Complex roots of unity on the real plane

B.Zilber

April-July, 2003 *

We consider the theory of the structure

\[ \mathbb{C}_{\mathbb{R}, \text{roots}} = (\mathbb{C}, +, \cdot, R, U) \]

where \( R \) is a unary predicate for the real axis of the complex plane \( \mathbb{C} \) and \( U \) the unary predicate for the complex roots of unity.

A weaker structure \( (\mathbb{C}, +, \cdot, U) \) is known to be \( \omega \)-stable (see [Z]). Anand Pillay asked if \( \mathbb{C}_{\mathbb{R}, \text{roots}} \) is well behaving in the context of real model theory, and this has been further discussed in [Mi].

We give here a complete axiomatisation of the theory of \( \mathbb{C}_{\mathbb{R}, \text{roots}} \) and prove that the theory allows elimination of quantifiers in a reasonable language. The elimination of quantifiers in fact shows that definable sets in the standard model are finite boolean combinations of some countable unions of semi-algebraic cells.

Let \( U_0 = U(\mathbb{C}) \), the complex roots of unity. We use the following Lang property of \( U_0 \) (see [L], Ch.I, s.6 for details):

For every polynomial \( p(x_1, \ldots, x_n) \) over \( \mathbb{Q}(U_0) \) (the extension of \( \mathbb{Q} \) by the roots of unity) there is a finite collection of cosets \( S_1, \ldots, S_k \) of algebraic subgroups of \( (\mathbb{C}^*)^n \) given by a finite system of equations of the form

\[ x^m = \gamma_m \]

for non-trivial monomials \( x^m \) and elements \( \gamma_m \in U_0 \) such that

* with corrections suggested by O. Belegradek in January 2005
\{a \in U^n_0 : p(a) = 0\} = \bigcup_i S_i \cap U^n_0.

Let \(T_{\mathbb{R},\text{roots}}\) be the theory of \(\mathbb{C}_{\mathbb{R},\text{roots}}\) and \((F, +, \times, R, U)\) a model of the theory. Since \(F = R + iR\), and \(R = R(F)\) is a definable (formal real) subfield, a subset \(S \subseteq F^n\) can be also viewed as a subset of \(R^{2n}\). Call \(S \subseteq F^n\) semi-algebraic if \(S\) is definable in the field structure \((R, +, \times)\).

**Theorem 1** The complete theory \(T_{\mathbb{R},\text{roots}}\) of \(\mathbb{C}_{\mathbb{R},\text{roots}}\) is given by the following axioms:

1. The universe \(F\) has a field structure, \(F = R + iR\) with \(i^2 = -1\) and \(R\) a real closed field;

2. \(U\) is a multiplicative divisible subgroup of \(F\) with \(n\)-torsion isomorphic to the cyclic group of order \(n\);

3. for any \(a \in U\) the unique representation
   \[ a = s + it, \quad s, t \in R \]
   yields \(s^2 + t^2 = 1\);

4. the projection \(\text{pr} U\) of \(U\) on the ’real’ axis \(R\) is dense in \([-1, 1]\), that is, for any \(-1 \leq a < b \leq 1\) we have \((a, b) \cap \text{pr} U \neq \emptyset\);

5. Lang’s property holds for \(U\), that is
   for every polynomial \(p(x_1, \ldots, x_n)\) over \(\mathbb{Q}(U_0)\) there is a finite collection of cosets \(S_1, \ldots, S_k\) of algebraic subgroups of \((F^*)^n\) given by finite system of equations of the form
   \[ x^m = \gamma_m \]
   for non-trivial monomials \(x^m\) and elements \(\gamma_m \in U_0\) such that
   \[ \{a \in U^n : p(a) = 0\} = \bigcup_i S_i \cap U^n; \]
6. $R \setminus acl(U)$ is dense in $R$, that is for any $a < b$ in $R$ and any semi-algebraic function $f : (0,1)^n \to R$ (with parameters)

$$(a,b) \setminus f((pr U)^n) \neq \emptyset.$$ 

The proof of the theorem follows from the lemmas below.

We write $T$ for $T_{R,\text{roots}}$.

**Lemma 0.1** Let $F$ be a model of $T$ and $A$ a multiplicatively independent over $U_0$ subset of $U(F)$.

Then $A$ is algebraically independent over $U_0$ in the field theoretic sense.

