EDN: DRKHYP
УДК 512.74

Algebraic Subgroups of the Complex Torus

Nikolay A. Mishko[*]
Siberian Federal University
Krasnoyarsk, Russian Federation

Received 10.06.2024, received in revised form 15.07.2024, accepted 24.09.2024

Abstract. We study monomial parameterizations of algebraic subgroups of the torus over an arbitrary field and separately over the field of complex numbers. It is proved that every monomial parameterization defines an algebraic group. The necessary and sufficient conditions for the injectivity and existence of such parameterizations are obtained.

Keywords: algebraic subgroups, monomial parameterization, complex algebraic torus.

Citation: N.A. Mishko, Algebraic Subgroups of the Complex Torus, J. Sib. Fed. Univ. Math. Phys., 2024, 17(6), 721–731. EDN: DRKHYP.

An algebraic subgroup of a group G is a subgroup endowed with an algebraic variety structure, i.e. defined by means of a system of polynomial equations. A natural example of the algebraic group is a set of solutions of a system of binomial equations: $z_1^{\alpha_1} z_2^{\alpha_2} \dots z_n^{\alpha_n} = z_1^{\beta_1} z_2^{\beta_2} \dots z_n^{\beta_n}$.

The following theorem shows that such groups in fact exhaust all algebraic varieties globally inheriting the group structure of the torus $(K^\times)^n$.

For vectors $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n$ and $z = (z_1, \dots, z_n) \in G^n$ (where G is a group) we write $z^\alpha = z_1^{\alpha_1} \cdot z_2^{\alpha_2} \cdot \dots \cdot z_n^{\alpha_n}$.

Theorem (Schmidt) [1]. *Let K be a field. Every algebraic subgroup H of the group $(K^\times)^n$ is defined by a system of some number N of binomial equations, namely, there are N indices $\alpha_i, \beta_i \in \mathbb{Z}^n$ such that $H = \{z \in (K^\times)^n \mid \forall 1 \leqslant i \leqslant N\colon z^{\alpha_i} = z^{\beta_i}\}$.*

Next, we'll give a self-contained (independent of other major theorems) proof of this theorem. For this purpose, we need an auxiliary statement.

1. Artin's theorem

We denote the set of homomorphisms between groups G and H by $\mathrm{Hom}(G, H)$.

Let G be a group, K be a field, and $K^\times$ be its multiplicative group. Then an arbitrary homomorphism $f \in \mathrm{Hom}(G, K^\times)$ is called *a character.* The characters $f_1, f_2, \dots, f_n$ are *linearly independent* if $\forall \alpha_1, \alpha_2, \dots, \alpha_n \in K\colon \alpha_1 f_1 + \alpha_2 f_2 + \dots + \alpha_n f_n = 0 \Rightarrow \alpha_1 = \alpha_2 = \dots = \alpha_n = 0$.

Theorem (Artin) [2]. *Any n pairwise distinct characters are linearly independent.*

Proof. Let us prove by induction on the number of characters n.

Take an arbitrary character f. Since it is a homomorphism, $f(1_G) = 1$ where 1_G is an identity element in the group G. But then if $\alpha f = 0$, then $\alpha = \alpha \cdot 1 = \alpha \cdot f(1_G) = 0$, which proves the base case.

Now let the statement of theorem be true for any n distinct characters. Let us prove it for $n+1$ characters. Let $\alpha_1 f_1 + \alpha_2 f_2 + \dots + \alpha_n f_n + \alpha_{n+1} f_{n+1} = 0$.

[*] siegmentationfault@yandex.ru

Fix an arbitrary $y \in G$. The for any $x \in G$ we have:

$$\alpha_1 f_1(yx) + \alpha_2 f_2(yx) + \ldots + \alpha_n f_n(yx) + \alpha_{n+1} f_{n+1}(yx) = 0. \tag{1}$$

Since all f_i are homomorphisms, $f_i(yx) = f_i(y) f_i(x)$, and therefore:

$$\alpha_1 f_1(y) f_1(x) + \alpha_2 f_2(y) f_2(x) + \ldots + \alpha_n f_n(y) f_n(x) + \alpha_{n+1} f_{n+1}(y) f_{n+1}(x) = 0.$$

On the other hand, for $x \in G$ it is also true that: $\alpha_1 f_1(x) + \alpha_2 f_2(x) + \ldots + \alpha_n f_n(x) + \alpha_{n+1} f_{n+1}(x) = 0$.

Multiplying this equation by $f_{n+1}(y)$, we'll get:

$$\alpha_1 f_{n+1}(y) f_1(x) + \alpha_2 f_{n+1}(y) f_2(x) + \ldots + \alpha_n f_{n+1}(y) f_n(x) + \alpha_{n+1} f_{n+1}(y) f_{n+1}(x) = 0. \tag{2}$$

Subtracting (1) from (2), we obtain: $\alpha_1(f_{n+1}(y) - f_1(y)) f_1(x) + \ldots + \alpha_n(f_{n+1}(y) - f_n(y)) f_n(x) = 0$. x was chosen arbitrarily, so we get a linear combination of n characters: $\alpha_1(f_{n+1}(y) - f_1(y)) f_1 + \ldots + \alpha_n(f_{n+1}(y) - f_n(y)) f_n = 0$.

But then, using the inductive hypothesis, $\alpha_i(f_{n+1}(y) - f_i(y)) = 0$. Now, choosing y for each $i = 1, \ldots, n$ such that $f_{n+1}(y) \neq f_i(y)$ (it's always possible because all f_i are pairwise distinct), we obtain that $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$.

Thus, given the above, $\alpha_{n+1} f_{n+1} = \alpha_1 f_1 + \alpha_2 f_2 + \ldots + \alpha_n f_n + \alpha_{n+1} f_{n+1} = 0$. According to the base case again, $\alpha_{n+1} = 0$. □

2. Proof of Schmidt's theorem

Proof. Let $I \subseteq \mathbb{Z}^n$ be a finite set of indices, and let $P_j(z) = \sum\limits_{i \in I} a_{ji} z^i$ be the k polynomials defining the subgroup: $H = \{z \in (K^\times)^n \mid \forall 1 \leqslant j \leqslant k\colon P_j(z) = 0\}$.

Since $z_1^i z_2^i = (z_1 z_2)^i$, the mapping $z \mapsto z^i$ defines character $\chi_i \in \operatorname{Hom}(H, K^\times)$.

Consider an equivalence relation $i \sim j \Leftrightarrow \chi_i = \chi_j$ on the set I. It partitions I into m classes I_1, I_2, $\ldots$, I_m. Then for all $i_1, i_2 \in I_j$ it is true that $\chi_{i_1} = \chi_{i_2}$. Let us denote this character corresponding to each I_k by $\chi_k = \chi_{i_1} = \chi_{i_2}$.

