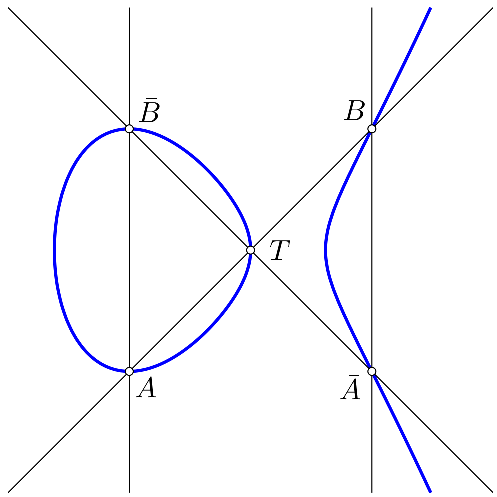

Figure 11: A $(6_2, 4_3)$ configuration on an elliptic curve Γ_6.

To construct a $(12_4, 16_3)$ configuration whose points are on an elliptic curve, we start with an elliptic curve $\Gamma_{2\times 6}$ which contains the torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, assign the six points $A, \bar{A}$, $B, \bar{B}$, $C, \bar{C}$ in a suitable way to the elements of the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (see the table below and Figure 12), and construct with Schroeter's construction with these six points the points $D, \bar{D}$, $E, \bar{E}$, and $F, \bar{F}$:

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,4)$	$(0,5)$
$\Gamma_{2\times 6}$	$\bar{D} = \mathscr{O}$	A	B	$D = T$	$\bar{A}$	$\bar{B}$
$\Gamma_{2\times 6}$	$\bar{F}$	C	E	F	$\bar{C}$	$\bar{E}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$	$(1,5)$

Notice that $A, \bar{A}$, $B, \bar{B}$, $D, \bar{D}$, as well as $C, \bar{C}$, $E, \bar{E}$, $D, \bar{D}$, are the pairs of opposite vertices of a complete quadrilateral. These two complete quadrilaterals consist of 10 points and 8 lines. Together with the 2 points F and $\bar{F}$, and the 4 lines AE,

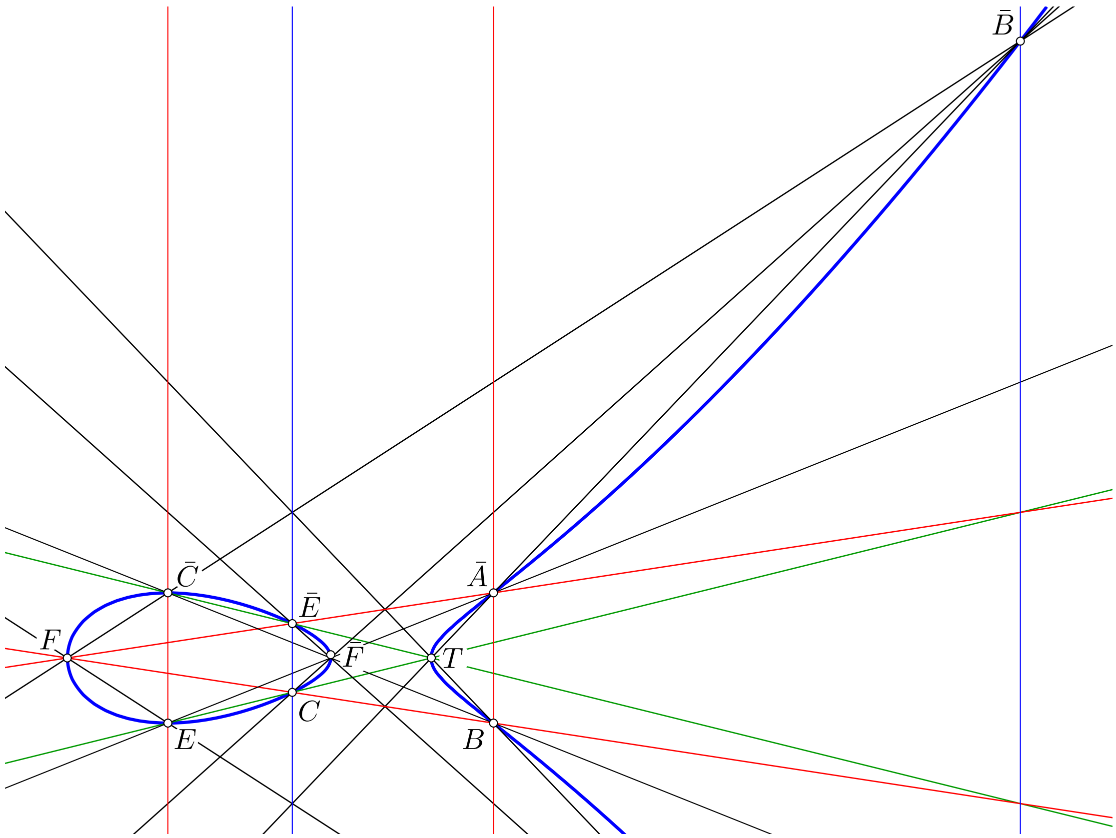

Figure 12: A $(12_4, 16_3)$ configuration on an elliptic curve $\Gamma_{2\times 6}$.

$\bar{A}\bar{E}$, $\bar{A}E$, $A\bar{E}$, we obtain a $(12_4, 16_3)$ configuration where all 12 points belong to an elliptic curve $\Gamma_{2\times 6}$. $(12_4, 16_3)$ configurations have been discussed quite intensively in the literature (see, *e.g.*, [3, 8, 10] and the references therein), the more astonishing it is how easily Schroeter's construction yields this configuration on an elliptic curve.