**Proof** Immediate from Lang’s property. □

Now let $F$ and $E$ be models of $T$. By Jonsson’s theory there are saturated models $F' \succ F$ and $E' \succ E$ of some cardinality $\kappa$ (with $2^\mu < \kappa$ for any $\mu < \kappa$) we may assume that $F' = F$ and $E' = E$ and want to prove that $F \cong E$.

**Lemma 0.2** Let $\mu$ be an ordinal less than $\kappa$, $A_\mu \cup A^*_\mu$ be a subset of $R(F)$.

$A^*_\mu \subseteq pr \, U(F)$, $A_\mu \subseteq R(F)$, card $A_\mu \leq |\mu|$, card $A^*_\mu \leq |\mu|$, such that

(i) $A^*_\mu \subseteq pr \, U(F)$ is algebraically independent;

(ii) $A_\mu$ is algebraically independent over $U(F)$.

Then

(a) $pr \, U(F) \setminus aclA^*_\mu \neq \emptyset$

(b) $R(F) \setminus acl(U(F) \cup A_\mu) \neq \emptyset$

and

(c) for any $a^*_\mu \in pr \, U(F) \setminus aclA^*_\mu$ and $a_\mu \in R(F) \setminus acl(U(F) \cup A_\mu)$ the new sets $A^*_{\mu+1} = A^*_\mu \cup \{a^*_\mu\}$ and $A_{\mu+1} = A_\mu \cup \{a_\mu\}$ satisfy properties (i) and (ii).

**Proof** (a) follows by saturatedness from the fact that $pr \, U(F)$ is infinite.

(b) follows by saturatedness from axiom 6.

(c) is obvious from assumptions. □
Corollary 1 There exists a transcendence basis of $F$ of the form $A \cup A^*$ with $A^* \subseteq \text{pr} U(F)$, $A \subseteq R(F)$, $\text{pr} U(F) \subseteq \text{acl} A^*$, $\text{card } A = \text{card } A^* = \kappa$.

For $X \subseteq R$ we denote $\text{dcl} X$ the definable closure of $X$ in the $(R, +, \times)$. We notice that $\text{dcl}$ is just the closure under all semi-algebraic functions, that is the functions 0-definable in the formal reals.

We say that a bijection $\phi$ between subsets $A$ and $B$ of $R$ is a semi-algebraic isomorphism if there is an extension of $\phi$ to a bijection $\phi : \text{dcl} A \rightarrow \text{dcl} B$ preserving semi-algebraic functions and $\prec$.

Lemma 0.3 There exist transcendence bases $\tilde{A} \cup \tilde{A}^* \subseteq R(F)$ and $\tilde{B} \cup \tilde{B}^* \subseteq R(E)$ of $F$ and $E$ correspondingly with $\tilde{A}^* \subseteq \text{pr} U(F)$, $\tilde{B}^* \subseteq \text{pr} U(E)$, transcendence bases of $\text{pr} U$ and a semi-algebraic isomorphism $\phi : \tilde{A} \cup \tilde{A}^* \rightarrow \tilde{B} \cup \tilde{B}^*$ such that $\phi(\tilde{A}) = \tilde{B}$.

Proof Let

$$A \cup A^* = \{a_i : i < \kappa\} \cup \{a_i^* : i < \kappa\}$$

and

$$B \cup B^* = \{b_i : i < \kappa\} \cup \{b_i^* : i < \kappa\}$$

be transcendence bases of $F$ and $E$ correspondingly constructed by Corollary 1.

We construct $\tilde{A} \cup \tilde{A}^*$, $\tilde{B} \cup \tilde{B}^*$ and $\phi$ by transfinite induction.

