Torsion Points on an Algebraic Subset of an Affine Torus

Eriko Hironaka*

September 26, 1996

1 Introduction

Let $V \subset (\mathbb{C}^*)^r$ be an algebraic subset. Laurent has shown that the torsion points on V lie on a finite union of translates of affine subtori contained in V. It follows that the number, $p_V(n)$, of torsion points of order n on V is polynomial periodic. In this paper, we find formulas and bounds for the degree and period of $p_V(n)$ in terms of defining equations for V.

Counting torsion points on algebraic subsets of an affine torus is useful for studying abelian representations of a finitely presented group Γ. For example, the Alexander invariants define a stratification of the character variety for Γ, which naturally embeds in $(\mathbb{C}^*)^r$, and the first Betti number of unbranched coverings can be computed from the torsion points on these strata (cf. [A-S], [H]).

In [Lau], Laurent gives the following description of the set of torsion points $\mathrm{Tor}(V)$ on V.

Theorem 1 *(Laurent) For any algebraic subset V of $(\mathbb{C}^*)^r$ there is a finite set of rational planes $Q_1, .., Q_\ell \subset V$ such that*

$$\mathrm{Tor}(V) = \bigcup_{i=1}^{\ell} \mathrm{Tor}(Q_i).$$

Here, a *rational plane* $Q \subset (\mathbb{C}^*)^r$ is a subset of the form ηP, where $P \subset (\mathbb{C}^*)^r$ is an *affine subtorus*, or connected algebraic subgroup, and $\eta \in (\mathbb{C}^*)^r$ is an element of finite order. Laurent's result extends further than the statement we give here and settles a more general conjecture of Lang ([Lan], p.220).

It follows from Theorem 1 (cf. [A-S]) that $p_V(n)$ is a *polynomial periodic* function in n, that is, there exist periodic functions $a_0(n), \dots, a_d(n)$ such that

$$p_V(n) = a_0(n) + a_1(n)n + \dots + a_d(n)n^d.$$

*Research partially supported by N.S.E.R.C. grant OGP0170260

For, by Theorem 1, the Zariski closure of V has a decomposition into a finite union of rational planes

$$\overline{\mathrm{Tor}(V)}^{\mathrm{Zar}} = Q_1 \cup \ldots \cup Q_\ell$$

and hence $p_V(n)$ is given by the following formula

$$p_V(n) = \sum_{k=1}^{\ell} \sum_{1 \le i_1 < \ldots < i_k \le \ell} (-1)^{\ell-k} p_{Q_{i_1} \cap \ldots \cap Q_{i_k}}(n). \tag{1}$$

It is not hard to see that a finite intersection of rational planes is a finite union of disjoint rational planes (see Proposition 3.6 for a more precise description). Furthermore, the number of n-torsion points on a rational plane Q is given by

$$p_Q(n) \quad = \quad \begin{cases} n^{\dim(Q)} & \text{if } \mathrm{ord}(Q) \mid n, \\ 0 & \text{otherwise,} \end{cases}$$

where $\mathrm{ord}(Q)$ is the least integer n such that Q^n contains the identity element of $(\mathbb{C}^*)^r$.

We will concentrate on finding the degree and period of p_V. The *degree* of p_V, written $\deg(p_V)$, is the largest d such that $a_d(n)$ is not identically zero and the *period* of p_V, written $\mathrm{per}(p_V)$, is the least common multiple of the periods of $a_0(n), \ldots, a_d(n)$. Thus, for example, if $Q \subset (\mathbb{C}^*)^r$ is a rational plane, then $\mathrm{ord}(Q) = \mathrm{per}(p_Q)$. As with ordinary polynomials the degree of p_V determines the order of growth of $p_V(n)$: if $\deg(p_V) = d$, then

$$p_V(n) = O(n^d)$$

and for some fixed integer c

$$p_V(n) \asymp n^d$$

for all $n \equiv c \pmod{\mathrm{per}(p_V)}$.