Combining like terms at each χ_k in the polynomials P_j, we obtain:

$$P_j = \sum_{i \in I} a_{ji} \chi_i = \sum_{k=1}^{m} \left(\sum_{i \in I_k} a_{ji} \right) \chi_k.$$

But P_j vanishes on the whole H, so: $\sum\limits_{k=1}^{m} \left(\sum\limits_{i \in I_k} a_{ji} \right) \chi_k = 0$.

All χ_k are pairwise distinct by their definition, so Artin's theorem applies. We conclude that: $\sum\limits_{i \in I_k} a_{ji} = 0$.

Finally, let N_k be the cardinality of I_k, $I_k = \{i_{k,1}, i_{k,2}, \ldots, i_{k,N_k}\}$, and $N = \sum\limits_{k=1}^{m} (N_k - 1)$. I_k were taken such that the characters $\chi_{i_{k,i}}$ and $\chi_{i_{k,j}}$ coincide on H for fixed k and any i and j. In other words, this means that any element $z \in H$ satisfies the equations $z^{i_{k,i}} = z^{i_{k,j}}$ for all $1 \leqslant i \leqslant N_k$ and $1 \leqslant j \leqslant N_k$.

Since the equality is reflexive, symmetric, and transitive, the system of all equations $z^{i_{k,i}} = z^{i_{k,j}}$ is equivalent to the system of N equations composed of consecutive indices:

$$z^{i_{1,1}} = z^{i_{1,2}}, z^{i_{1,2}} = z^{i_{1,3}}, \ldots, z^{i_{1,N_1 - 1}} = z^{i_{1,N_1}}, z^{i_{2,1}} = z^{i_{2,2}}, \ldots, z^{i_{m,N_m - 1}} = z^{i_{m,N_m}}.$$

We denote the set of solutions of this system by A.

Let us show that A coincides with H. Indeed, let $z \in H$. Then, as noted before, by definition of I_k it is true that $z^{i_{k,j}} = \chi_k(z) = z^{i_{k,j+1}}$; that is, $z \in A$ and $H \subseteq A$.

Conversely, let $z \in A$. Then by definition of A we have $z^{i_{k,j_1}} = z^{i_{k,j_1+1}} = \ldots = z^{i_{k,j_2-1}} = z^{i_{k,j_2}}$ for all $1 \leqslant j_1 \leqslant j_2 \leqslant N_k$. Choose a representative $i_k \in I_k$ in each I_k and combine like terms:

$$P_j(z) = \sum_{k=1}^{m} \left(\sum_{i \in I_k} a_{ji} \right) z^{i_k} = \sum_{k=1}^{m} 0 \cdot z^{i_k} = 0,$$

which means $z \in H$, that is, $A \subseteq H$.

Thus, $H = A$, so it suffices to take all the consecutive indices from I_k as α_i and β_i. □

3. Injectivity of monomial parameterizations

For an abelian group G and vectors $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}^k$ consider the mapping $\phi_\alpha(t) = (t^{\alpha_1}, t^{\alpha_2}, \ldots, t^{\alpha_n})$ from G^k to G^n where α is a matrix with rows α_i. Since $(t_1 \cdot t_2)^{\alpha_i} = t_1^{\alpha_i} \cdot t_2^{\alpha_i}$, ϕ_α is a homomorphism. Further we will see that if K is a field, then the mapping ϕ_α for the group $G = K^\times$ defines *a parameterization* of some algebraic group.

Proposition. *$\phi_E = 1_{G^n}$ where E is an $n \times n$ identity matrix, 1_X is an identity function on X.*

Proposition. $\forall \alpha \in \mathbb{Z}^{k \times m}$, $\beta \in \mathbb{Z}^{m \times n}$: $\phi_\alpha \circ \phi_\beta = \phi_{\alpha\beta}$.

Proof. Indeed, consider $t \in G^n$. Then the i-th component of $\phi_\alpha(\phi_\beta(t))$ is equal to $\phi_\beta^{\alpha_i}(t) = (t^{\beta_1})^{\alpha_i^1} \ldots (t^{\beta_m})^{\alpha_i^m} = t_1^{\beta_1^1 \alpha_i^1 + \ldots + \beta_m^1 \alpha_i^m} \ldots t_n^{\beta_1^n \alpha_i^1 + \ldots + \beta_m^n \alpha_i^m} = t^{(\alpha\beta)_i}$. □

Together these two propositions constitute a condition for functoriality. More precisely, consider the category $\mathrm{Matr}(R)$ of matrices over the ring R whose objects are the natural numbers and the arrows between the numbers m and n are the matrices $R^{n \times m}$, and the category Grp of small groups with small groups as objects and homomorphisms between them as arrows. Then the functor $\phi : \mathrm{Matr}(\mathbb{Z}) \to \mathrm{Grp}$ is defined:

$$\phi = \begin{cases} k \mapsto G^k; \\ \alpha \mapsto \phi_\alpha. \end{cases}$$

As Lemma 2 shows, in fields of characteristic zero this functor is faithful.

Lemma 1. *Let K be a field such that* $\mathrm{char}(K) = 0$. *Then $K^\times$ contains an element of infinite order.*

Proof. Indeed, consider $2 = 1 + 1 \in K^\times$. Then for any $n > 0$:

$$2^n - 1 = (1+1)^n - 1 = \sum_{k=0}^{n} C_k^n 1^k 1^{n-k} - 1 = \sum_{k=0}^{n} C_k^n \cdot 1 - 1 = \left(\sum_{k=1}^{n} C_k^n \right) \cdot 1.$$

On the right side we have the sum of $\sum\limits_{k=1}^{n} C_k^n > 0$ units. Since $\mathrm{char}(K) = 0$, this sum is not equal to zero, that is, $2^n - 1 \neq 0$. □

We denote *a standard basis* over $\mathbb{Z}^k$ by e_i, that is, a vector with one on the i-th place and zeroes on the others. We denote the j-th component of the vector α_i by α_i^j and the vector consisting of the j-th components by $\alpha^j = (\alpha_1^j, \alpha_2^j, \ldots, \alpha_n^j)$.

Lemma 2. $\operatorname{char}(K) = 0 \Rightarrow \forall \alpha, \beta \in \mathbb{Z}^{n\times k}$: $\phi_\alpha = \phi_\beta \Leftrightarrow \alpha = \beta$.

Proof. The left-to-right implication is obvious.

Conversely, let $\phi_\alpha = \phi_\beta$. Using Lemma 1 we fix an element $z \in K^\times$ of infinite multiplicative order. Then for all $1 \leqslant i \leqslant n$ it is true that $(z^{\alpha^i_1}, \dots, z^{\alpha^i_k}) = \phi_\alpha(z\cdot e_i) = \phi_\beta(z\cdot e_i) = (z^{\beta^i_1}, \dots, z^{\beta^i_k})$.

