

## THE UNDECIDABILITY OF CYCLOTOMIC TOWERS

CARLOS R. VIDELA

(Communicated by Carl G. Jockusch, Jr.)

ABSTRACT. Let  $\mathbb{Q}(p^\infty)$  be the field obtained by adjoining to  $\mathbb{Q}$  all  $p$ -power roots of unity where  $p$  is a prime number. We prove that the theory of  $\mathbb{Q}(p^\infty)$  is undecidable.

### 1. INTRODUCTION

Our main result is the undecidability of the field  $\mathbb{Q}(p^\infty)$  in the vocabulary  $L = \{+, \cdot, 0, 1\}$ . In some cases we obtain the undecidability of the field obtained by adjoining to the rationals all  $p$ -power roots of unity for  $p$  in a finite set of prime numbers. This is a small part of the maximal abelian extension of  $\mathbb{Q}$ . The decision problem for this field is open and I believe it was first raised by A. Robinson. To prove the theorem we need some results from logic and number theory explained below. Basically, a result of J. Robinson giving a condition for undecidability of algebraic integer rings, a result of ours on the definability of such rings in algebraic fields and a result of D. Rohrlich about points on elliptic curves in cyclotomic towers.

### 2. PRELIMINARY RESULTS

2.1. Let  $R \subset \tilde{\mathbb{Z}}$  be a ring of algebraic integers. To a formula  $\varphi(x, \vec{y})$  (where  $\vec{y} = (y_1, \dots, y_n)$ ) in the vocabulary  $L$  we can define a family  $\{\varphi(x, \vec{r}) : \vec{r} \in R^n\}$  of subsets of  $R$  where  $\varphi(x, \vec{r}) = \{s \in R : R \models \varphi(s, \vec{r})\}$ . The following result holds:

**2.2. Proposition.** *Let  $R \subset \tilde{\mathbb{Z}}$  be a ring and suppose there is a collection of subsets of  $R$  as above containing finite sets of arbitrarily large size. Then the ring  $R$  is undecidable.*

The proof of the above proposition in the case in which all sets in the family are finite and  $R$  is the ring of integers of a field of algebraic numbers is due to J. Robinson [2], p. 302. It has been noted by W. Henson ([1], p. 199) that the assumption of finiteness of all sets can be dropped and it is easy to see that  $R$  can be taken to be any subring of  $\tilde{\mathbb{Z}}$ .

In [6] we showed that the ring  $\tilde{\mathbb{Z}} \cap \mathbb{Q}(p^\infty)$  is definable with parameters. That is, there exists a formula  $\varphi(x, y_1, \dots, y_m)$  in  $L$  such that for some  $\alpha_1, \dots, \alpha_m \in \mathbb{Q}(p^\infty)$  we have

$$r \in \tilde{\mathbb{Z}} \cap \mathbb{Q}(p^\infty) \iff \mathbb{Q}(p^\infty) \models \varphi(r, \alpha_1, \dots, \alpha_m).$$

---

Received by the editors November 23, 1998 and, in revised form, February 1, 1999.  
1991 *Mathematics Subject Classification.* Primary 03B25, 12L05.

The set of parameters  $\{\alpha_1, \dots, \alpha_m\}$  is troublesome in what follows, so we work with the ring  $R_p$  defined below which is definable in  $L$ :

$r \in R_p$  if and only if  $\forall c_1 \dots c_m \in \mathbb{Q}(p^\infty)$  (if  $\varphi(x, c_1, \dots, c_m)$  is a ring  $\Rightarrow \varphi(r, c_1, \dots, c_m)$ ).

By the above result  $\mathbb{Z} \subset R_p \subset \tilde{\mathbb{Z}} \cap \mathbb{Q}(p^\infty)$ . Hence to establish the undecidability of  $\mathbb{Q}(p^\infty)$  it is enough to show that Proposition 2.2 holds for  $R_p$ . In order to prove this we will use a result of D. Rohrlch ([3], p. 409) stated in 2.3 below.