If $\overline{\mathrm{Tor}(V)}^{\mathrm{Zar}} = Q_1 \cup \ldots \cup Q_\ell$, where $Q_1, \ldots, Q_\ell$ are rational planes, then (1) implies that

(i) $\deg(p_V) = \max\,\{\dim(Q_i) : i = 1, \ldots, \ell\}$,

(ii) $\mathrm{per}(p_V)$ divides the least common multiple of $\mathrm{ord}(Q)$ where Q ranges among connected components of

$$Q_{i_1} \cap \ldots \cap Q_{i_k}, \quad 1 \le i_1 < \ldots < i_k \le \ell.$$

In section 2, Theorem 2, we give bounds for $\deg(p_V)$ and $\mathrm{per}(p_V)$, when V is defined over $\mathbb{Q}$. More precise formulas for $\deg(p_V)$ and $\mathrm{per}(p_V)$, for general V, are obtained later in section 5 after developing notation and theory in sections 3 and 4.

The main ingredients of Laurent's proof of Theorem 1 can be stated as follows. Given an algebraic subset $V \subset (\mathbb{C}^*)^r$, one defines a finite set Π of mappings,

$$\phi : (\mathbb{C}^*)^r \to \Gamma_\phi, \qquad \phi \in \Pi$$

to algebraic groups Γ_ϕ. These mappings have the following properties.

(A) All the fibers of ϕ are finite unions of rational planes; and

(B)

$$\mathrm{Tor}(V) = \bigcup_{\phi \in \Pi} \phi^{-1}(\mathcal{S}_\phi),$$

where $\mathcal{S}_\phi \subset \Gamma_\phi$ are finite subsets.

We will go further in this paper by finding the fibers in (A) and the sets S_ϕ in (B) explicitly in terms of defining equations for V and relating them to the degree and period of p_V.

Techniques for finding the fibers in (A) are given in section 3, where we develop some tools for studying rational planes and give properties of monomial mappings. Our approach is to focus on the relationship between algebraic subgroups of $(\mathbb{C}^*)^r$ and subgroups of $\mathbb{Z}^r$. We use this correspondence to describe the rational planes in fibers of monomial mappings (see Lemma 3.4 and Corollary 3.5) and, as a consequence, in the intersection of a finite set of rational planes (see Proposition 3.6).

In many natural applications, for example, the Alexander strata mentioned above, the algebraic subsets V are defined over $\mathbb{Q}$, so we will concentrate on this case. Then, the sets S_ϕ in (B) are related to formal $\mathbb{Q}$-linear combinations of roots of unity. In section 4, we review some of the theory of $\mathbb{Q}$-linear relations among roots of unity developed by Schoenberg. The main idea is to view formal $\mathbb{Q}$-linear relations as convex polygons with rational sides and angles. Schoenberg shows in [S] that all the convex polygons can be obtained from regular p-gons, where p ranges over prime numbers. We describe these ideas in section 4 and include proofs of Mann's bound on the order of roots of unity satisying a linear equation of a given length (see Proposition 4.3) and of Schoenberg's result (see Corollary 4.4).

The results in sections 3 and 4 are used in section 5 to find the rational planes in an algebraic subset $V \subset (\mathbb{C}^*)^r$ (see Proposition 5.2) and to give formulas for $\deg(p_V)$ and bounds on $\mathrm{per}(p_V)$ (see Proposition 5.3 and Theorem 3) in terms of defining equations for V.

In section 6 we conclude with some illustrative examples. For instance, we find p_V when V is the Fermat curve

$$x^m + y^m = 1, \qquad m \geq 1$$

see Example 3. In this case, the bounds for the degree and period of p_V given in Theorem 2 are attained.

Acknowledgement. I gives me pleasure to thank E. Jahangard for useful discussions during the research for this paper.

2 Notation and main result

In this section we will set up some notation to state our main result, Theorem 2. This theorem gives bounds on the degree and period of p_V rather than exact formulas for them and applies to varieties V defined over $\mathbb{Q}$. A more general result, Theorem 3, is stated and proved in section 5, but the bounds in Theorem 2 are easier to state and to compute.