Thus, $z^{\alpha^i_j} = z^{\beta^i_j}$, that is, $z^{\alpha^i_j - \beta^i_j} = 1$. z has infinite multiplicative order, so $\alpha^i_j - \beta^i_j = 0$. □

We denote a $\mathbb{Z}$-*linear span* of α_1, …, α_n by $\operatorname{Span}_{\mathbb{Z}}(\alpha_1, \dots, \alpha_n) = \{k_1\alpha_1 + \dots + k_n\alpha_n \mid k_1, \dots, k_n \in \mathbb{Z}\}$. We say that α_1, …, α_n span the whole lattice $\mathbb{Z}^k$ if $\operatorname{Span}_{\mathbb{Z}}(\alpha_1, \dots, \alpha_n) = \mathbb{Z}^k$.

It is easy to obtain a necessary condition for the injectivity of the mapping ϕ_α. For this purpose, we note that the following proposition is obvious.

Proposition. $\operatorname{Span}_{\mathbb{Z}}(\alpha_1, \dots, \alpha_n) = \mathbb{Z}^k \Leftrightarrow \forall i$: $e_i \in \operatorname{Span}_{\mathbb{Z}}(\alpha_1, \dots, \alpha_n)$.

Lemma 3. *If vectors $\alpha_i \in \mathbb{Z}^k$ span the whole lattice $\mathbb{Z}^k$, then ϕ_α is injective.*

Proof. ϕ_α is a homomorphism, so it suffices to show that $\ker(\phi_\alpha) = \{1\}$. We'll take $t \in G^k$ such that $\phi_\alpha(t) = 1$ and prove that $t = 1$.

Indeed, since α_i span the whole lattice, each e_j can be expressed as their linear combination: $e_j = b^j_1\alpha_1 + \dots + b^j_n\alpha_n$.

$\phi_\alpha(t) = 1$ means $t^{\alpha_i} = 1$ for all $1 \leqslant i \leqslant n$. Fix $1 \leqslant j \leqslant k$ and raise both sides of this equation to the power of b^j_i: $t^{b^j_i\alpha_i} = (t^{\alpha_i})^{b^j_i} = 1^{b^j_i} = 1$. Finally, multiply the obtained equations: $t_j = t^{e_j} = t^{b^j_1\alpha_1+\dots+b^j_n\alpha_n} = t^{b^j_1\alpha_1} \dots t^{b^j_n\alpha_n} = 1 \cdot \ldots \cdot 1 = 1$. □

Now we will show that the obtained necessary condition is also sufficient for the group $G = \mathbb{C}^\times$.

We will use the existence of *Smith normal form* for integer matrices [3]. Let $\operatorname{diag}^{m\times n}_r(x_1, \dots, x_r)$ be a diagonal matrix $\operatorname{diag}(x_1, \dots, x_r)$ augmented (or cut off) from the bottom right by zeroes to a matrix of size $m \times n$.

Theorem (on the existence of Smith normal form).

$\forall \alpha \in \mathbb{Z}^{m\times n}$: $\exists \beta_1 \in \mathrm{GL}^m(\mathbb{Z}), \beta_2 \in \mathrm{GL}^n(\mathbb{Z})$: $\exists \varepsilon_1, \dots, \varepsilon_r \in \mathbb{Z} \setminus \{0\}$: $\beta_1\alpha\beta_2 = \operatorname{diag}^{m\times n}_r(\varepsilon_1, \dots, \varepsilon_r)$, *where* $\varepsilon_1 \mid \varepsilon_2 \mid \dots \mid \varepsilon_r$ *(the so-called invariant factors) and* $r = \operatorname{rank}(\alpha)$.

Since the numbers ε_1, …, ε_r are chosen in a unique way up to the invertible element, that is, up to ±1 in the case of $\mathbb{Z}$, we can always choose them positive. For them we denote the matrix $\operatorname{diag}^{m\times n}_r(\varepsilon_1, \dots, \varepsilon_r)$ by $\operatorname{SNF}(\alpha)$.

In addition, since ϕ defines the functor, it is clear that ϕ_β is bijective if $\beta \in \mathrm{GL}^n(\mathbb{Z})$. Indeed, $\phi_\beta \circ \phi_{\beta^{-1}} = \phi_{\beta\beta^{-1}} = \phi_E = 1_{(K^\times)^n}$ and $\phi_{\beta^{-1}} \circ \phi_\beta = \phi_{\beta^{-1}\beta} = \phi_E = 1_{(K^\times)^n}$. Therefore, the following lemma holds.

Lemma 4. $\phi_\alpha : (\mathbb{C}^\times)^k \to (\mathbb{C}^\times)^n$ *is injective if and only if*

$$\operatorname{SNF}(\alpha) = \operatorname{diag}^{n\times k}_k(1, 1, \dots, 1).$$

Proof. Using the theorem, let us take unimodular matrices $\beta_1 \in \mathrm{GL}^n(\mathbb{Z})$ and $\beta_2 \in \mathrm{GL}^k(\mathbb{Z})$ such that $\beta_1\alpha\beta_2 = \operatorname{SNF}(\alpha)$. Then, $\alpha = \beta_1^{-1}\operatorname{SNF}(\alpha)\beta_2^{-1}$ and $\phi_\alpha = \phi_{\beta_1^{-1}\operatorname{SNF}(\alpha)\beta_2^{-1}} = \phi_{\beta_1^{-1}} \circ \phi_{\operatorname{SNF}(\alpha)} \circ \phi_{\beta_2^{-1}}$.

Since, by the remark above, $\phi_{\beta_1^{-1}}$ and $\phi_{\beta_2^{-1}}$ are bijective, ϕ_α is injective if and only if $\phi_{\operatorname{SNF}(\alpha)}$ is injective.

$\phi_{\operatorname{SNF}(\alpha)}(t_1, \dots, t_k) = (t_1^{\varepsilon_1}, \dots, t_r^{\varepsilon_r}, 1, \dots, 1)$, but $t \mapsto t^\varepsilon$ is injective over $\mathbb{C}^\times$ only if $\varepsilon = \pm1$ (otherwise $t^\varepsilon = t^\varepsilon \cdot 1 = t^\varepsilon \cdot u^\varepsilon = (tu)^\varepsilon$ where $u \neq 1$ is a nontrivial ε-th root of unity). By choice of signs, $\phi_{\operatorname{SNF}(\alpha)}$ is injective only if $\varepsilon_1 = \ldots = \varepsilon_r = 1$ and $r = k \leqslant n$. □

Let us formulate one more auxiliary theorem [4].

Theorem 1. *Let $\alpha \in \mathbb{Z}^{n\times k}$. The following statements are equivalent:*

1. *The rows of the matrix α span the whole lattice $\mathbb{Z}^k$.*
2. *The maximal minors of the matrix α are coprime.*
3. $\mathrm{SNF}(\alpha) = \mathrm{diag}_k^{n\times k}(1, \dots, 1)$.

