1

The Manin-Mumford Conjecture, an elliptic Curve, its Torsion Points & their Galois Orbits

P. Habegger

Abstract

This is an extended write-up of my five hour lecture course in July 2013 on applications of o-minimality to problems in Diophantine Geometry. The course covered arithmetic properties of torsion points on elliptic curves and how they combine with the Pila-Wilkie Point Counting Theorem and the Ax-Lindemann-Weierstrass Theorem to prove a special case of the Manin-Mumford Conjecture.

1 Overview

These notes are a write-up of my lecture course titled *Diophantine Applications* which was part of the *LMS-EPSRC Short Instructional Course – O-Minimality and Diophantine Geometry* in Manchester, July 2013. The purpose of the short course was to present recent developments involving the interaction of methods from Model Theory with problems in Number Theory, most notably the André-Oort and Manin-Mumford Conjectures, to an audience of students in Model Theory and Number Theory.

At the heart of this connection is the powerful Pila-Wilkie Counting Theorem [26]. It gives upper bounds for the number of rational points on sets which are definable in an o-minimal structure.

The Manin-Mumford Conjecture concerns the distribution of points of finite order on an abelian variety with respect to the Zariski topology. We give a rather general version of this conjecture, later on we often work in the situation

O-Minimality and Diophantine Geometry, ed. G. O. Jones and A. J. Wilkie. Published by Cambridge University Press. © Cambridge University Press 2015.

where the base field is $\overline{\mathbf{Q}}$, the algebraic closure of $\mathbf{Q}$ inside the field of complex numbers $\mathbf{C}$. But soon we concentrate on the power of an elliptic curve.

Theorem 1.1 (Raynaud [32]) *Let A be an abelian variety defined over $\mathbf{C}$. Let $\mathcal{X}$ be an irreducible closed subvariety of A. We write*

$$A_{tors} = \{P \in A(\mathbf{C});\ P \textit{ has finite order}\}$$

for the group of all torsion points of A. Then $\mathcal{X}(\mathbf{C}) \cap A_{tors}$ is Zariski dense in $\mathcal{X}$ if and only if $\mathcal{X}$ is an irreducible component of an algebraic subgroup of A.

Any algebraic subgroup of A is a finite union of translates of an irreducible algebraic subgroup by points of finite order. The theory of abelian varieties guarantees that the torsion points lie Zariski dense on any algebraic subgroup. Showing that torsion points do not lie Zariski dense on a subvariety that is not a component of an algebraic subgroup is the difficult part of the Manin-Mumford Conjecture.

Prior to Raynaud's proof he was able to handle the case of a curve $\mathcal{X}$ [31]. Earlier partial results are due to Bogomolov [3, 4].

Lang [17] was interested in the analogous problem with A replaced by $(\mathbf{C}^\times)^n$, where $R^\times$ denotes the unit group of any ring R. Here the points of finite order are those whose coordinates are roots of unity. In his paper, Lang presents proofs of the Manin-Mumford Conjecture for $(\mathbf{C}^\times)^2$ attributed to Ihara, Serre, and Tate independently. In a paper published in the same year, Mann [20] treated hypersurfaces in any power of $\mathbf{C}^\times$.

Later, Hindry [12] proved the generalization to all semi-abelian varieties defined over $\mathbf{C}$.

In the mean time new proofs of variants of the Manin-Mumford Conjecture using various techniques have appeared in the literature: Hrushovski [16] used the Model Theory of difference fields, Pink-Rössler [28, 29] used classical Algebraic Geometry, and Ratazzi-Ullmo [30] used equidistribution.

Based on a strategy due to Zannier, he himself and Pila [27] used the aforementioned counting theorem and lower bounds for the *Galois orbit* of torsion points to give yet another proof of the Manin-Mumford Conjecture for abelian varieties if the base field is $\overline{\mathbf{Q}}$. This general technique had broad implications for *open* problems in diophantine geometry such as the André-Oort Conjecture [25].

One aim of the short course was to present the ingredients required to prove the Manin-Mumford Conjecture for an algebraic curve inside a product of elliptic curves using the approach laid out in [27]:

- The Pila-Wilkie Counting Theorem.
- An o-minimal approach to the Ax-Lindemann-Weierstrass Theorem which is a special case of Schanuel's Conjecture in functional setting.
- Bounding from below the size of a Galois orbit of point of finite order on an elliptic curve.