As was pointed by L. van den Dries, the use of  $R_p$  is not necessary. It turns out that  $\tilde{\mathbb{Z}} \cap \mathbb{Q}(p^\infty)$  is already definable without parameters. The argument is as follows. Let  $\mathbb{Q}(\alpha_1, \dots, \alpha_m) = \mathbb{Q}(\alpha)$  and let  $f$  be the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ . Let  $\alpha_i = g_i(\alpha)$  with  $g_i \in \mathbb{Q}[x]$  and the degree of  $g_i$  less than the degree of  $f$ . In the formula above (defining  $\tilde{\mathbb{Z}} \cap \mathbb{Q}(p^\infty)$ ) replace each occurrence of  $\alpha_i$  by  $g_i(\alpha)$  and add the condition  $f(\alpha) = 0$ . This gives us a new formula  $\phi(x, \alpha)$  which defines in  $\mathbb{Q}(p^\infty)$  the ring  $\tilde{\mathbb{Z}} \cap \mathbb{Q}(p^\infty)$ . Since  $\mathbb{Q}(p^\infty)$  and  $\tilde{\mathbb{Z}} \cap \mathbb{Q}(p^\infty)$  are closed under conjugation one can eliminate the occurrence of  $\alpha$  by quantifying it out.

2.3. Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  with complex multiplication by the ring of integers of an imaginary quadratic field, and let  $P$  be a finite set of primes where  $E$  has good reduction. Let  $L$  be the maximal abelian extension of  $\mathbb{Q}$  unramified outside  $P$  and infinity and let  $E(L)$  be the group of points on  $E$  which are defined over  $L$ . Then  $E(L)$  is finitely generated.

### 3. MAIN RESULTS

3.1. We first consider  $p$  odd. Let  $E$  be the elliptic curve  $y^2 = x^3 + 8x$ . It has discriminant equal to  $-2^{15}$ ,  $j$ -invariant equal to  $(12)^3$  and has complex multiplication by the ring of integers of  $\mathbb{Q}(\sqrt{-1})$ . The point  $P_0 = (1, 3)$  belongs to  $E(\mathbb{Q})$  and has infinite order since  $2P_0 = (\frac{7^2}{6^2}, \frac{113 \cdot 7}{6^3})$ .

We will use  $E$  to define a family of sets in  $\mathbb{Q}(p^\infty)$  as required in Proposition 2.2. First note the following.

Suppose  $(\frac{a}{b}, \frac{c}{d}) \in E(\mathbb{Q})$  with  $a, b, c, d \in \mathbb{Z}$ ,  $(a, b) = (c, d) = 1$ . Then we may assume  $b^3 = d^2$  because from the equation it follows that  $b^3c^2 = d^2(a^3 + 8ab^2)$  and so  $b^3|d^2$  and  $d^2|b^3$ . Hence  $d^2 = \pm b^3$ . We may take  $b > 0$  since if  $b < 0$ , then  $b = -b'$  with  $b' > 0$  and  $\frac{a}{b} = \frac{-a}{b'}$ .

3.2. For the next step, take  $N$  points  $P_i = (\frac{a_i}{b_i}, \frac{c_i}{d_i}) \in E(\mathbb{Q})$   $a_i, b_i, c_i, d_i \in \mathbb{Z}$ ,  $(a_i, b_i) = 1$ . We twist  $E$  to a new curve which has  $N$  integral points. Here we follow the idea involved in exercise 9.3 of Silverman's book [4], p. 272.

Let  $E_{\tilde{b}}$  be the curve  $y^2 = x^3 + 8(b_1 \dots b_N)^2x$ . Then the integral set of points  $P_i = (a_i b_1 \dots b_{i-1} b_{i+1} \dots b_N, c_i d_1 \dots d_{i-1} d_{i+1} \dots d_N)$ , for  $1 \leq i \leq N$  belong to  $E_{\tilde{b}}$  as is easily checked. On the other hand the discriminant of  $E_{\tilde{b}}$  is equal to  $-2^{15}(b_1 \dots b_N)^6$  and the  $j$ -invariant is  $12^3$ . Hence  $E_{\tilde{b}}$  also has complex multiplication by the ring of integers of  $\mathbb{Q}(\sqrt{-1})$ .

3.3. Let  $p$  be an odd prime, and let  $n_p$  be the size of the group  $E(\mathbb{F}_p)$ . Choose  $\ell$  a prime number bigger than  $n_p$ . Then the sequence of points  $P_0, \ell P_0, \ell^2 P_0, \dots$  is infinite and if  $\ell^n P_0 = (\frac{a_n}{b_n}, \frac{c_n}{d_n})$  with  $a_n, b_n, c_n, d_n \in \mathbb{Z}$   $(a_n, b_n) = (c_n, d_n) = 1$  we have:

- a)  $\widetilde{P_0} \neq \widetilde{0}$  (here  $\sim$  is reduction mod  $p$ ),
- b)  $\widetilde{\ell^n P_0} = \ell^n \widetilde{P_0} \neq \widetilde{0}$ .