Thus, from Lemma 4 and Theorem 1 we obtain a necessary and sufficient condition for the injectivity of ϕ_α.

Theorem. *ϕ_α is injective over the field $K = \mathbb{C}$ if and only if α_i span the whole lattice $\mathbb{Z}^k$.*

4. Monomial parameterizability of torus subgroups

As in the case of the theory of curves and surfaces, we say that a subgroup of an algebraic torus is *parameterizable* if it can be expressed as an image of some mapping. Similarly, a subgroup is *monomially parameterizable* if it can be expressed as an image of ϕ_α for some matrix α.

Since ϕ_α is the homomorphism, its image $\mathrm{Im}(\phi_\alpha)$ is a subgroup in $(K^\times)^n$. Next we'll study two questions: whether $\mathrm{Im}(\phi_\alpha)$ is an algebraic subgroup and whether any algebraic subgroup is expressed by some ϕ_α.

For this, first of all, we note that the system of binomial equations $z^{\beta'_i} = z^{\beta''i}$ is equivalent to the system $z^{\beta'_i - \beta''_i} = 1$, that is, exactly the kernel of the operator $\phi_{\beta'_i - \beta''_i}$; therefore, the first question is equivalent to whether a given homomorphism ϕ_α can be extended to the exact sequence $(K^\times)^k \xrightarrow{\phi_\alpha} (K^\times)^n \xrightarrow{\phi_\beta} (K^\times)^m$.

Lemma 5. *Let G be a group, H be an abelian group, $f \in \mathrm{Hom}(G, H)$, $g \in \mathrm{Hom}(H, G)$, and $g \circ f = 1_G$. Then the sequence $G \xrightarrow{f} H \xrightarrow{f\circ g - 1_H} H$ is exact.*

Proof. Indeed, $(f \circ g - 1_H) \circ f = f \circ g \circ f - f = f - f = 0$, that is, $\mathrm{Im}(f) \subseteq \ker(f \circ g - 1_H)$. Conversely, let $h \in \ker(f \circ g - 1_H)$. Then $f(g(h)) - h = 0 \Leftrightarrow h = f(g(h))$, that is, $h \in \mathrm{Im}(f)$ and $\ker(f \circ g - 1_H) \subseteq \mathrm{Im}(f)$. □

Lemma 6. *ϕ_α for $\alpha \in \mathbb{Z}^{n\times k}$ can be expressed as some image $\mathrm{Im}(\phi_\beta)$ if the mappings $g \mapsto g^{\varepsilon_i}$ are surjective in G for all ε_i from $\mathrm{SNF}(\alpha)$.*

Proof. Let us again write α as $\alpha = \beta_1^{-1}\varepsilon\beta_2^{-1}$ where $\varepsilon = \mathrm{diag}_r^{n\times k}(\varepsilon_1, \dots, \varepsilon_r)$.

Consider $\delta = \mathrm{diag}_r^{n\times r}(1, \dots, 1)$ and $\alpha' = \beta^{-1}\delta$. $\phi_{\alpha'}$ is injective since it is a composition of injective functions. On the other hand, it is obvious that:

$$\mathrm{Im}(\phi_\alpha) = \phi_{\beta_1^{-1}}(\phi_\varepsilon(\phi_{\beta_2^{-1}}(G^k))) = \phi_{\beta_1^{-1}}(\phi_\varepsilon(G^k)) = \phi_{\beta_1^{-1}}(\phi_\delta(G^r)) = \mathrm{Im}(\phi_{\alpha'}).$$

It is easy to see that $\beta' = \delta^\top\beta$ is a left inverse of the matrix α', and hence $\phi_{\beta'}$ is a left inverse of $\phi_{\alpha'}$. Since $(\phi_{\alpha'} \circ \phi_{\beta'})\phi_{-E} = \phi_{\alpha'\beta' - E}$, we only need to apply Lemma 5. □

Theorem 2. *Any parameterization ϕ_α for $\alpha \in \mathbb{Z}^{n\times k}$ defines an algebraic subgroup of $(K^\times)^n$ if the field K is algebraically closed.*

The answer to the second question is somewhat more complicated. For example, the equation $z^n = 1$ defines an algebraic group for any $n \in \mathbb{Z}$ consisting of n points on $\mathbb{C}^\times$; but if $n \neq 0, \pm 1$ it is easy to see that it cannot be parameterized by any ϕ_α.

Indeed, notice that the group $\operatorname{Im}(\phi_\alpha)$ is isomorphic to the group $(\mathbb{C}^\times)^r$. In the proof of Lemma 6 we saw that for any ϕ_α we can construct an injective $\phi_{\alpha'} : (\mathbb{C}^\times)^r \to (\mathbb{C}^\times)^n$ such that $\operatorname{Im}(\phi_\alpha) = \operatorname{Im}(\phi_{\alpha'})$; but then $\phi_{\alpha'}$ defines the desired isomorphism. Thus, the following proposition holds.

Proposition. *For any matrix $\alpha \in \mathbb{Z}^{n\times k}$ the group $\operatorname{Im}(\phi_\alpha)$ is isomorphic to an algebraic torus of dimension at mosk k.*

Moreover, since the mapping $\phi_{\alpha'}$ is polynomial, it is, in particular, continuous in the standard topology on $K = \mathbb{C}$. The set $(\mathbb{C}^\times)^r$ is connected, and, as we know, the continuous image of a connected set is connected, so next proposition is also true.

Proposition. $\operatorname{Im}(\phi_\alpha) \subseteq (\mathbb{C}^\times)^n$ *is connected.*

Now notice that the group $z^n = 1$ is connected exactly when $n = 0, \pm 1$. This indicates that the criterion for the existence of a monomial parameterization for an algebraic torus subgroup is connectedness.

We denote the group of n-th root of unity in the field K (given by the equation $z^n = 1$) by $\omega_K(n) \subseteq K^\times$. For a vector $x \in \mathbb{Z}^k$ we denote $\omega_K(x) = \omega_K(x_1) \times \ldots \times \omega_K(x_k) \subseteq (K^\times)^k$. For brevity, we will write $\omega(x) = \omega_{\mathbb{C}}(x)$. It is known that the group $\omega(x)$ is isomorphic to the group $\mathbb{Z}/x_1\mathbb{Z} \times \ldots \times \mathbb{Z}/x_k\mathbb{Z}$.

To prove the criterion described before, consider the number $\Pi(\alpha) = |\omega_K(\varepsilon)|$ where $|G|$ is the order of the group G. $|G \times H| = |G||H|$, so $\Pi(\alpha) = |\omega_K(\varepsilon_1)| \cdot \ldots \cdot |\omega_K(\varepsilon_r)|$. Since $\omega(n)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, in the case of the field $K = \mathbb{C}$ it is also true that $\Pi(\alpha) = \varepsilon_1 \cdot \ldots \cdot \varepsilon_r$.

