Undecidability of the Minimal Model of Ruler and Compass Constructions (?)

Michael Beeson

June 5, 2012

The problem

The theory of ruler and compass geometry is mutually interpretable with the theory of Euclidean fields. That theory is undecidable, by Ziegler, since it is a finite extension of field theory. On the other hand, it is a subtheory of the theory of real closed fields, which is decidable by Tarski. We are interested in the minimal model of the theory of Euclidean fields, which we call the Tarski field $\mathbb{T}$. This is the least subfield of the real numbers that is closed under square roots of positive elements. The question at hand is whether the theory of this field is undecidable.

I will present some history and a plan for a proof. It is not claimed that this proof is correct; the point of this presentation is to see if it is correct or can be made correct.

Early history

- Tarski 1951 (but done much earlier) proved the decidability of the theory of real closed fields, and of each specific real closed field.
- J. Robinson 1949 proved the undecidability of $\mathbb{Q}$ (and hence, the undecidability of the theory of fields).
- J. Robinson 1959 proved the undecidability of each specific algebraic number field and its ring of integers.

Robinson's later work

- J. Robinson 1962 proved the undecidability of the ring of totally real algebraic integers, leaving open the ring of all algebraic integers.
- J. Robinson 1965 surveys results obtained by 1965. She mentions (p. 305) as open problems, the field of all totally real algebraic numbers and the Tarski field $\mathbb{T}$. She also mentions (p. 311) the field of rational functions over a finite field (which was later shown undecidable by Rumely).

More history

- Cohen 1969 proved the decidability of the p-adic fields $\mathbb{Q}_p$.
- Ziegler 1982 proved the undecidability of any finitely axiomatizable theory of fields. Note: this is not relevant to the decidability of $\mathbb{T}$.
- Rumely 1980 proved the undecidability of the theory of global fields (a global field is a finite extension either of $\mathbb{Q}$ or of the field of rational functions over a finite field).

Introduction to Robinson 1949

Robinson's 1949 proof used quadratic forms and the Hasse-Minkowski theorem. Like all other undecidability results in field theory or ring theory, it proceeds by constructing a first-order definition of the integers $\mathbb{Z}$. We note that one can use the theorem that every positive integer is the sum of four squares to define the natural numbers $\mathbb{N}$ once $\mathbb{Z}$ is defined, so in general it doesn't matter if we define $\mathbb{Z}$ or $\mathbb{N}$. (In $\mathbb{T}$ it is even easier, we can just say that n is a square.)

Robinson 1949

The positive integers will be defined in $\mathbb{Q}$ by an instance of mathematical induction,

$$\phi(0, a, b) \wedge n > 0 \wedge \forall n(\phi(n, a, b) \rightarrow \phi(n + 1, a, b)) \rightarrow \phi(k, a, b).$$

Note that the formula ϕ contains parameters a and b.

Robinson's instance of induction

$$\phi(n) := \exists w\,(E_{n,a,b}(w) = 0)$$

where w is a list of variables, e.g. $w = (x, y, z)$, and $E_{n,a,b}(w)$ is a polynomial in the indicated variables (including those written as subscripts here) with integer coefficients. In Robinson's proof, w is (x, y, z) and E is taken to be quadratic:

$$E_{n,a,b}(x, y, z) = bz^2 + abn^2 + 2 - x^2 - ay^2.$$

In any generalization to $\mathbb{T}$, E would need to be cubic (or possibly of higher degree, with cyclic Galois group), since quadratic equations are all solvable in $\mathbb{T}$ if they are solvable in the reals.

Sketch of Robinson's 1949 proof

Let $\mathbb{K}$ be a field that we want to prove undecidable, for example $\mathbb{Q}$ or $\mathbb{T}$. To apply Robinson's method, we need to prove that a member k of $\mathbb{K}$ satisfies $\phi(k)$ if and only if k is a positive integer. Every integer k will automatically satisfy $\phi(k)$, since ϕ is an instance of mathematical induction. It is the other direction that is difficult: we must prove that if $\phi(k)$ is satisfied, then k is a positive integer. Since $\phi(k)$ includes $k > 0$, it suffices to prove k is an integer.