Part a) is obvious. To see b) note that the order of  $P_0$  in  $E(\mathbb{F}_p)$  is bigger than one and divides  $n_p$ . If  $\ell^n \widetilde{P}_0 = \widetilde{0}$ , then  $n \geq 1$  and  $\text{order}(P_0) | \ell^n$  which is impossible.

Now  $\ell^n \widetilde{P}_0 \neq \widetilde{0}$  implies that  $b_n \not\equiv 0 \pmod p$  and  $d_n \not\equiv 0 \pmod p$ . Otherwise, if  $p$  divides either  $b_n$  or  $d_n$ , then  $3 \text{ord}_p b_n = 2 \text{ord}_p d_n > 0$  and so projectively  $\ell^n P_0 = [\frac{a_n d_n}{b_n}, c_n, d_n]$ . Reducing mod  $p$  we get  $\ell^n \widetilde{P}_0 = [0, 1, 0] = \widetilde{0}$  which is impossible.

We are almost done. Apply 2.3 to the curve  $E_{\bar{b}}$  to conclude that  $E_{\bar{b}}(\mathbb{Q}(p^\infty))$  is finitely generated. Hence all the points are contained in a finite extension  $L_n$  of  $\mathbb{Q}$ . By Siegel's theorem the set of integral points of  $E_{\bar{b}}(L_n)$  is finite and by combining 3.2 and 3.3 we can make this finite set arbitrarily large.

We have therefore established Proposition 2.2 for  $R_p$ . As our definable collection of sets we can use  $\{\exists x(y^2 - x^3 + 8\lambda x = 0) : \lambda \in R_p\}$ .

3.4. Let  $p = 2$ . For this case we use  $E : y^2 + y = x^3 - 38x + 90$ . The discriminant of  $E$  is  $-19^3$  and  $j = -3^3 \cdot 2^{15}$ . The curve has complex multiplication by the ring of integers of  $\mathbb{Q}(\sqrt{-19})$  ([5], p. 483).

The point  $P = (0, 9) \in E(\mathbb{Q})$  and  $2P = (4, -2), 4P = (\frac{28}{9}, \frac{-53}{27})$ .

Hence  $P$  has infinite order. If  $(\frac{a}{b}, \frac{c}{d}) \in E(\mathbb{Q})$  (with  $a, b, c, d \in \mathbb{Z}, (a, b) = (c, d) = 1$ ), then as before we may assume  $d^2 = b^3$ . To get curves from  $E$  which have integral points and satisfy 2.3 as in the odd case we use  $E_{d,b} : y^2 + dy = x^3 - 38b^2x + 90b^3$  with  $d^2 = b^3$ . A calculation shows that the discriminant of  $E_{d,b}$  is  $-19^3 b^6$  and the  $j$  invariant is  $-3^3 \cdot 2^{15}$ . We may now repeat the argument in 3.3.

3.5. As a final remark note the following. Let  $A$  be a finite set of prime numbers and define  $\mathbb{Q}_A$  to be the field obtained by adjoining to  $\mathbb{Q}$  all  $p$ -power roots of unity to  $\mathbb{Q}$  for  $p \in A$ . In [6] we showed that  $\widetilde{\mathbb{Z}} \cap \mathbb{Q}_A$  is definable. So, for certain finite sets  $A$  of prime numbers we obtain the undecidability of  $\mathbb{Q}_A$ . For example, if the set  $A$  consists of odd primes, then we may use the construction in 3.1–3.3. For an arbitrary finite set of primes we only have a partial result. First we need a lemma of D. Rohrllich:

**Lemma.** *Let  $A$  be a finite set of primes. Then there exists an elliptic curve  $E$  over  $\mathbb{Q}$  and a point of infinite order  $Q \in E(\mathbb{Q})$  such that  $E$  has good reduction at every  $p \in A$  and the reduction of  $Q$  modulo  $p$  is nonzero for every  $p \in A$ .*