Lemma 7. *If $\Pi(\beta) = 1$, then there is α such that $\ker(\phi_\beta) = \operatorname{Im}(\phi_\alpha)$.*

Proof. Let $H = \ker(\phi_\beta)$. Without loss of generality, we assume that the rows of the matrix β are linearly independent over $\mathbb{Z}$ (it is clear that the rows expressed as a linear combination of the other rows can be removed from the matrix β without changing the kernel).

Let us write the Smith normal form for β: $\beta = \beta_1^{-1}\varepsilon\beta_2^{-1}$. Since, according to the remark above, β has full rank, the matrix ε has no zero rows. Furthermore, $\Pi(\beta) = 1$, so $|\omega_K(\varepsilon_i)| = 1$, that is, the equations $z^{\varepsilon_i} = 1$ have only $z = 1$ as a solution.

The kernel of ε is given by vectors of the form $(0, \ldots, 0, t_{k+1}, \ldots, t_n)$. Consider a matrix $\delta \in \mathbb{Z}^{n\times(n-k)}$ corresponding to the linear operator

$$(t_1, \ldots, t_{n-k}) \mapsto (0, \ldots, 0, t_1, \ldots, t_{n-k}).$$

Let also $\alpha = \beta_2\delta$. We'll prove that $\operatorname{Im}(\phi_\alpha) = \ker(\phi_\beta)$.

Indeed, by definition of δ it holds that δ, $\varepsilon\delta = 0$, so $\phi_\beta \circ \phi_\alpha = \phi_{\beta_1^{-1}\varepsilon\beta_2^{-1}\beta_2\delta} = \phi_{\beta_1^{-1}\varepsilon\delta} = \phi_0 = 1$, that is, $\operatorname{Im}(\phi_\alpha) \subseteq \ker(\phi_\beta)$.

Conversely, let $z \in \ker(\phi_\beta)$. Then $\phi_{\beta_1^{-1}}(\phi_{\varepsilon\beta_2^{-1}}(z)) = \phi_\beta(z) = 1$, so $\phi_\varepsilon(\phi_{\beta_2^{-1}}(z)) = \phi_{\varepsilon\beta_2^{-1}}(z) = \phi_{\beta_1}(1) = 1$. From the form of the matrix ε we obtain that $\phi_{\beta_2^{-1}}(z) = (1, \ldots, 1, t_{k+1}, \ldots, t_n) = \phi_\delta(t_{k+1}, \ldots, t_n)$; that is, $z = \phi_{\beta_2}(\phi_\delta(t_{k+1}, \ldots, t_n)) = \phi_\alpha(t_{k+1}, \ldots, t_n)$ for some t_j. Thus, $z \in \operatorname{Im}(\phi_\alpha)$ and $\ker(\phi_\beta) \subseteq \operatorname{Im}(\phi_\alpha)$. □

Theorem 3. *The number of connected components of $\ker(\phi_\beta) \subseteq (\mathbb{C}^\times)^n$ is equal to $\Pi(\beta)$.*

Proof. Consider again the Smith normal form of β: $\beta = \beta_1^{-1}\varepsilon\beta_2^{-1}$. $\phi_{\beta_1^{-1}}$ is isomorphism, so $\ker(\phi_\beta) = \ker(\phi_{\varepsilon\beta_2^{-1}})$.

We denote the rows of β_2^{-1} by b_i. For a vector $u \in \omega(\varepsilon)$ consider the set $H_u = \{z \in (\mathbb{C}^\times)^n \mid \forall 1 \leqslant i \leqslant r\colon z^{b_i} = u_i\}$. The condition $\phi_\varepsilon(\phi_{\beta_2^{-1}}(z)) = 1$ is obviously equivalent to the condition $\exists u \in \omega(\varepsilon)$: $z \in H_u$. Clearly, the sets H_u are disjunctive, so $\ker(\phi_\beta)$ decomposes into a disjunctive union: $\ker(\phi_\beta) = \bigsqcup_{u\in\omega(\varepsilon)} H_u$. There are exactly $\Pi(\beta)$ vectors $u \in \omega(\varepsilon)$, so it suffices to show that each component H_u is connected.

Since, by definition, $H_1 = \ker(\phi_{\delta\beta_2^{-1}})$ where $\delta = \mathrm{diag}_r^{k\times n}(1,\dots,1)$ and $\Pi(\delta\beta_2^{-1}) = 1$, the component H_1 is connected by the remark.

Fix u and consider the matrix $\tau = \mathrm{diag}(1/u_1,\dots,1/u_r,1,\dots,1)$ and the mapping $\psi = \phi_{\beta_2} \circ \phi_\tau \circ \phi_{\beta_2^{-1}}$. ψ is a continuous bijection, moreover, $\psi^{-1} = \phi_{\beta_2} \circ \phi_{\tau^{-1}} \circ \phi_{\beta_2^{-1}}$.

By definition, $\phi_{\beta_2^{-1}}(\psi(z)) = \phi_{\tau\beta_2^{-1}}(z)$. So if $z \in H_u$, then $\psi(z)^{b_i} = z^{b_i}/u_i = u_i/u_i = 1$. Conversely, if $z \in H_1$, then $\psi^{-1}(z)^{b_i} = u_i z^{b_i} = u_i$. Thus, $\psi(H_u) = H_1$, that is, H_u is homeomorphic to H_1, but H_1 is connected. □

As we saw before, any algebraic subgroup H of the torus $(K^\times)^n$ can be expressed as $\ker(\phi_\beta)$ for some β. Notice that $\Pi(\beta)$ does not depend on the choice of β for the group H.

Theorem 4. *If* $\mathrm{char}(K) = 0$ *and* $\ker(\phi_\beta) = \ker(\phi_{\beta'})$*, then* $\Pi(\beta) = \Pi(\beta')$.

Proof. Let us write down the Smith normal forms: $\beta = \beta_1^{-1}\varepsilon\beta_2^{-1}$ and $\beta' = {\beta'}_1^{-1}\varepsilon'{\beta'}_2^{-1}$. So we have: $\ker(\phi_{\varepsilon\beta_2^{-1}}) = \ker(\phi_\beta) = \ker(\phi_{\beta'}) = \ker(\phi_{\varepsilon'{\beta'}_2^{-1}})$.

Let $\varepsilon = \mathrm{diag}_r^{k\times n}(\varepsilon_1,\dots,\varepsilon_r)$ and $\varepsilon' = \mathrm{diag}_{r'}^{k'\times n}(\varepsilon'_1,\dots,\varepsilon'_r)$. We write $\delta = \mathrm{diag}_r^{k\times n}(1,\dots,1)$ and $\delta' = \mathrm{diag}_{r'}^{k'\times n}(1,\dots,1)$.

Since $\Pi(\delta\beta_2^{-1}) = \Pi(\delta'{\beta'}_2^{-1}) = 1$, both groups are parameterized according to Lemma 7 by some ϕ_α and $\phi_{\alpha'}$ respectively.