Suppose that for $\mu < \kappa$

$$\tilde{A}_\mu \cup \tilde{A}_\mu^* = \{\tilde{a}_i : i < \mu\} \cup \{\tilde{a}_i^* : i < \mu\}$$

and

$$\tilde{B}_\mu \cup \tilde{B}_\mu^* = \{\tilde{b}_i : i < \mu\} \cup \{\tilde{b}_i^* : i < \mu\}$$

have been constructed with $\phi_\mu$ given by the enumeration and

$$\text{acl}(\tilde{A}_\mu \cup \tilde{A}_\mu^*) \supseteq \{a_i : i < \mu\} \cup \{a_i^* : i < \mu\}$$

and

$$\text{acl}(\tilde{B}_\mu \cup \tilde{B}_\mu^*) \supseteq \{b_i : i < \mu\} \cup \{b_i^* : i < \mu\}.$$
By back-and-forth method it is enough to show that by letting $\tilde{a}_\mu^*$ equal to the first element of $A^* \setminus \text{acl} \tilde{A}_\mu^*$ and $\tilde{a}_\mu$ equal to the first element of $A \setminus \text{acl}(\text{pr}(U(F) \cup \tilde{A}_\mu))$ we can extend the isomorphism $\phi$ to $\tilde{A}_{\mu+1} \cup \tilde{A}_{\mu+1}^*$. Denote $p_{\mu,A}^*$ the semi-algebraic type of $\tilde{a}_\mu^*$ over $\tilde{A}_\mu^* \cup \tilde{A}_\mu$ and $p_{\mu,B}^*$ the corresponding type over $\tilde{B}_\mu^* \cup \tilde{B}_\mu$. Notice that the types are given by collections of formulas of the form $f_1 < x < f_2$ for $f_1, f_2$ semi-algebraic terms over the parameters. Since the parameters of the two types are semi-algebraically conjugated, by elimination of quantifiers in real closed fields, $p_{\mu,B}^*$ is consistent. Also the type contains the condition $-1 < x < 1$ for its variable $x$. Since the projection $\text{pr}(U)$ of $U$ on $R$ is dense in $[-1, 1]$ and $p_{\mu,B}^*(R)$ is an intersection of intervals, the type is consistent with $x \in \text{pr}(U)$. By saturatedness we find $\tilde{b}_\mu^* \in U(E)$ realizing $p_{\mu,B}^*$.

Now let $p_{\mu,A}$ be the semi-algebraic type of $\tilde{a}_\mu$ over $\tilde{A}_{\mu+1} \cup \tilde{A}_\mu$ and $p_{\mu,B}$ the correspondent type in $E$. Again, $p_{\mu,B}(R)$ is a given as an intersection of intervals. By axiom 6 this is finitely consistent with the collection of formulas saying that $x \notin \text{acl}(U \cup \tilde{A}_{\mu+1} \cup \tilde{A}_\mu)$. Hence by saturatedness there exists $\tilde{b}_\mu \in R(F) \cap p_{\mu,B}(F) \setminus \text{acl}(U(F) \cup \tilde{A}_{\mu+1} \cup \tilde{A}_\mu)$.  

\[\tilde{b}_\mu \in R(F) \cap p_{\mu,B}(F) \setminus \text{acl}(U(F) \cup \tilde{A}_{\mu+1} \cup \tilde{A}_\mu)\]

\[\tilde{b}_\mu \in R(F) \cap p_{\mu,B}(F) \setminus \text{acl}(U(F) \cup \tilde{A}_{\mu+1} \cup \tilde{A}_\mu)\]

\[\tilde{b}_\mu \in R(F) \cap p_{\mu,B}(F) \setminus \text{acl}(U(F) \cup \tilde{A}_{\mu+1} \cup \tilde{A}_\mu)\]

\[\tilde{b}_\mu \in R(F) \cap p_{\mu,B}(F) \setminus \text{acl}(U(F) \cup \tilde{A}_{\mu+1} \cup \tilde{A}_\mu)\]

\[\tilde{b}_\mu \in R(F) \cap p_{\mu,B}(F) \setminus \text{acl}(U(F) \cup \tilde{A}_{\mu+1} \cup \tilde{A}_\mu)\]

\[\tilde{b}_\mu \in R(F) \cap p_{\mu,B}(F) \setminus \text{acl}(U(F) \cup \tilde{A}_{\mu+1} \cup \tilde{A}_\mu)\]

[Proof of the Theorem. We extend the isomorphism $\phi$ of the bases of $F$ and $E$ of Lemma 0.3 can be extended to a semi-algebraic isomorphism $\tilde{\phi} : F \to E$. Now let $A^U = \{a + i\sqrt{1 - a^2} : a \in \tilde{A}^*\}$. Obviously $A^U \subseteq U(F)$ and is a maximal algebraically independent subset of $U(F)$. By Lemma 0.1 $A^U$ is a maximal multiplicatively independent subset of $U(F)$.