The key: Hasse-Minkowski

Robinson shows, using Hasse-Minkowski, that the solvability of $E_{n,a,b}(x) = 0$ depends only on what primes divide the denominator of n. Hence the implication $\phi(n, a, b) \Rightarrow \phi(n + 1, a, b)$ will always hold. We wish to show that if her instance of induction holds, then no prime p can divide the denominator of k. To that end suppose p divides the denominator of k. Then Robinson shows how to select a and b such that $\phi(0, a, b)$ holds and for $k \neq 0$, $E_{k,a,b}(x) = 0$ is solvable if and only if the denominator of k is not divisible by p. (Namely, she takes $b = p$ and a to be an odd prime q such that q is not square mod p.)

Can we generalize Robinson 1949 to $\mathbb{T}$?

Let's consider the following plan: replace $\mathbb{Q}$ by $\mathbb{T}$, and replace quadratic forms by cubic norm forms, so that Hasse principle will still hold. By elementary field theory, cubic equations with coefficients in a subfield $\mathbb{K}$ of $\mathbb{T}$ of finite degree over $\mathbb{Q}$ are solvable in $\mathbb{T}$ if and only if they are solvable in $\mathbb{K}$, so the number theory of solvability of cubic equations in $\mathbb{T}$ reduces to the number theory of their solvability in such fields $\mathbb{K}$. To get $\phi(n, a, b) \Rightarrow \phi(n + 1, a, b)$ we only need the Hasse principle (which works for cubic norm forms!)

Can we generalize Robinson 1949 to $\mathbb{T}$?

So, the main task would be to show that cubic norm forms enable us to construct a polynomial $E_{k,a,b}(x)$ such that, for each rational k and prime p dividing k, there exists a and b such that $E_{0,a,b}(x) = 0$ is solvable and for $k \neq 0$, $E_{k,a,b}(x) = 0$ is solvable if and only if p does not divide the denominator of k. Following Robinson's lead, we could try to take $b = p$ and show that for each p, there is a prime q such that $E_{n,q,p}(x) = 0$ is solvable if and only if p does not divide the denominator of n.

Robinson 1949 and norm forms

Consider Robinson's equation $E_{n,a,b}$ given above. Note that $x^2 + ay^2$ is the norm form of the quadratic field $\mathbb{Q}(\sqrt{-a})$. The equation can thus be written as

$$bN(z + n\sqrt{-a}) = N(x - y\sqrt{-a}).$$

The norm form from $\mathbb{K}(a^{1/3})$ to $\mathbb{K}$ is given explicitly by

$$f(a, x, y, z) = x^3 + ay^3 + a^2z^3 - 3axyz.$$

By analogy to Robinson 1949, we could consider the equation

$$bf(a, u, v, n) = f(a, x, y, z).$$

Whether this can be made to work I do not know.

Robinson 1959

Lemma (Robinson's finiteness lemma)

Let $\mathbb{K}$ be an algebraic number field, of degree d over $\mathbb{Q}$, and let f be a nonzero element of $\mathbb{K}$. Then there are only finitely many algebraic integers a of $\mathbb{K}$ such that f is divisible by $a + j$ for all $j = 1, 2, \ldots, d$.

The proof is only one paragraph long and doesn't use any difficult number theory, but nevertheless the lemma is crucial. The importance of the lemma is that it can be used to define $\mathbb{N}$, either within the ring of integers of $\mathbb{K}$, or within $\mathbb{K}$ if $\mathcal{O}$ can be defined.

Defining $\mathbb{N}$ from $\mathcal{O}$, Robinson 1959

Define

$$\tau(a, f, g, h) \leftrightarrow f \neq 0 \wedge a + 1 | f \wedge \ldots \wedge a + d | f \wedge 1 + ag | f.$$

Then

$$n \in \mathbb{N} \leftrightarrow \exists f, g, h \left\{ \tau(0, f, g, h) \wedge \right.$$
$$\left. \forall a [\tau(a, f, g, h) \Rightarrow a = n \vee \tau(a + 1, f, g, h)] \right\}.$$

Now the right-to-left implication follows from the lemma, since the right side will require $\tau(j, f, g, h)$ for $j = 0, 1, 2, \ldots$, and if n is not an integer, there is nothing to stop this list, and the lemma will be violated.

$$\tau(a,f,g,h) \leftrightarrow f \neq 0 \wedge a+1|f \wedge \ldots \wedge a+d|f \wedge 1+ag|f.$$

$$n \in \mathbb{N} \leftrightarrow \exists f,g,h \left\{\tau(0,f,g,h) \wedge \forall a[\tau(a,f,g,h) \Rightarrow a = n \vee \tau(a+1,f,g,h)]\right\}.$$