$\mathrm{Im}(\phi_\alpha) = \ker(\phi_{\delta\beta_2^{-1}}) \subseteq \ker(\phi_{\varepsilon\beta_2^{-1}}) = \ker(\phi_{\varepsilon'{\beta'}_2^{-1}})$, so $\phi_{\varepsilon'{\beta'}_2^{-1}} \circ \phi_\alpha = 1$. Using Lemma 2, $\varepsilon'{\beta'}_2^{-1}\alpha = 0$. Multiplying both sides of the equality by the matrix $\mathrm{diag}(1/\varepsilon'_1,\dots,1/\varepsilon'_r,1,\dots,1)$ one obtains that $\delta'{\beta'}_2^{-1}\alpha = 0$; but this means that $\ker(\phi_{\delta\beta_2^{-1}}) = \mathrm{Im}(\phi_\alpha) \subseteq \ker(\phi_{\delta'{\beta'}_2^{-1}})$. Similarly we get the converse inclusion. Thus, $\ker(\phi_{\delta\beta_2^{-1}}) = \ker(\phi_{\delta'{\beta'}_2^{-1}})$.

Consider the quotient group $\ker(\phi_\beta)/\ker(\phi_{\delta\beta_2^{-1}}) = \ker(\phi_{\beta'})/\ker(\phi_{\delta'{\beta'}_2^{-1}})$, also called *the component group.* The mapping $\phi_{\delta\beta_2^{-1}} : \ker(\phi_\beta) \to \omega_K(\varepsilon) \times \{1\} \times \ldots \times \{1\}$ induces an injective homomorphism from the quotient. In addition, in the Theorem 3 the bijection between the components H_u was constructed (it generalises unchanged to the case of an arbitrary field K), and hence they are all nonempty. This means that $\phi_{\delta\beta_2^{-1}}$ is surjective, so the induced mapping is also surjective. The reasoning is similar for the group $\omega_K(\varepsilon')$. Thus, we have a chain of isomorphisms:

$$\omega(\varepsilon) \cong \ker(\phi_\beta)/\ker(\phi_{\delta\beta_2^{-1}}) = \ker(\phi_{\beta'})/\ker(\phi_{\delta'{\beta'}_2^{-1}}) \cong \omega(\varepsilon').$$

Isomorphic groups have the same order, and hence $\Pi(\beta) = |\omega_K(\varepsilon)| = |\omega_K(\varepsilon')| = \Pi(\beta')$. □

Finally, for any algebraic subgroup H of the torus we can define a number $\Pi(H)$ equal to $\Pi(\beta)$ for any β such that $H = \ker(\phi_\beta)$.

Now for any algebraic subgroup $H \subseteq (\mathbb{C}^\times)^n$ we define *the identity component* H° as a connected component containing an identity element of the group H. It follows from Theorem 3 that $\Pi(H^\circ) = 1$. Thus, the following statements are proved.

Theorem 5. *An algebraic subgroup* H *of the torus* $(K^\times)^n$ *is parameterizable if and only if* $\Pi(H) = 1$.

Consequence. *An algebraic subgroup* H *of the torus* $(\mathbb{C}^\times)^n$ *is parameterizable if and only if it is connected.*

Consequence. *Every algebraic subgroup H of the torus $(\mathbb{C}^\times)^n$ contains a parameterizable subgroup H° of the same dimension.*

Proof. All components of H are homeomorphic, what immediately proves the theorem. □

5. Linear independence over an abelian group

In any abelian group G there is naturally defined multiplication by integers. For a vector $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{Z}^k$ and element $g \in G$ we mean by $g\alpha$ the vector $(\alpha_1 g, \ldots, \alpha_k g) \in G^k$. We say that the collection of vectors $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}^k$ is *linearly independent over an abelian group* if

$$\forall g_1, \ldots, g_n \in G\colon g_1\alpha_1 + \ldots + g_n\alpha_n = 0 \Rightarrow g_1 = \ldots = g_n = 0.$$

We see that the linear independence of vectors from $\mathbb{Z}^k$ over the additive group of the field $\mathbb{R}$ is equivalent to the ordinary linear independence in the vector space $\mathbb{R}^k$. However, for example, $\mathbb{R}/2\pi\mathbb{Z}$, as it is known, has no ring structure, so it makes no sense to talk about the $\mathbb{R}/2\pi\mathbb{Z}$-module $(\mathbb{R}/2\pi\mathbb{Z})^k$, as well as about linear independence in it.

Let us immediately show how this definition is related to the studied parameterizations ϕ_α.

Theorem 6. *$\phi_\alpha : G^k \to G^n$ is injective if and only if α^j are linearly independent over the group G.*

Proof. It follows directly from the fact that the injectivity of a homomorphism is equivalent to the triviality of its kernel. □

Next, we need two general lemmas.

Lemma 8. *Let G and H be abelian groups. $\mu_1, \ldots, \mu_n \in \mathbb{Z}^k$ are linearly independent over $G \times H$ if and only if they are linearly independent over G and over H.*

Proof. The elements of $G \times H$ can be expressed as pairs (g, h) where $g \in G$ and $h \in H$, so linear independence over $G \times H$ can be written as:

$$\forall (g_1, h_1) \ldots, (g_n, h_n) \in G \times H\colon (g_1, h_1)\mu_1 + \ldots + (g_n, h_n)\mu_n = 0 \Rightarrow (g_1, h_1) = \ldots = (g_n, h_n) = 0.$$

Furthermore, it is clear that

$$(g_1, h_1)\mu_1 + \ldots + (g_n, h_n)\mu_n = 0 \Leftrightarrow g_1\mu_1 + \ldots + g_n\mu_n = 0 \wedge h_1\mu_1 + \ldots + h_n\mu_n = 0,$$

as well as

$$(g_1, h_1) = \ldots = (g_n, h_n) = 0 \Leftrightarrow g_1 = \ldots = g_n = 0 \wedge h_1 = \ldots = h_n = 0.$$

By fixing $g_1 = \ldots = g_n = 0$ and then $h_1 = \ldots = h_n = 0$, we'll obtain the left-to-right implication. The right-to-left implication is obvious. □

Lemma 9. *Let G and H be abelian groups, $f : G \to H$ be an isomorphism. Then $\mu_1, \ldots, \mu_n \in \mathbb{Z}^k$ are linearly independent over G if and only if they are linearly independent over H.*

Proof. Since f is an isomorphic, we obtain a chain of equivalences:

$$\begin{aligned}
&\forall g_1, \ldots, g_n \in G\colon g_1\alpha_1 + \ldots + g_n\alpha_n = 0 \Rightarrow g_1 = \ldots = g_n = 0\\
\Leftrightarrow\ &\forall g_1, \ldots, g_n \in G\colon f(g_1\alpha_1 + \ldots + g_n\alpha_n) = 0 \Rightarrow g_1 = \ldots = g_n = 0\\
\Leftrightarrow\ &\forall g_1, \ldots, g_n \in G\colon f(g_1)\alpha_1 + \ldots + f(g_n)\alpha_n = 0 \Rightarrow f(g_1) = \ldots = f(g_n) = 0\\
\Leftrightarrow\ &\forall h_1, \ldots, h_n \in H\colon h_1\alpha_1 + \ldots + h_n\alpha_n = 0 \Rightarrow h_1 = \ldots = h_n = 0.
\end{aligned}$$
□

Applying the lemmas, we obtain the injectivity criterion for the case $K = \mathbb{C}$.