Denote $G(A)$ the group generated by $A^U$ and all the roots of any power of elements of $A^U$ (the divisible hull of $A^U$). By definitions $G(A) = U(F)$. Define $B^U$ and $G(B)$ similarly. $\phi$ extends uniquely to a semi-algebraic isomorphism $A^U \to B^U$ and hence to $U(F) \to U(E)$. Further on we have a unique extension to a semi-algebraic isomorphism $\tilde{\phi} : F \to E$. Since $\tilde{\phi}$ preserves $U$, $R$ and the field structure, we have the required isomorphism between the two models of $T$. $\square$]
We now want to see $\mathbb{C}_{R,\text{roots}}$ as a structure definable naturally in the reals. Let $L^U$ be the definable extension of the language of the field of reals (including $<$) which contains a name $P_{\varphi,k}(x_1, \ldots, x_m, y)$ for each definable predicate on $R$ of the form

$$\exists v_1, \ldots, v_k \bigwedge_{i \leq k} v_i \in \text{pr } U & \varphi(x_1, \ldots, x_m, v_1, \ldots, v_k)$$

where $\varphi$ is quantifier-free formula in the language of $(R, +, \cdot, <)$.

One can see that the predicate $U \subseteq R^2$ is definable in $L^U$, so $R$ in the language $L^U$ is definable equivalent to the structure $\mathbb{C}_{R,\text{roots}}$.

**Theorem 2** $T_{\mathbb{R},\text{roots}}$ has elimination of quantifiers in the language $L^U$.

**Proof**

Claim. For any $\bar{a}$, a tuple in a model $F$ of $T$, the $L^U$-quantifier-free type $q = q_{\text{ftp}}(\bar{a})$ of the tuple is a complete type.

The theorem follows by compactness from the claim.

To prove the claim we assume that $F$ is saturated and show that if $\bar{b}$ is a tuple satisfying $q$ in any other saturated model $E$ of the same cardinality, then there is an isomorphism $F \to E$ sending $\bar{a}$ to $\bar{b}$.

Up to enumeration we can assume that $\bar{a} = (a_1, \ldots, a_n)$ with $\{a_1, \ldots, a_l\}$ algebraically independent over $\text{pr } U(F)$ and for each $i \in \{l + 1, \ldots, n\}$, $P_{f_i,k}(a_1, \ldots, a_l, a_i)$ holds for some semi-algebraic $f_i$ and some $k > 0$. This effectively means that for some $a_1^*, \ldots, a_k^* \in \text{pr } U(F)$ we have $a_i = f_i(a_1^*, \ldots, a_k^*, a_1, \ldots, a_l)$. By choosing $k$ minimal possible we get $a_1^*, \ldots, a_k^*$ algebraically independent. Since $l$, the minimal $k$ and corresponding $f_i$ are all invariants of type $q$ we have similar $\{b_1, \ldots, b_l, b_1^*, \ldots, b_k^*\}$ for $\bar{b}$.

Thus we can start the construction of bases by Lemma 0.2 by letting $A_l = \{a_1, \ldots, a_l\}$, $A_l^* = \{a_1^*, \ldots, a_k^*\}$ (assuming $l \geq k$) and $B_l = \{b_1, \ldots, b_l\}$, $B_l^* = \{b_1^*, \ldots, b_k^*\}$. Then the construction of Lemma 0.3 extends $A_l \cup A_l^*$ and $B_l \cup B_l^*$ to isomorphic bases and we can finish by an isomorphism of the structures as in the proof of Theorem 1. The isomorphism $\phi : F \to E$ sending $\langle a_1^*, \ldots, a_k^*, a_1, \ldots, a_l \rangle$ to $\langle b_1^*, \ldots, b_k^*, b_1, \ldots, b_l \rangle$ we have thus constructed uniquely determines that $\phi(\bar{a}) = \phi(\bar{b})$, since type $q$ tells how the tuple is co-ordinatised by the basis via semi-algebraic functions. This proves the claim.
and the theorem. □

References


[M] C.Miller *Tameness in expansions of the real field*, to appear in Logic Colloquium ’01