Notation. Let $\Lambda_r = \mathbb{C}[t_1, \ldots, t_r]$ denote the ring of Laurent polynomials. A monomial $t_1^{\lambda_1} \ldots t_r^{\lambda_r} \in \Lambda_r$ will be written as t^λ where $\lambda = (\lambda_1, \ldots, \lambda_r)$. Thus, coordinate functions $t_1, \ldots, t_r$ and the usual basis for $\mathbb{Z}^r$ determine a canonical isomorphism between Λ_r and $\mathbb{C}[\mathbb{Z}^r]$.

A Laurent polynomial $f \in \Lambda_r = \mathbb{C}[t_1^{\pm 1}, \ldots, t_r^{\pm 1}]$ will be written as

$$f(t) = \sum_{\lambda \in \mathcal{L}(f)} a_\lambda t^\lambda,$$

where $\mathcal{L}(f) \subset \mathbb{Z}^r$ is a finite subset and $a_\lambda \in \mathbb{C}^*$.

For a finite subset $\mathcal{F} \subset \Lambda_r$, our main theorem will describe the rational planes in the zero set $V(\mathcal{F})$ and bounds for the degree and period of $p_{V(\mathcal{F})}$ in terms of the functions in $\mathcal{F}$. Two main ingredients will be numbers $N[R(\mathcal{F})]$ and $D(\mathcal{F})$ which can be computed from the number of coefficients of functions in $\mathcal{F}$ and certain subgroups of $\mathbb{Z}^r$ associated to the exponents of functions in $\mathcal{F}$.

Define

$$R(\mathcal{F}) = \max \{|\mathcal{L}(f)| : f \in \mathcal{F}\},$$

where $|\mathcal{L}(f)|$ denotes the number of elements in $\mathcal{L}(f)$. For any positive integer R, let $N[R]$ denote the product of primes less than or equal to R.

The number $D(\mathcal{F})$ takes longer to define. For any $f \in \Lambda_r$, let Π_f be the set of all partitions $\mathcal{P}$ of $\mathcal{L}(f)$ such that each $\nu \in \mathcal{P}$ has at least two elements and for any finite subset $\mathcal{F} = \{f_1, \ldots, f_\ell\} \in \Lambda_r$, let

$$\Pi_{\mathcal{F}} = \Pi_{f_1} \times \ldots \times \Pi_{f_\ell}.$$

For any partition $\mathcal{P} \in \Pi_f$, let $\varepsilon(\mathcal{P}, f) \subset \mathbb{Z}^r$ be the subgroup generated by

$$\{\lambda - \mu : \ \exists \nu \in \mathcal{P}, \ \lambda, \mu \in \nu\};$$

for any $\pi = (\mathcal{P}_1, \ldots, \mathcal{P}_k) \in \Pi_{\mathcal{F}}$, let $\varepsilon(\pi, \mathcal{F}) \subset \mathbb{Z}^r$ be the sum

$$\varepsilon(\mathcal{P}_1, f_1) + \ldots + \varepsilon(\mathcal{P}_k, f_k);$$

and for any subset $\mathcal{U} \subset \Pi_{\mathcal{F}}$, let $\varepsilon(\mathcal{U}, \mathcal{F}) \subset \mathbb{Z}^r$ be the subgroup generated by

$$\bigcup_{\pi \in \mathcal{U}} \varepsilon(\pi, \mathcal{F}).$$

For any subgroup $\epsilon \subset \mathbb{Z}^r$, define

$$\overline{\epsilon} = \{\lambda \in \mathbb{Z}^r : n\lambda \in \epsilon, \text{ for some } n \in \mathbb{N}\}.$$

For any finite abelian group G, let $D(G)$ be the largest order of any element in G. Define

$$D(\mathcal{U}, \mathcal{F}) = D(\overline{\varepsilon(\mathcal{U}, \mathcal{F})}/\varepsilon(\mathcal{U}, \mathcal{F}))$$

and

$$D(\mathcal{F}) = \text{lcm } \{D(\mathcal{U}, \mathcal{F}) : \mathcal{U} \subset \Pi_{\mathcal{F}}\}.$$

Our main result is the following.