For the left-to-right implication, we choose $f = (n+1)!$, and define S by

$$a \in S \leftrightarrow a+1|f \wedge \ldots \wedge a+d|f.$$

By the lemma, S is finite. Let g be a positive integer divisible by all the differences $a-b$ for a and b distinct elements of S, and also such that for a a nonzero member of S, $1+ag$ does not divide 1. The latter is possible if g is so large that all the conjugates of $1+ag$ lie outside the unit circle (Since $N(1+ag) > 1$, then $1+ag$ is not a unit.) Then put

$$h = (1+g)(1+2g)\ldots(1+ng).$$

The verification of the right-hand side is then straightforward. Note that f, g, and h are rational integers, so they are certainly integers of $\mathbb{K}$.

Importance of Robinson 1959

In this way, Robinson reduced the problem of proving the undecidability of $\mathbb{K}$ to showing how to define the ring of integers $\mathcal{O}$ of $\mathbb{K}$. Breaking the problem into two steps this way is an important reduction.

Robinson went on to show that $\mathcal{O}$ is definable in any algebraic number field $\mathbb{K}$, and hence $\mathbb{N}$ is too. She used some non-trivial number theory about the Hilbert symbol and the existence of infinitely many prime ideals in ideal classes.

Robinson 1959 uses only *quadratic* forms

This is possible because in any fixed $\mathbb{K}$ of finite degree over $\mathbb{Q}$, there will be plenty of quadratic extensions of $\mathbb{K}$. But in the Tarski field $\mathbb{T}$, this is not the case, so we can't use the construction of Robinson 1965 directly. Even her first lemma does not help us, since the formula in the lemma depends on the degree of $\mathbb{K}$ over $\mathbb{Q}$. Conclusion: even though Robinson's 1959 proof is substantially different from her 1949 proof, and works for algebraic number fields (which the 1949 proof did not), it still won't help us with $\mathbb{T}$. But the idea of first defining $\mathcal{O}$ and then $\mathbb{N}$ will.

The Hasse Norm Principle

The Hasse Norm Principle says that norm forms satisfy the local-global principle, provide the norm is of a cyclic field extension. Since quadratic fields of course are cyclic, that "explains" the Hasse-Minkowski theorem; and since every three-element group is cyclic, it also implies that cubic norm forms satisfy the local-global principle.

Theorem (Hasse Norm Principle)

Let $\mathbb{K}$ be a cubic extension of $\mathbb{Q}$. Then the rational number α is a norm of some element of $\mathbb{K}$ if and only if α, considered as an element of $\mathbb{Q}_p$, is a norm of an element of $K_{\mathfrak{P}}$, for every place $\mathfrak{P}$ of $\mathbb{K}$ above p.

Proof. See Cohen, *Number Theory, vol I*, Theorem 5.5.1, p. 318.

Cubic norm forms, continued

There is also a sufficient condition for α to be the norm $\mathcal{N}(\beta)$ of some element β of $\mathbb{K}$:

Theorem

Let $\mathbb{K}$ be a cubic extension of $\mathbb{Q}$. Then the rational number α is a norm of some element of $\mathbb{K}$ if for some ideal I of $\mathbb{K}$ we have $\alpha\mathbb{Z}_k = \mathcal{N}(I)$.

Proof. See Cohen vol. I, Theorem 5.5.1, p. 318.

Remark. There is therefore some hope of using cubic norm forms to prove the undecidability of $\mathbb{T}$.

Rumely 1980

Cubic norm forms can be explicitly computed: The norm of $x + yb^{1/3} + zb^{2/3}$ in $\mathbb{Q}(b^{1/3})$ is given by

$$N(b, x, y, z) = x^3 + by^3 + b^2z^3 - 3bxyz.$$

Following Rumely we let $\alpha = (\alpha_0, \alpha_1, \alpha_2)$ etc., and

$$R(t; c, d) \leftrightarrow \exists \alpha\beta\gamma w\, (w = N(d, \alpha) \wedge cw = N(cd, \beta) \wedge t = N(w, \gamma))$$

Rumely thinks that we can't use just one cubic norm, but we need to use two nested norms in this fashion. I did not understand why.