Consequence. *ϕ_α is injective if and only if α^j are linearly independent over the groups $\mathbb{R}$ and $\mathbb{R}/2\pi\mathbb{Z}$.*

Proof. Let $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ be a circle group, a subgroup in $\mathbb{C}^\times$. From the trigonometric form $z = re^{i\theta}$ we see that the group $\mathbb{C}^\times$ is isomorphic to the product $\mathbb{R}^\times_{>0} \times S^1$. The mapping $t \mapsto e^t$ defines the isomorphism of the groups $\mathbb{R}$ and $\mathbb{R}^\times_{>0}$, and the mapping $\theta \mapsto e^{i\theta}$ defines the isomorphism between $\mathbb{R}/2\pi\mathbb{Z}$ and S^1; this proves a corollary by virtue of the previous two lemmas. □

Consequence. *If ϕ_α is injective over $K = \mathbb{C}$, then* $\operatorname{rank}(\alpha) = k$*.*

Proof. As noted before, linear independence over $\mathbb{R}$ is equivalent to linear independence in the vector space $\mathbb{R}^k$ over $\mathbb{R}$, and this in turn is equivalent to having full rank. □

In particular, this means that a parameterization with the $k > n$ variables is automatically non-injective, which is to be expected.

Noticing that $\mathbb{R}^\times_{>0} \cong \mathbb{R}^\times_{>0} \times \mathbb{Z}/1\mathbb{Z}$, $\mathbb{R}^\times \cong \mathbb{R}^\times_{>0} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{H}^\times \cong \mathbb{R}^\times_{>0} \times S^3$ (quaternions), it is easy to obtain similar conditions for the injectivity of ϕ_α over the groups $\mathbb{R}^\times_{>0}$, $\mathbb{R}^\times$, and $\mathbb{H}^\times$.

It seems natural that, since the vectors α^j are integer-valued, their linear independence over $\mathbb{R}$ must reduce to linear independence over $\mathbb{Z}$. Let us prove this.

Lemma. *$\mu_1, \ldots, \mu_n \in \mathbb{Z}^k$ are linearly independent over $\mathbb{R}$ if and only if they are linearly independent over $\mathbb{Q}$.*

Proof. The left-to-right implication is obvious. Conversely, let $\mu_1, \ldots, \mu_n$ be linearly independent over $\mathbb{Q}$. Consider their linear combination: $r_1\mu_1 + \ldots + r_n\mu_n = 0$.

It is known that $\mathbb{R}$ is an (infinite-dimensional) vector space over $\mathbb{Q}$, and any vector space has a (Hamel) basis under the assumption of the axiom of choice [5]. Using this, let us fix a Hamel basis B for $\mathbb{R}$ over $\mathbb{Q}$. Let us decompose r_i by this basis:

$$r_i = q_i^1 b_1 + \ldots + q_i^s b_s$$

where $q_i^j \in \mathbb{Q}$ and $b_j \in B$. There are finitely many vectors r_i, so the set of basis vectors b_j for them can be chosen to be the same. Let us substitute the decomposition into the linear combination:

$$\begin{aligned} r_1\mu_1 + \ldots + r_n\mu_n &= (q_1^1 b_1 + \ldots + q_1^s b_s)\mu_1 + \ldots + (q_n^1 b_1 + \ldots + q_n^s b_s)\mu_n = \\ &= (q_1^1\mu_1 + \ldots + q_n^1\mu_n)b_1 + \ldots + (q_1^s\mu_1 + \ldots + q_n^s\mu_n)b_s = \\ &= 0. \end{aligned}$$

We obtain in each coordinate a rational linear combination of the numbers b_j equal to zero. By virtue of linear independence, all these coordinates are equal to zero, so we have: $q_1^j\mu_1 + \ldots + q_n^j\mu_n = 0$.

However, all q_i^j are rational, and μ_i are linearly independent over $\mathbb{Q}$, so $q_i^j = 0$. Thus, $r_i = q_i^1 b_1 + \ldots + q_i^s b_s = 0 \cdot b_1 + \ldots + 0 \cdot b_s = 0$. □

Lemma. *$\mu_1, \ldots, \mu_n \in \mathbb{Z}^k$ are linearly independent over $\mathbb{Q}$ if and only if they are linearly independent over $\mathbb{Z}$.*

Proof. The left-to-right implication is again obvious. Conversely, let $q_1\mu_1 + \ldots + q_n\mu_n = 0$ where $q_i \in \mathbb{Q}$. We choose the common denominator $q \in \mathbb{N} \setminus \{0\}$ for the fractions q_i. We denote the numerators by $p_i \in \mathbb{Z}$, that is, $q_i = p_i/q$.

Then $(p_1\mu_1 + \ldots + p_n\mu_n)/q = 0$, so $p_1\mu_1 + \ldots + p_n\mu_n = 0$. All p_i are integers, so using linear independence over $\mathbb{Z}$ we obtain that $p_1 = \ldots = p_n = 0$. Thus, $q_i = p_i/q = 0/q = 0$. □

Consequence. $\mu_1, \ldots, \mu_n \in \mathbb{Z}^k$ *are linearly independent over* $\mathbb{R}$ *if and only if they are linearly independent over* $\mathbb{Z}$.

Let us study in more detail the corollaries of linear independence over $\mathbb{R}/2\pi\mathbb{Z}$.

Proposition. $\mu_1, \ldots, \mu_n$ *are linearly independent over* $\mathbb{R}/2\pi\mathbb{Z}$ *if and only if they are linearly independent over* $\mathbb{R}/\mathbb{Z}$.

Proof. This follows from that the groups $\mathbb{R}/2\pi\mathbb{Z}$ and $\mathbb{R}/\mathbb{Z}$ are isomorphic. □

For a number $d \in \mathbb{Z}$ and a vector $x \in \mathbb{Z}^k$ we mean by $d \mid x$ that $d \mid x_i$ for all $1 \leqslant i \leqslant k$ or, equivalently, $d \mid \gcd(x_1, \ldots, x_n)$.