Theorem 2 *Let $V = V(\mathcal{F}) \subset (\mathbb{C}^*)^r$ be any algebraic subset defined over $\mathbb{Q}$.*

(i) For each maximal rational plane Q in V, there is a $\pi \in \Pi_{\mathcal{F}}$ so that Q is a translate of the affine subtorus of $(\mathbb{C}^*)^r$ defined by the set of binomials

$$\{t^\lambda - 1 : \lambda \in \overline{\varepsilon(\pi, \mathcal{F})}\};$$

(ii)

$$\deg(p_V) \leq r - \min_{\pi \in \Pi_{\mathcal{F}}} \operatorname{rank}(\overline{\varepsilon(\pi, \mathcal{F})});$$

(iii)

$$\operatorname{per}(p_V) \quad | \quad N[R(\mathcal{F})]\ D(\mathcal{F}).$$

This theorem together with finer versions will be proved in section 5.

3 Character groups and rational planes

The main tool we use in this paper is a natural correspondence between between affine subtori of $(\mathbb{C}^*)^r$ and subgroups of $\mathbb{Z}^r$. The relation is explained in section 3.1 and applied in section 3.2 to give properties of rational planes.

3.1 Subgroups of $\mathbb{Z}^r$ and algebraic subgroups of $(\mathbb{C}^*)^r$.

For any subgroup $\varepsilon \subset \mathbb{Z}^r$, let $V(\varepsilon)$ be the closed points of $\operatorname{Spec}(\mathbb{C}[\mathbb{Z}^r/\varepsilon])$. Then, there is a natural identification of $V(\varepsilon)$ with the group of characters of $\mathbb{Z}^r/\varepsilon$, since any closed point corresponds to a ring epimorphism $\mathbb{C}[\mathbb{Z}^r/\varepsilon] \to \mathbb{C}$. Define $I_\varepsilon \subset \Lambda_r$ to be the ideal generated by

$$\{t^\lambda - 1 : \lambda \in \varepsilon\}.$$

Then the kernel of the map $\mathbb{C}[\mathbb{Z}^r] \to \mathbb{C}[\mathbb{Z}^r/\varepsilon]$ is the image of I_ε in $\mathbb{C}[\mathbb{Z}^r]$ under the identification $\Lambda_r \cong \mathbb{C}[\mathbb{Z}^r]$. Thus, there is a natural embedding of $V(\varepsilon)$ into $(\mathbb{C}^*)^r$ with $V(\varepsilon) = V(I_\varepsilon)$ and $I_\varepsilon = I(V(\varepsilon))$. This embedding preserves group structure as well as the algebraic structure of $V(\varepsilon)$.

For any algebraic subset $V \subset (\mathbb{C}^*)^r$, define

$$\varepsilon(V) = \{\lambda \in \mathbb{Z}^r : t^\lambda - 1 \text{ vanishes on } V\}.$$

Lemma 3.1 *If $\varepsilon \subset \mathbb{Z}^r$ is any subgroup, then $\varepsilon(V(\varepsilon)) = \varepsilon$.*

Proof. Observe that for any subgroup $\varepsilon \subset \mathbb{Z}^r$, if $t^\lambda - 1 \in I_\varepsilon$, then λ must be a sum of elements in ε. This gives the inclusion $\varepsilon(V(\varepsilon)) \subset \varepsilon$. The other inclusion is clear.

■

Lemma 3.2 *Any subtorus P of $(\mathbb{C}^*)^r$ is of the form $V(\varepsilon)$ for some $\varepsilon \subset \mathbb{Z}^r$.*

Proof. Since P is itself isomorphic to $(\mathbb{C}^*)^s$ for some $0 \leq s \leq r$, the embedding $\psi : P \to (\mathbb{C}^*)^r$ defines a ring epimorphism on coordinate rings

$$\psi^* : \mathbb{C}[\mathbb{Z}^r] \to \mathbb{C}[\mathbb{Z}^s].$$

We will show that ψ^* restricted to $\mathbb{Z}^r$ induces an epimorphism $\mathbb{Z}^r \to \mathbb{Z}^s$. This is the same as saying that the components of ψ are monomials. Since ψ preserves multiplication it also preserves the multiplication of $(\mathbb{C}^*)$. Thus, the components of ψ must be homogeneous. Furthermore, since the components of ψ can have no zeros or poles other than the origin, they must be monomials.