Defining the elements with order divisible by 3

Lemma (Rumely)

Let ℓ be a positive integer and p a prime number. Let $\mathbb{K}$ be an algebraic number field (for our purposes, $\mathbb{K}$ has the form $\mathbb{F}(e^{i\pi/3})$ where $\mathbb{F}$ is a subfield of $\mathbb{T}$). Let $\mathbb{L} = \mathbb{K}(b^{1/3})$ and let N be the norm from $\mathbb{L}$ to $\mathbb{K}$. Let p be a prime of $\mathbb{K}$ and let $\mathfrak{P}$ be a prime of $\mathbb{L}$ above p. If d is a unit of $\mathbb{K}$ that is not a cube, and the order of c at $\mathfrak{P}$ is 1 then

(i) for some c, d, $R(t; c, d)$ is satisfied in $\mathbb{K}$ only by t in $\mathbb{K}$ whose order at $\mathfrak{P}$ is congruent to 0 mod 3, and

(ii) If t has order at $\mathfrak{P}$ congruent to 0 mod 3, and in addition has order zero at $\mathfrak{Q}$ for a certain prime $\mathfrak{Q}$ depending on $\mathfrak{P}$, then $R(t; c, d)$ is satisfied in $\mathbb{K}$.

Proof. See Rumely, p. 199–202 (specializing to $\ell = 3$).

Defining $\mathcal{O}_p$

Using R it is easy to define the valuation ring $\mathcal{O}_p$ (a subset of $\mathbb{K}$); (see p. 198 of Rumely) by a first-order formula over $\mathbb{K}$, with variable p and independent of $\mathbb{K}$:

$$\mathcal{O}_p(x) \leftrightarrow \exists t(1 + gx^2 = t \wedge R(t, c, d)$$

where (c, d) are as in (i) above. Here we only have the quadratic $1 + gx^2$ on the right. But, on p. 203, Rumely defines

$$S_3(x; c_1, d_1, c_2, d_2) \leftrightarrow \exists t_1, t_2 \, (1 + c_1 x^3 = t_1 t_2$$
$$\wedge R(t_1; c_1, d_1) \wedge R(t_2; c_2, d_2)$$

and shows that for some (c_1, d_1, c_2, d_2), we have

$$\mathcal{O}_p(x) \leftrightarrow S_3(x; c_1, d_1, c_2, d_2).$$

Defining $\mathcal{O}$

Rumely then constructs a formula $Val_3(x; c, d)$ such that for any choice of parameters (c, d), either $Val_3(x; c, d)$ defines a valuation ring (in x) or it defines the whole of $\mathbb{K}$.
Namely,

$$Val_3(x; c) \quad \leftrightarrow \quad [\forall y, z((S(y) \wedge S(z)) \rightarrow (S(-y) \wedge S(y+z) \wedge S(yz))) \\ \forall y(y \neq 0 \rightarrow (S(y) \vee S(1/y)))] \rightarrow S(x).$$

Finally Rumely arrives (p. 205) at this: The ring of integers $\mathcal{O}_{\mathbb{K}}$ is arithmetically definable by a predicate independent of $\mathbb{K}$. Namely,

$$Int(t) \leftrightarrow \forall c Val_2(t; c) \wedge \forall c Val_3(t; c) \wedge \forall c Val_3(t; c).$$

(The second Val_3 has vector arguments, it is not a typo but we haven't use a different typeface for vectors here.)

Rumely defines $\mathbb{N}$ from $\mathcal{O}$

Given a definition Int of the integers of $\mathbb{K}$, Rumely (following Robinson 1962) defines

$$\begin{aligned} Set_N(t;g) \quad \leftrightarrow \quad & g_2 \neq 0 \wedge Int((t-g_1)g_2) \wedge \\ & g_3 \neq 0 \wedge (t-g_1)g_2((t-g_1)g_2+1)|_N g_3] \\ & (1+(t-g_1)g_2g_4)|_N g_5 \end{aligned}$$

$$n \in \mathbb{N} \leftrightarrow \exists g \{ Set_N(0,g) \wedge \forall t [Set_N(t,g) \Rightarrow (t = n \vee Set_N(t+1,g))] \}.$$

The crucial property of $Set_N(t;g)$ is that for a given choice of g only finitely many t can satisfy $Set_N(t,g)$ in a fixed algebraic number field. The number of t that can satisfy it increases with degree of the field, but the formula itself is fixed–it does not depend on the field.

Siegel 1921

The crucial property of $Set_N(t;g)$ relies on a theorem of Siegel, that for a given polynomial f, there are only a finite number of values of the norm of $f(x)$ in a given sphere. Robinson used this result both in her 1959 and her 1962 papers.