As a further example of Schroeter's construction, we construct a $(24_6, 48_3)$ configuration whose points are on an elliptic curve. In order to simplify the notation, we introduce the following terminology: For 4 pairwise distinct points $P, \bar{P}, Q, \bar{Q}$, let $(P, Q : S)$ be an abbreviation for the construction of the two points $S, \bar{S}$, where

$$S := PQ \wedge \bar{P}\bar{Q} \qquad \text{and} \qquad \bar{S} := P\bar{Q} \wedge \bar{P}Q\,.$$

Let Γ_{26} be an elliptic curve which contains the torsion subgroup $\mathbb{Z}/26\mathbb{Z}$, and let us assign the points $\mathscr{O}, T, A, \bar{A}, B, \bar{B}, C, \bar{C}$ to the elements $0, 13, 2, 15, 6, 19, 8, 21$, respectively. Now, we carry out the following constructions in the given order:

1. $(A, B : D)$	2. $(A, C : E)$	3. $(B, E : F)$	4. $(C, F : G)$
5. $(A, G : H)$	6. $(F, H : J)$	7. $(D, J : K)$	8. $(H, K : L)$
9. $(C, L : M)$	10. $(B, K : M)$	11. $(E, J : M)$	12. $(D, G : L)$

All together, we have constructed 24 points (including the six points $A, \bar{A}$, $B, \bar{B}$, $C, \bar{C}$):

$\mathbb{Z}/26\mathbb{Z}$	2	4	6	8	10	12	14	16	18	20	22	24
Γ_{26}	A	F	B	C	H	J	G	E	D	L	K	M
Γ_{26}	$\bar{A}$	$\bar{F}$	$\bar{B}$	$\bar{C}$	$\bar{H}$	$\bar{J}$	$\bar{G}$	$\bar{E}$	$\bar{D}$	$\bar{L}$	$\bar{K}$	$\bar{M}$
$\mathbb{Z}/26\mathbb{Z}$	15	17	19	21	23	25	1	3	5	7	9	11

In addition, we have constructed 48 lines and each of the 24 points is incident to 6 lines, while each of the 48-lines is incident to 3 points. Therefore, we have a $(24_6, 48_3)$ configuration all whose points are on the elliptic curve Γ_{26}. Notice that if we just consider the 12 points $A, B, C, \ldots, M$ and the 12 lines ABD, ACE, $BEF, \ldots, DGL$, then we obtain a (12_3) configuration (*i.e.*, a $(12_3, 12_3)$ configuration), all whose points are on the elliptic curve Γ_{26}.

Acknowledgement

We would like to thank the referee for his or her careful reading and the suggestions that helped improve the substance of the article.

References

[1] Michel Chasles. *Aperçu historique sur l'origine et le développement des méthodes en géométrie.* Éditions Jacques Gabay, Sceaux, 1989. Reprint of the 1837 original.

[2] H. S. M. Coxeter and S. L. Greitzer. *Geometry revisited*, volume 19 of *New Mathematical Library.* Random House, Inc., New York, 1967.

[3] Harald Gropp. The construction of all configurations $(12_4, 16_3)$. In *Fourth Czechoslovakian Symposium on Combinatorics, Graphs and Complexity (Prachatice, 1990)*, volume 51 of *Ann. Discrete Math.*, pages 85–91. North-Holland, Amsterdam, 1992.

[4] Branko Grünbaum. *Configurations of points and lines*, volume 103 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, 2009.

[5] Lorenz Halbeisen and Norbert Hungerbühler. Pairing pythagorean pairs. *Journal of Number Theory* (to appear). arxiv.org/abs/2101.08163

[6] Lorenz Halbeisen, Norbert Hungerbühler, and Arman Shamsi Zargar. New parametrisations of elliptic curves with torsion groups $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, and $\mathbb{Z}/14\mathbb{Z}$. arxiv.org/abs/2106.06861

[7] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proceedings of the London Mathematical Society (3)*, 33(2):193–237, 1976.

[8] N. S. Mendelsohn, R. Padmanabhan, and B. Wolk. Designs embeddable in a plane cubic curve. (Part 2 of Planar projective configurations). *Note Mat.*, 7(1):113–148, 1987.

[9] N. S. Mendelsohn, R. Padmanabhan, and Barry Wolk. Straight edge constructions on planar cubic curves. *C. R. Math. Rep. Acad. Sci. Canada*, 10(2):77–82, 1988.

[10] Václav Metelka. On two special configurations $(12_4, 16_3)$. *Časopis Pěst. Mat.*, 110(4):351–355, 1985.

[11] F. Patrick Rabarison. Structure de torsion des courbes elliptiques sur les corps quadratiques. *Acta Arithmetica*, 144(1):17–52, 2010.

[12] Heinrich Schroeter. *Die Theorie der ebenen Curven dritter Ordnung.* B. G. Teubner, Leipzig, 1888.

[13] Heinrich Schröter. Ueber eine besondere Curve 3^{ter} Ordnung und eine einfache Erzeugungsart der allgemeinen Curve 3^{ter} Ordnung. *Mathematische Annalen*, 5(1):50–82, 1872.

[14] Heinrich Schröter. Ueber Curven dritter Ordnung. *Mathematische Annalen*, 6(1):85–111, 1873.