Let $\varepsilon \subset \mathbb{Z}^r$ be the kernel of the epimorphism $\mathbb{Z}^r \to \mathbb{Z}^s$ induced by ψ. Then, the kernel of ψ^* is I_ε, so $P = V(\varepsilon)$.

■

.

Remark. Another way to say the above is that there is a naturally duality between algebraic subgroups of $(\mathbb{C}^*)^r$ and quotient groups of $\mathbb{Z}^r$ given by the contravariant functors $\mathrm{Hom}_{\mathcal{A}}(-, \mathbb{C}^*)$ and $\mathrm{Hom}(-, \mathbb{C}^*)$, where $\mathrm{Hom}_{\mathcal{A}}(V, W)$ is the ring of morphisms between algebraic subgroups V, W of $(\mathbb{C}^*)^r$ which preserve both the algebraic and multiplicative structure. For brevity and because they are not necessary for the results of this paper, we omit the details.

3.2 Rational planes and monomial mappings.

Given a subgroup $\varepsilon \subset \mathbb{Z}^r$, let $\overline{\varepsilon}$ be the subgroup of $\mathbb{Z}^r$ defined by

$$\overline{\varepsilon} = \{\lambda \in \mathbb{Z}^r : \exists n \in \mathbb{N},\ n\lambda \in \varepsilon\}.$$

For any subgroup $\varepsilon \subset \mathbb{Z}^r$ and $m \in \mathbb{N}$, let

$$\varepsilon_m = \{\lambda \in \mathbb{Z}^r : m\lambda \in \varepsilon\}.$$

Lemma 3.3 *For any subgroup $\varepsilon \in \mathbb{Z}^r$, $V(\overline{\varepsilon})$ is an affine subtorus of $(\mathbb{C}^*)^r$. Furthermore, there is an injective (non-canonical) endomorphism*

$$T : \widehat{\overline{\varepsilon}/\varepsilon} \hookrightarrow (\mathbb{C}^*)^r,$$

from the character group $\widehat{\overline{\varepsilon}/\varepsilon}$ into $(\mathbb{C}^*)^r$, such that $V(\varepsilon)$ decomposes as a disjoint union

$$V(\varepsilon) = \bigcup_{\eta \in T(\widehat{\overline{\varepsilon}/\varepsilon})} \eta V(\overline{\varepsilon}).$$

Proof. The epimorphisms

$$\mathbb{Z}^r \to \mathbb{Z}^r/\varepsilon \longrightarrow \mathbb{Z}^r/\overline{\varepsilon}$$

induce inclusions

$$V(\overline{\varepsilon}) \hookrightarrow V(\varepsilon) \hookrightarrow (\mathbb{C}^*)^r.$$

Since $\mathbb{Z}^r/\overline{\varepsilon}$ is a free abelian group, $V(\overline{\varepsilon})$ is an affine subtorus of $(\mathbb{C}^*)^r$.

The inclusion $\overline{\varepsilon}/\varepsilon \hookrightarrow \mathbb{Z}^r/\varepsilon$ induces a surjective map on character groups

$$\psi : V(\varepsilon) \to \widehat{\overline{\varepsilon}/\varepsilon}$$

whose identity fiber F_1 equals $V(\overline{\varepsilon})$.

We need to find a splitting for ψ. Write $\mathbb{Z}^r/\varepsilon$ as the product

$$\mathbb{Z}^r/\varepsilon = \mathbb{Z}^s \times G,$$

where G is finite. Then $G \cong \overline{\varepsilon}/\varepsilon$ and $\mathbb{Z}^s \cong \mathbb{Z}^r/\overline{\varepsilon}$. Thus, there is a surjection $\mathbb{Z}^r/\varepsilon \to \overline{\varepsilon}/\varepsilon$ whose restriction to $\overline{\varepsilon}/\varepsilon$ is the identity. Let $T : \widehat{\overline{\varepsilon}/\varepsilon} \to V(\varepsilon)$ be the induced endomorphism of character groups. Then T defines a splitting for ψ and we are done.