This lecture concerns the last part. In Section 2.1 we will give a brief introduction to the relevant parts of the theory of elliptic curves. In Section 2.2 we will see how to attach a function, definable in some o-minimal structure, to the uniformizing map coming from the Weierstrass function. The uniformizing map establishes the link between points of finite order on the elliptic curve and rational points.

On the arithmetic side we will investigate the Galois orbit of a torsion point in Section 3.

Suppose we are presented with an elliptic curve E defined by an equation with coefficients in a number field K and a K-rational point T on E of finite order n. In order to get the method running we require a lower bound

$$[K(T):K] \geq cn^{\delta} \tag{1.1}$$

where $c > 0$ and $\delta > 0$ are constants that are allowed to depend on E but not on T. The left-hand side is precisely the size of the Galois orbit

$$\left\{\sigma(T);\ \sigma \in \mathrm{Gal}(\overline{K}/K)\right\}.$$

The crucial feature of (1.1) is the *polynomial* dependency in n. It is needed to compete with the upper bound coming from the Pila-Wilkie Theorem, as we will see in Section 4. In the multiplicative setting, the lower bound analogous to (1.1) follows from the most basic facts on cyclotomic fields and Euler's totient function. For elliptic curves, one can quite easily prove a sub-polynomial lower bound for $[K(T):K]$. But breaking the polynomial barrier involves more care than in the multiplicative case.

In Section 4 we combine our efforts and rely also on results presented in Jonathan Pila's, Martin Orr's, and Alex Wilkie's notes in this volume to give a proof based on [27] of the Manin-Mumford Conjecture for curves in the power E^g.

Theorem 1.2 *Let E be an elliptic curve defined over a number field K contained in $\mathbf{C}$ and suppose $\mathcal{X} \subseteq E^g$ is an irreducible algebraic curve also defined over K. Then $\mathcal{X}(\mathbf{C}) \cap E^g_{tors}$ is infinite if and only if $\mathcal{X}$ is an irreducible component of an algebraic subgroup of E^g.*

In the appendix we give a proof of a special case of a theorem of Elkies for local height functions on elliptic curves. This inequality leads to a polynomial lower bound for the Galois orbit of a torsion point on an elliptic curve.

Most of the material presented in these lecture notes is classical. No emphasis was made to formulate things in their proper generality; the presentation was chosen to give a pragmatic introduction to the tools required to prove Theorem 1.2. Two excellent starting points for a more detailed overview of the theory of elliptic curves from the arithmetic point of view (and beyond) are books of Silverman [36] and Cassels [7]. For the theory of heights, which also plays an important role in this course, we refer to books of Bombieri and Gubler [5] or Hindry and Silverman [14].

2 Elliptic Curves

2.1 The Group Law and Points of Finite Order

Let K be a subfield of $\mathbf{C}$. An elliptic curve E defined over K is a smooth, projective curve of genus 1 with a prescribed K-rational point P_0. In this situation E can be represented by a Weierstrass equation

$$y^2 = 4x^3 - g_2x - g_3 \tag{1.2}$$

where $g_2, g_3 \in K$ satisfy $g_2^3 - 27g_3^2 \neq 0$. This condition guarantees that we obtain a smooth curve.

Certainly, (1.2) defines an affine curve, whereas the elliptic curve E is projective by definition. It is silently understood that E is isomorphic to the projective curve in $\mathbf{P}^2$ cut out by the homogenized equation

$$y^2z = 4x^3 - g_2xz^2 - g_3z^3.$$

The K-rational point P_0 then corresponds to $[0:1:0]$. It is the only point missing from the affine curve defined by (1.2).