Working with $\mathbb{T}$ and $\mathbb{T}(e^{i\pi/3})$

Fix a subfield $\mathbb{F}$ of $\mathbb{T}$, such that $\mathbb{F}$ has finite degree over $\mathbb{Q}$. Let $\mathbb{K} = \mathbb{F}(e^{i\pi/3})$. Then $\mathbb{K}$ has degree 3 over $\mathbb{F}$, and $\mathbb{K}$ is a subfield of $\mathbb{T}(e^{i\pi/3}$. There is a formula that defines the algebraic integers of $\mathbb{K}$ over $\mathbb{K}$, independently of the fields $\mathbb{F}$ and $\mathbb{K}$, i.e. the same formula works for all of them. We claim that the same formula also defines the algebraic integers of $\mathbb{T}(e^{i\pi/3})$ over $\mathbb{T}$.

R is absolute for degree-power-of-2 extensions

To say that a predicate is *absolute upwards* means that if it's true in $\mathbb{K}$ (with parameters in $\mathbb{K}$) then it's true in extensions of $\mathbb{K}$. Vice-versa is *absolute downwards*.

R just says that certain cubic polynomial equations are solvable; the point is that no more cubic polynomial equations are solvable in $\mathbb{T}$ than in any of its finite-degree subfields that contain $\mathbb{Q}(e^{i\pi/3})$, all of which have degree a power of 2 over $\mathbb{Q}(e^{i\pi/3})$. Hence R is absolute with respect to extensions of power-of-2 degree.

Absoluteness of S_3

Now consider the formula

$$S_3(x; c_1, d_1, c_2, d_2) \quad \leftrightarrow \quad \exists t_1, t_2\, (1 + c_1 x^3 = t_1 t_2 \\ \wedge R(t_1; c_1, d_1) \wedge R(t_2; c_2, d_2)$$

We want to show this holds in $\mathbb{T}$ if and only if it holds in a finite-degree subfield K. Since R is absolute with respect to extensions of degree a power of 2, what we must show is that if t_1 and t_2 exist in $\mathbb{T}$, then they exist in any finite-degree subfield $\mathbb{K}$ of $\mathbb{T}$ that contains c_1, c_2, d_1, and d_2. Suppose that t_1 and t_2 exist in $\mathbb{T}$. Looking at the definition of R, we see that the issue is to prove that if $N(d, \alpha)$ is in $\mathbb{K}$ for some $\alpha = (a_0, a_1, a_2)$ in $\mathbb{T}^3$ then α is already in $\mathbb{K}^3$. But that is so, since the equation $\beta = N(\alpha)$ is cubic, so it is either solvable already in $\mathbb{K}$, or not solvable in $\mathbb{T}$. Hence S is also absolute with respect to power-of-2-degree extensions.

Int is absolute downwards

Int is defined (p. 205 Rumely) by

$$Int(t) \Leftrightarrow \forall c Val_2(t;c) \wedge \forall c Val_3(t,c) \wedge \forall c Val_3(t,c)$$

(The second Val_3 has vector arguments.)
Suppose $Int(t)$ holds in $\mathbb{T}(e^{i\pi/3})$. Let $\mathbb{K}$ be an algebraic number field contained in $\mathbb{T}(e^{i\pi/3})$ with t in $\mathbb{K}$. We need to check that the right side holds in $\mathbb{K}$. For that we need Val_3 and Val_2 to be absolute downwards. These predicates say that x belongs to S_2 (or S_3) if S_2 is a valuation ring or is everything, and as c varies, $S_2(x,c)$ varies over all valuation rings. So the only essential use of the $\forall c$ quantifiers in Int is to ensure that the particular choices of c needed to pick out $\mathcal{O}_p$ are included; Those choices are c_1, c_2, c_3, c_4 where these c's are constructed (Rumely p. 200) from Artin's Reciprocity Law. So they do lie in $\mathbb{K}$, since $\mathbb{K}$ satisfies Artin's reciprocity law. Therefore the right side holds in $\mathbb{K}$ as claimed.