Lemma. *If* $\mu_1, \ldots, \mu_n$ *are linearly independent over* $\mathbb{R}/\mathbb{Z}$*, then:*

$$\forall d \in \mathbb{Z}\colon \forall x \in \mathbb{Z}^n\colon d \mid x_1\mu_1 + \ldots + x_n\mu_n \Rightarrow d \mid x.$$

Proof. Indeed, consider $q_i = x_i/d \in \mathbb{R}/\mathbb{Z}$. The divisibility of $x_1\mu_1 + \ldots + x_n\mu_n$ by d means that in $\mathbb{R}/\mathbb{Z}$ it holds that $(x_1\mu_1 + \ldots + x_n\mu_n)/d = 0$, i.e. $q_1\mu_1 + \ldots + q_n\mu_n = 0$. However, by virtue of linear independence, it is true that $q_1 = \ldots = q_n = 0$, but this means $d \mid x_i$ for all $1 \leqslant i \leqslant n$. □

A simple non-injectivity criterion follows immediately.

Lemma. *If* ϕ_α *is injective, then* $\forall j\colon \gcd(\alpha^j) = 1$.

Consequence. *If* $\exists j\colon \gcd(\alpha^j) \neq 1$*, then* ϕ_α *is not an injective mapping.*

Proof. Choosing $x_j = 1$ and $x_1 = \ldots = x_{j-1} = x_{j+1} = \ldots = x_k = 0$, we obtain that:

$$\begin{gathered}\forall d \in \mathbb{Z}\colon \forall x \in \mathbb{Z}^k\colon d \mid x_1\alpha^1 + \ldots + x_k\alpha^k \Rightarrow d \mid x \\ \Rightarrow \forall j\colon \forall d \in \mathbb{Z}\colon d \mid \alpha^j \Rightarrow d \mid 1 \Leftrightarrow \forall j\colon \gcd(\alpha^j) = 1.\end{gathered}$$ □

We denote the set of prime numbers by $\mathbb{P} \subseteq \mathbb{Z}$.

Lemma. *For arbitrary integer vectors* $\mu_1, \ldots, \mu_n$ *it is true that:*

$$\begin{gathered}\forall d \in \mathbb{Z}\colon \forall x \in \mathbb{Z}^n\colon d \mid x_1\mu_1 + \ldots + x_n\mu_n \Rightarrow d \mid x \\ \Leftrightarrow \forall p \in \mathbb{P}\colon \forall \beta \in \mathbb{N}\colon \forall x \in \mathbb{Z}^n\colon p^\beta \mid x_1\mu_1 + \ldots + x_n\mu_n \Rightarrow p^\beta \mid x \\ \Leftrightarrow \forall p \in \mathbb{P}\colon \forall x \in \mathbb{Z}^n\colon p \mid x_1\mu_1 + \ldots + x_n\mu_n \Rightarrow p \mid x.\end{gathered}$$

Proof. The left-to-right implications are obvious. Let us prove the right-to-left ones. Fix an arbitrary $d \in \mathbb{Z}$ and some vector $x \in \mathbb{Z}^k$. Factor d into prime numbers: $d = p_1^{\beta_1} \ldots p_m^{\beta_m}$.

Since $x_1\mu_1 + \ldots + x_n\mu_n$ is divisible by d, it is also divisible by every $p_i^{\beta_i}$. Using premise, we obtain that $p_i^{\beta_i} \mid x$ for all $1 \leqslant i \leqslant m$; but then $d = p_1^{\beta_1} \ldots p_m^{\beta_m} \mid x$ as required.

Next, fix a power $\beta \in \mathbb{N}$ and a prime number p. Since $x_1\mu_1 + \ldots + x_n\mu_n$ is divisible p^β, it is also divisible by p, so it follows from the premise that $p \mid x$.

But this means that x_i/p are integers, so $(x_1/p)\mu_1 + \ldots + (x_n/p)\mu_n$ is divisible by $p^{\beta-1}$. Applying the premise again, we obtain that $p \mid x/p$. Repeating this procedure β times, we finally conclude that $p \mid x/p^{\beta-1}$; but this is equivalent to $p^\beta \mid x$. □

The last condition can be rewritten as linear independence of vectors μ_i over the fields $\mathbb{Z}/p\mathbb{Z}$ for all primes p, which is equivalent to having the full rank for the matrix μ.

Consequence. *For arbitrary integer vectors $\mu_1, \ldots, \mu_n$ it is true that:*

$$\begin{aligned} &\forall d \in \mathbb{Z}\colon \forall x \in \mathbb{Z}^n\colon d \mid x_1\mu_1 + \ldots + x_n\mu_n \Rightarrow d \mid x \\ \Leftrightarrow\ &\forall p \in \mathbb{P}\colon \forall x \in (\mathbb{Z}/p\mathbb{Z})^n\colon x_1\mu_1 + \ldots + x_n\mu_n = 0 \Rightarrow x = 0 \\ \Leftrightarrow\ &\forall p \in \mathbb{P}\colon \operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(\mu) = \max(n,k). \end{aligned}$$

Finally, we can re-prove the already mentioned sufficient condition.

Consequence. *If ϕ_α is injective, then α_i span the whole lattice.*

Proof. Assume that α_i do not generate the lattice. Then the maximal minors of the matrix α have a common divisor $d > 1$.

Take some prime divisor p of the number d. Since the maximal minors are divisible by d, they are also divisible by p; therefore in the field $\mathbb{Z}/p\mathbb{Z}$ all maximal minors of α are equal to zero. So we have that $\operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(\alpha) < \max(n,k)$ [5], but this contradicts the corollary. □

This work is supported by the Krasnoyarsk Mathematical Center and financed by the Ministry of Science and Higher Education of the Russian Federation (Agreement no. 075-02-2024-1429).

References

[1] W.M.Schmidt, Heights of points on subvarieties of $\mathbb{G}_m^n$, London Mathematical Society Lecture Note Series, Issue 235: Number Theory. Séminaire de théorie des nombres de Paris 1993–94, 1996, 157–187.

[2] E.Artin, Galois Theory, London, University of Notre Dame, 1942, 1944.

[3] H.J.S.Smith, On systems of linear indeterminate equations and congruences. Philos, *Philosophical Transactions of the Royal Society*, **151**(1861), 293–326.

[4] T.M.Sadykov, A.K.Tsikh, Multivariate Hypergeometric and Algebraic Functions, Moscow, Nauka, 2014.

[5] N.Bourbaki, Algèbre: Chapitres 1 à 3. Éléments de mathématique, Berlin, Springer, 2006.

Алгебраические подгруппы комплексного тора

Николай А. Мишко
Сибирский федеральный университет
Красноярск, Российская Федерация

Аннотация. В работе изучаются мономиальные параметризации алгебраических подгрупп тора над произвольным полем и отдельно над полем комплексных чисел. Доказывается, что всякая мономиальная параметризация определяет алгебраическую группу. Получены необходимые и достаточные условия инъективности и существования такого рода параметризаций.

Ключевые слова: алгебраические подгруппы, мономиальная параметризация, комплексный алгебраический тор.