The Weierstrass equation is by no means uniquely determined by (E, P_0). Indeed, any $u \in K^\times$ can be used to make a change of coordinates

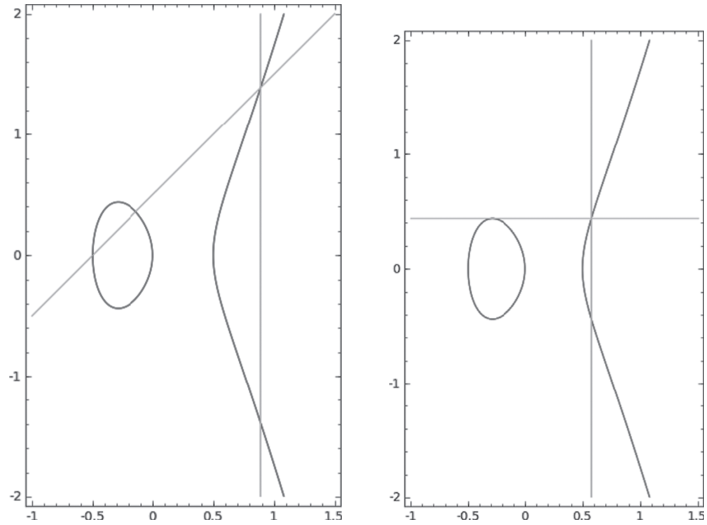
$$(x', y') = (u^2x, u^3y)$$

and obtain a new Weierstrass equation

$$y'^2 = 4x'^3 - g_2'x' - g_3' \quad \text{with} \quad g_2' = u^4g_2 \quad \text{and} \quad g_3' = u^6g_3$$

for E.

One of the most basic, but important, facts is that the points of E carry the structure of an abelian group with neutral element P_0. There are several ways to



(A) Summing two distinct points

(B) Doubling a point

Figure 1.1 The chord and tangent construction for $y^2 = 4x^3 - x$

define the group law. Possibly the most straightforward method is via the well known chord and tangent construction which has a very geometric flavor. The procedure is illustrated in Figure 1.1. Given two *distinct* points on the affine portion of E we connect them by a line. This line intersects the elliptic curve in a third point which, after changing the sign of the y-coordinate, is the sum of the original points, cf. 1.1A. If the original points differ in the y-coordinate only, then their sum is the neutral element. We extend this to a binary operation on all points of E by treating P_0 as the neutral element in a group law. Adding a point on the affine part to itself requires some more care; now we intersect the tangent of E at this point to get a third point. The duplicate of the original point is obtained by again flipping the sign of the y-coordinate, cf. 1.1B. Of course, we define the duplication of P_0 to be again P_0.

The binary operation described above is given by rational functions with coefficients in K. With the exception of the law of associativity it is easy to see that this binary operation defines an abelian group law on the K-rational points of E with neutral element P_0; see Chapter III.2 [36] for explicit formulas. At least in principle it should be possible to verify associativity by an elaborate computation. On the other hand, there are approaches using the Riemann-Roch Theorem (Proposition 3.4 in Chapter III [36]) and a geometric one in Chapter 7 [7].

To simplify notation we write 0 for the neutral element P_0 and use $+$ to denote the group law. For each $n \in \mathbf{Z}$ we have the multiplication-by-n map

$$[n] : E(K) \to E(K).$$

It is a non-constant morphism $[n] : E \to E$ of algebraic curves. So $[n]$ can be represented by rational functions with coefficients in K.

Example 1.3 *Let us see how things look for $n = 2$. If $(x, y) \in E(\mathbf{C}) \smallsetminus \{0\}$ and $y \neq 0$, then*

$$[2](x,y) = \left(\frac{x^4 + \frac{g_2}{2}x^2 + 2g_3x + \frac{g_2^2}{16}}{4x^3 - g_2x - g_3}, \right.$$
$$\left. \frac{2x^6 - \frac{5g_2}{2}x^4 - 10g_3x^3 - \frac{5}{8}g_2^2x^2 - \frac{g_2g_3}{2}x + \frac{g_2^3}{32} - g_3^2}{y^3} \right), \quad (1.3)$$

which is well defined as $4x^3 - g_2x - g_3 = y^2 \neq 0$. Roots of the cubic $4x^3 - g_2x - g_3$ are precisely the x-coordinates of the points in $E(\mathbf{C})$ of order 2.

Definition 1.4 The group of torsion points of E is

$$E_{\text{tors}} = \{T \in E(\mathbf{C});\ \text{there exists an integer } n \geq 1 \text{ with } [n](T) = 0\}.$$

If $n \in \mathbf{N} = \{1, 2, 3, \ldots\}$ we write

$$E[n] = \{T \in E_{\text{tors}};\ [n](T) = 0\}$$

for the group of points of finite order dividing n.

The structure of E_{tors} and $E[n]$ as abelian groups is well known. We will uncover both in the next section using the Weierstrass function.