Int defines the algebraic integers of $\mathbb{T}(e^{i\pi/3})$

Proof. Suppose $Int(t)$ holds in $\mathbb{T}(e^{i\pi/3})$. The crucial point is that Int is absolute downwards. Therefore, t is an algebraic integer of $\mathbb{K}$. Therefore it's an algebraic integer of $\mathbb{T}(e^{i\pi/3})$.
Conversely, suppose t is an algebraic integer of $\mathbb{T}(e^{i\pi/3})$. Then it is an algebraic integer of some $\mathbb{K}$, so the formula on the right holds over $\mathbb{K}$. Given c in $\mathbb{T}(e^{i\pi/3})$, either $Val_3(t;c)$ defines a valuation ring, or is satisfied by every x in every $\mathbb{K}$ containing c; since Val_3 is absolute for power-of-2-degree extensions, the right side holds in $\mathbb{T}(e^{i\pi/3})$. Conversely, if the right side holds over $\mathbb{T}(e^{i\pi/3})$ for some t, then it holds over any $\mathbb{K}$ containing t, so t is an algebraic integer of that $\mathbb{K}$, so t is an algebraic integer of $\mathbb{T}(e^{i\pi/3})$. That completes the proof of the lemma.

Int is absolute

Lemma

Int is absolute for degree-power-of-2 extensions.

Proof. We already proved that it is absolute downwards, using the fact that $\mathbb{K}$ satisfies Artin's Reciprocity Law. Now we prove it is absolute upwards. Recall the definition:

$$Int(t) \Leftrightarrow \forall c Val_2(t;c) \wedge \forall c Val_3(t,c) \wedge \forall c Val_3(t,c)$$

Suppose $Int(t)$ holds in K_1 and K_2 has degree a power of 2 over K_1. Let c be in $\mathbb{K}_2$. Then either $Val_3(x,c)$ holds for all x (in which case it holds for $x = t$), or the set of x in K_2 for which it holds is a valuation ring. But over any field, including $\mathbb{K}_2$, there are "good" values of c that define any given valuation ring. Hence t belongs to all valuation rings of K_2. Hence $Int(t)$ holds in $\mathbb{K}_2$. That completes the proof of the lemma.

$\mathbb{N}$ is definable in $\mathbb{T}(e^{i\pi/3})$ from $\mathcal{O}$, the integers of $\mathbb{T}(e^{i\pi/3})$

Proof. The definition of Set_N involves the formula $Int(x)$ that has been constructed above to define the algebraic integers in a fixed algebraic number field. Now we claim that this definition works in $\mathbb{T}$ too.
Recall the definition:

$$\begin{aligned} Set_N(t;g) \quad \leftrightarrow \quad & g_2 \neq 0 \wedge Int((t-g_1)g_2) \wedge \\ & g_3 \neq 0 \wedge (t-g_1)g_2((t-g_1)g_2+1)|_N g_3] \\ & (1+(t-g_1)g_2g_4)|_N g_5 \end{aligned}$$

Left to right: suppose n is a natural number. Let g be chosen so that exactly $\{1,\ldots,n\}$ satisfies $Set_N(t,g)$ over some finite-degree $\mathbb{K}$. Then the right-hand side is satisfied in $\mathbb{T}(e^{i\pi/3})$, since Int is absolute upwards for power-of-2-degree extensions.

$$\begin{aligned} Set_N(t;g) \quad &\leftrightarrow \quad g_2 \neq 0 \wedge Int((t-g_1)g_2) \wedge \\ & \qquad g_3 \neq 0 \wedge (t-g_1)g_2((t-g_1)g_2+1)|_N g_3] \\ & \qquad (1+(t-g_1)g_2g_4)|_N g_5 \end{aligned}$$

Right to left: Suppose n is not a natural number and the right side holds in $\mathbb{T}(e^{i\pi/3})$. Then let g be given by the right hand side. Then for every natural number k (regarded as a member of $\mathbb{T}(e^{i\pi/3})$) $\mathbb{T}$ satisfies $Set_N(k,g)$, since $k=n$ never holds. But the natural numbers all belong to $\mathbb{Q}(n)$, so there does come a natural number k such that $Set_N(k,g)$ fails in $\mathbb{Q}(n)$. But Set_N is absolute downwards, since Int is absolute downwards, so if it holds in $\mathbb{T}(e^{i\pi/3})$, then it holds in $\mathbb{Q}(n)$. Contradiction.

Theorem: $\mathbb{N}$ is definable in $\mathbb{T}$

Proof. $\mathbb{T}(e^{i\pi/3})$ is faithfully interpretable in $\mathbb{T}$ as triples of elements of $\mathbb{T}$; that is, there are formulas with three variables defining addition and multiplication of triples (a, b, c), reflecting the arithmetic on $a + b\zeta + c\zeta^2$, where $\zeta = e^{i\pi/3}$.