*Proof.* For each  $p \in A$  choose an elliptic curve  $E_p$  over  $\mathbb{F}_p$  and a nonzero point  $Q \in E_p(\mathbb{F}_p)$ . For  $p \geq 5$  the existence of a nonzero point in  $E_p(\mathbb{F}_p)$  is automatic for any  $E_p$ . For  $p = 2$  or  $3$  we can choose  $E_p$  so that  $E_p(\mathbb{F}_p) \neq \{0\}$ . Since  $A$  can be enlarged without loss of generality, we may assume that there are distinct primes  $r, s, t \in A$  such that  $2Q_r \neq 0, 2Q_s = 0$ , and  $2Q_t = 0$ . Thus  $Q_s$  and  $Q_t$  are points of order 2 but  $Q_r$  has order  $> 2$ . For each  $p \in A$  choose a generalized Weierstrass equation for  $E_p$  over  $\mathbb{F}_p$ , say

$$E_p : y^2 + a_{1,p}xy + a_{3,p}y = x^3 + a_{2,p}x^2 + a_{4,p}x + a_{6,p},$$

and write  $Q_p = (u_p, v_p)$ . By the Chinese Remainder Theorem there are integers  $a_1, a_2, a_3, a_4, a_5, a_6, u, v$  such that  $a_i \equiv a_{i,p}, u \equiv u_p$ , and  $v \equiv v_p$  modulo  $p$  for all  $p \in A$ . Put

$$c = (v^2 + a_1uv + a_3v) - (u^3 + a_2u^2 + a_4u + a_6)$$

and define  $E$  by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + (a_6 + c).$$

Since  $c \equiv 0$  modulo  $p$  for all  $p \in A$  we see that the equation for  $E$  reduces modulo  $p$  to the equation for  $E_p$ . In particular, since  $A$  may be assumed nonempty it follows that  $E$  is an elliptic curve (i.e. the discriminant of the above equation for  $E$  is nonzero because it is nonzero modulo  $p$  for  $p \in A$ ). Also  $E$  has good reduction modulo  $p$  for all  $p \in A$ , and the point  $Q = (u, v) \in E(\mathbb{Q})$  reduces to  $Q_p$  for all  $p \in A$  and in particular reduces to a nonzero point for each  $p \in A$ . We claim that  $Q$  has infinite order. It suffices to show that  $2Q$  has infinite order. Now  $2Q$  is nonzero because it is nonzero modulo  $r$ . But  $2Q$  reduces to zero modulo two distinct primes, namely  $s$  and  $t$ , and therefore, since it is nonzero, it is also not a torsion point (a nonzero torsion point can reduce to zero in at most one characteristic). Therefore  $2Q$  has infinite order.

Next, we repeat the constructions in 3.2 and 3.3 to the curve  $E$  and point  $Q$  of the lemma. Writing  $Q = (\frac{a}{b}, \frac{c}{d})$   $a, b, c, d \in \mathbb{Z}$ ,  $(a, b) = (c, d) = 1$  it follows that  $d^2 = b^3$  and the twist we use is

$$E_{d,b} : y^2 + a_1 \frac{d}{b} xy + a_3 dy = x^3 + a_2 bx^2 + a_4 b^2 x + (a_6 + c)b^3.$$

The discriminant of  $E_{d,b}$  is  $b^6 \Delta_E$  and the  $j$  invariant is equal to that of  $E$ . The argument in 3.3 fails only at the point where we apply Rohrlich's theorem. In general, we cannot expect  $E$  to have complex multiplication. However, as Rohrlich points in his paper ([3], p. 422), if the Taniyama–Weil and the Birch–Swinnerton–Dyer conjectures are true, then his theorem holds for all elliptic curves over  $\mathbb{Q}$ . Hence  $\mathbb{Q}_A$  would be undecidable for all finite sets of prime numbers.

#### REFERENCES

- [1] L. van den Dries, Elimination theory for the ring of algebraic integers, *J. reine angew. Math.* 388 (1988), 189–205. MR **89k**:03038
- [2] J. Robinson, On the decision problem for algebraic rings, *Studies in Mathematical Analysis and Related Topics*, Stanford Univ. Press, Stanford 1962, 297–304. MR **26**:3609
- [3] D.E. Rohrlich, On  $L$ -functions of elliptic curves and cyclotomic towers, *Invent. Math.* 75 (1984), 409–423. MR **86g**:11038b
- [4] J. Silverman, *The arithmetic of Elliptic Curves*, G.T.M. 106, Springer–Verlag, New York 1986. MR **87g**:11070
- [5] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, G.T.M 151, Springer–Verlag, New York 1994. MR **96b**:11074
- [6] C.R. Videla, Definability of the ring of integers in pro- $p$  extensions of numbers fields, submitted (1997).

DEPARTAMENTO DE MATEMÁTICAS, CINVESTAV–IPN, A. POSTAL 14–740, MÉXICO, D.F. 07000, MÉXICO

*E-mail address:* cvidela@math.cinvestav.mx