Torsion points of E are algebraic over K, i.e.

$$E_{\text{tors}} = \{T \in E(\overline{K});\ T \in E_{\text{tors}}\}$$

where $\overline{K}$ is the algebraic closure of K in $\mathbf{C}$. We reproduce this well known proof here. It involves the action of $\text{Aut}(\mathbf{C}/K)$, the field automorphisms of $\mathbf{C}$ that fix elements of K, a central concept for our arguments later on. If $P \in E(\mathbf{C})$, then

$$P \mapsto \sigma(P)$$

defines an automorphism of $E(\mathbf{C})$ as an abelian group; here σ acts on the coordinates of P if $P \neq 0$ and $\sigma(0) = 0$. Recall that $[n]$ is represented by rational functions with coefficients in K and so

$$\sigma([n](P)) = [n](\sigma(P)).$$

CAMBRIDGE

Cambridge University Press
978-1-107-46249-6 - O-Minimality and Diophantine Geometry: London Mathematical Society Lecture Note Series: 421
Edited by G. O. Jones and A. J. Wilkie
Excerpt
More information

Say T has finite order $n \geq 1$, then so does $\sigma(T)$. In particular, the orbit

$$\{\sigma(T);\ \sigma \in \mathrm{Aut}(\mathbf{C}/K)\} \tag{1.4}$$

is contained in a fiber of $[n]$. As $[n]$ is a non-constant morphism, all these fibers are finite and in particular $E[n]$ is finite. Thus (1.4) is finite. In particular, T cannot have a coordinate that is transcendental over K. This yields $T \in E(\overline{K})$, as desired. So already the Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on $E[n]$ and E_{tors}.

It is not difficult to adapt the argument above to use only the duplication morphism $[2]$, which we described explicitly in Example 1.3, and its iterates $[2^n]$. Indeed, by the Pigeonhole Principle $T \in E(\mathbf{C})$ is torsion if and only if $[2^n](T) = [2^m](T)$ for integers $0 \leq n < m$.

2.2 Uniformizing the complex points E

Here we describe an elliptic curve E from the analytic point of view. In the end it is the interplay between the algebraic and the analytic world that makes the strategy described in Section 1 feasible. Our goal is to attach a definable function to the inverse of the uniformizing map determined by a Weierstrass equation.

Suppose E is presented by the Weierstrass equation (1.2) with $g_2, g_3 \in \mathbf{C}$. There is a unique discrete, rank 2 subgroup $\Omega \subseteq \mathbf{C}$, called the periods of E, with the following properties.

- The series

  $$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega \smallsetminus \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

  determines a meromorphic, Ω-periodic function with poles of order 2 at points of Ω and no poles in $\mathbf{C} \smallsetminus \Omega$. It is called the Weierstrass function attached to (1.2). Moreover, this function satisfies the differential equation

  $$\wp'^2 = 4\wp^3 - g_2\wp - g_3$$

  and induces a surjective, analytic homomorphism of groups $u : \mathbf{C} \to E(\mathbf{C})$ defined by

  $$u : z \mapsto \begin{cases} [\wp(z) : \wp'(z) : 1] & : \text{ if } z \in \mathbf{C} \smallsetminus \Omega, \\ [0 : 1 : 0] & : \text{ if } z \in \Omega \end{cases}$$

  with kernel Ω.
- The coefficients in (1.2) are related to the periods by

  $$g_2 = 60 \sum_{\omega \in \Omega \smallsetminus \{0\}} \frac{1}{\omega^4} \quad \text{and} \quad g_3 = 140 \sum_{\omega \in \Omega \smallsetminus \{0\}} \frac{1}{\omega^6}.$$

The existence of Ω follows from the theory of modular functions, see for example Proposition 5, Chapter VII [34]. Weierstrass functions are studied in Chapter VI [36].

Let us fix a $\mathbf{Z}$-basis (ω_1, ω_2) of the periods Ω. We can think of $u(\nu_1\omega_1 + \nu_2\omega_2)$ as a function in the real coordinates ν_1 and ν_2. In these coordinates, the period lattice Ω becomes $\mathbf{Z}^2$. So u induces a surjective group homomorphism $\mathbf{R}^2 \to E(\mathbf{C})$ with kernel $\mathbf{Z}^2$. Apart from the integral points $\mathbf{Z}^2$ this homomorphism takes values in the affine part of E, i.e. the solutions in $\mathbf{C}^2$ of (1.2). The preimage of E_{tors} is precisely $\mathbf{Q}^2$ and we get isomorphisms of groups

$$E_{\text{tors}} \cong (\mathbf{Q}/\mathbf{Z})^2 \quad \text{and} \quad E[n] \cong (\mathbf{Z}/n\mathbf{Z})^2 \tag{1.5}$$

for all $n \in \mathbf{N}$.

Our goal is to uniformize the affine part of E by a function that is definable in the o-minimal structure $\mathbf{R}_{\text{an}}$, the o-minimal structure generated by restricted real analytic functions. A reasonable candidate is

$$\begin{aligned} [-1/2, 1/2]^2 \smallsetminus \{(0,0)\} &\to \mathbf{C}^2 = \mathbf{R}^4 \\ (\nu_1, \nu_2) &\mapsto (\wp(\nu_1\omega_1 + \nu_2\omega_2), \wp'(\nu_1\omega_1 + \nu_2\omega_2)) \end{aligned} \tag{1.6}$$

where we identify the target $\mathbf{C}^2$ with $\mathbf{R}^4$ by taking real and imaginary parts on both factors of $\mathbf{C}^2$.

However, we must take some care, as (1.6) does not extend to a real analytic function on an open neighborhood of the compact set $[-1/2, 1/2]^2$ due to the pole at $(0, 0)$ This issue is not too severe. We must merely remind ourselves that the Weierstrass function $\wp$ has a double pole at $z = 0$ and hence $\wp'$ has a triple pole there. In a sufficiently small neighborhood $(-\epsilon, \epsilon)^2$ of $(0, 0)$ the mapping $(\nu_1, \nu_2) \mapsto \wp'(\nu_1\omega_1 + \nu_2\omega_2)$ does not vanish and

$$(\nu_1, \nu_2) \mapsto \left(\frac{\wp(\nu_1\omega_1 + \nu_2\omega_2)}{\wp'(\nu_1\omega_1 + \nu_2\omega_2)}, \frac{1}{\wp'(\nu_1\omega_1 + \nu_2\omega_2)} \right) \in \mathbf{C}^2 \tag{1.7}$$

is real analytic on $(-\epsilon, \epsilon)^2$ if we send $(0, 0)$ to 0. The mapping (1.7) composed with

$$(z, w) \mapsto \begin{cases} (zw^{-1}, w^{-1}) & : \text{if } w \neq 0, \\ (0, 0) & : \text{otherwise} \end{cases} \tag{1.8}$$

coincides outside of $(0, 0)$ with (1.6). Now (1.8) is semi-algebraic and therefore definable in $\mathbf{R}_{\text{an}}$. As the composite of two definable functions is again definable we find that (1.6) is definable in $\mathbf{R}_{\text{an}}$ when restricted to $(-\epsilon, \epsilon)^2 \smallsetminus \{(0, 0)\}$.

Now that we have handled the singularity at the origin, definability of (1.6) in $\mathbf{R}_{\text{an}}$ is straightforward. Indeed, its restriction to the compact set

$[-1/2,1/2]^2 \smallsetminus (-\epsilon,\epsilon)^2$ clearly extends to a real analytic map on some larger open set; take for example $[-3/4,3/4]^2 \smallsetminus [-\epsilon/2,\epsilon/2]^2$.

For technical reasons, i.e. to achieve injectivity, it is convenient to restrict (1.6) further to $(-1/2,1/2]^2 \smallsetminus \{(0,0)\}$. This does not affect the definability property we just proved. We thus obtain a bijection

$$\begin{aligned}(-1/2,1/2]^2 \smallsetminus \{(0,0)\} &\to \{(x,y)\in \mathbf{C}^2;\ y^2 = 4x^3 - g_2x - g_3\}\\ &= E(\mathbf{C}) \smallsetminus \{0\}\end{aligned}$$

which is definable in $\mathbf{R}_{\mathrm{an}}$. We will work with the inverse map

$$\xi : E(\mathbf{C}) \smallsetminus \{0\} \to (-1/2,1/2]^2, \tag{1.9}$$

which is also definable in $\mathbf{R}_{\mathrm{an}}$.

As we started out with a group homomorphism we find $\xi(E_{\mathrm{tors}} \smallsetminus \{0\}) \subseteq \mathbf{Q}^2$. More precisely, if $n \in \mathbf{N}$ and $T \in E_{\mathrm{tors}} \smallsetminus \{0\}$ has order dividing n, then $\xi(T) \in \frac{1}{n}\mathbf{Z}^2$.

This concludes our discussion on definability properties of a single Weierstrass function. Peterzil and Starchenko [24] studied the definability question for a family of Weierstrass functions. In this generality one needs the larger o-minimal structure $\mathbf{R}_{\mathrm{an,exp}}$ generated by $\mathbf{R}_{\mathrm{an}}$ and the exponential function on the reals.

3 Galois Orbits of Torsion Points and Heights

3.1 The Arithmetic of Torsion Points

In this section we discuss Galois theoretic properties of torsion points on an elliptic curve E. As usual, we assume that E is presented by a Weierstrass equation (1.2) with coefficients g_2, g_3 in a field $K \subseteq \mathbf{C}$. Now we will assume in addition that K is a number field.

Roughly speaking, torsion points of E share many arithmetic properties with the roots of unity

$$\mu = \{\zeta \in \mathbf{C}^\times;\ \text{there is } n \in \mathbf{N} \text{ with } \zeta^n = 1\}.$$

Let us also write

$$\mu[n] = \{\zeta \in \mu;\ \zeta^n = 1\}$$

for all $n \in \mathbf{N}$.

In the table below we list some similarities between roots of unity and the torsion points of the elliptic curve E. We retain notation from Section 2.2 and use φ to denote Euler's totient function.

	Roots of unity	Torsion on E
Analytic description	$e^{2\pi\sqrt{-1}\nu}$ with $\nu \in \mathbf{Q}$	$u(\nu_1\omega_1 + \nu_2\omega)$ with $\nu_{1,2} \in \mathbf{Q}$
Group structure	$\mu \cong \mathbf{Q}/\mathbf{Z}$ $\mu[n] \cong \mathbf{Z}/n\mathbf{Z}$	$E_{\mathrm{tors}} \cong (\mathbf{Q}/\mathbf{Z})^2$ $E[n] \cong (\mathbf{Z}/n\mathbf{Z})^2$
Order vs. degree	If $\mathrm{ord}(\zeta) = n$, then $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(n) \geq c\frac{n}{\log\log 3n}$	If $\mathrm{ord}(T) = n$, then $[K(T) : K] \leq n^2$
Field properties	$\mathbf{Q}(\mu[n])/\mathbf{Q}$ Galois with group $(\mathbf{Z}/n\mathbf{Z})^\times = \mathrm{GL}_1(\mathbf{Z}/n\mathbf{Z})$	$K(E[n])/K$ Galois with group isomorphic to a subgroup of $\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$

We now justify the entries in this table. The middle column is classical algebra. The inequality

$$\varphi(n) \geq c\frac{n}{\log\log 3n} \tag{1.10}$$

holds for all $n \geq 1$ where $c > 0$ is an absolute constant by Theorem 328 [10]. Any ζ of order n generates $\mu[n]$. So if $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ then

$$\sigma(\zeta) = \zeta^a$$

for some exponent $a \in \mathbf{Z}$ that is uniquely determined modulo n. As σ is invertible, a must be coprime to n. We obtain a representation

$$\chi_n : \mathrm{Gal}(\mathbf{Q}(\mu[n])/\mathbf{Q}) \to (\mathbf{Z}/n\mathbf{Z})^\times = \mathrm{GL}_1(\mathbf{Z}/n\mathbf{Z})$$

determined by

$$\sigma(\zeta) = \zeta^{\chi_n(\sigma)}.$$

The representation χ_n is independent of the choice of the generator ζ of $\mu[n]$.

The analytic and group theoretic properties of the right column were discussed in Section 2.2 around (1.5). The upper bound for $[K(T):K]$ follows as $\mathrm{Gal}(\overline{K}/K)$ acts on the points of finite order n, of which there are at most n^2. However, if we return for a moment to the larger picture we require *lower bounds* for the Galois orbit of a torsion point to compete with the upper bound from the Pila-Wilkie Theorem. The easily obtainable upper bound in the table is in the wrong direction.