$\blacksquare$

Notation. A map

$$\psi : \widehat{H} \to \widehat{G}$$

between character groups which is induced by a homomorphism $\psi^* : G \to H$ is called a *monomial mapping*, since the induced map on coordinate rings is just the linear extension of ψ^* to a mapping $\mathbb{C}[G] \to \mathbb{C}[H]$.

Given a monomial mapping $\psi : (\mathbb{C}^*)^r \to \widehat{G}$, let $\varepsilon(\psi) \subset \mathbb{Z}^r$ be the image of the induced map

$$\psi^* : G \to \mathbb{Z}^r.$$

Lemma 3.4 *Let $\psi : (\mathbb{C}^*)^r \to \widehat{G}$ be a monomial map and set $\varepsilon = \varepsilon(\psi)$. For each $\mu \in$ $\mathrm{Tor}(\mathrm{im}(\psi))$, there is a $\tau \in \overline{\varepsilon}/\varepsilon$ such that, for some $\eta \in (\mathbb{C}^*)^r$ with $\mathrm{ord}(\eta) = \mathrm{ord}(\mu)\mathrm{ord}(\tau)$,*

$$\psi^{-1}(\mu) = \eta V(\varepsilon).$$

Proof. If $m = \mathrm{ord}(\mu)$, then the fiber $\psi^{-1}(\mu)^m$ lies in the identity fiber $V(\varepsilon)$. Furthermore, if $\eta \in \psi^{-1}(\mu)$ has finite order, then m divides $\mathrm{ord}(\eta)$.

We have $V(\varepsilon)^m = V(\varepsilon_m)$, so by Lemma 3.3,

$$V(\varepsilon_m) = \bigcup_{\gamma \in T(\overline{\varepsilon}/\varepsilon_m)} \gamma V(\overline{\varepsilon}).$$

Thus, for any $\eta \in \psi^{-1}(\mu)$,

$$\psi^{-1}(\mu)^m = \eta^m V(\varepsilon)^m = \eta^m V(\varepsilon_m)$$

and $\psi^{-1}(\mu)^m$ is a translate of $V(\varepsilon_m)$ in $V(\varepsilon)$. Thus, $\psi^{-1}(\mu)^m$ must contain an element of $T(V(\overline{\varepsilon}/\varepsilon))$.

This means we could have chosen $\eta \in \psi^{-1}(\mu)$ such that $\eta^m \in T(V(\overline{\varepsilon}/\varepsilon))$. If $\varepsilon_m = \varepsilon$, then $V(\varepsilon)^m = V(\varepsilon)$ and we could have chosen η so that $\eta^m = 1$, which would imply $\mathrm{ord}(\eta) = m$. Otherwise, set $\tau = \eta^m$. We will show that $\mathrm{ord}(\eta) = \mathrm{ord}(\tau)m$. We've seen that m divides $\mathrm{ord}(\eta)$. If $k = \mathrm{ord}(\eta)/m$, then $\tau^k = \eta^{mk} = 1$, so $\mathrm{ord}(\tau)$ divides k. Since $\eta^{\mathrm{ord}(\tau)m} = \tau^{\mathrm{ord}(\tau)} = 1$, we have $\mathrm{ord}(\eta) = \mathrm{ord}(\tau)m$.

■

Corollary 3.5 *Let $\psi : (\mathbb{C}^*)^r \to \widehat{G}$ be a monomial map and let $\varepsilon = \varepsilon(\psi)$. Then, for any $\mu \in \mathrm{im}(\psi)$ and connected component $Q \subset \psi^{-1}(\mu)$, we have*

(i) Q is a translate of $V(\overline{\varepsilon})$,

(ii) $\dim(Q) = r - \mathrm{rank}(\overline{\varepsilon})$, and

(iii) if μ has finite order, then

$$\mathrm{ord}(\mu) \mid \mathrm{ord}(Q) \mid \mathrm{ord}(\mu) D(\overline{\varepsilon}/\varepsilon),$$

where $D(\overline{\varepsilon}/\varepsilon)$ is the largest order of any element of $\overline{\varepsilon}/\varepsilon$.

We will now describe the dimensions and orders of intersections of rational planes.

Proposition 3.6 *Let $\varepsilon_1, \ldots, \varepsilon_k \subset \mathbb{Z}^r$ be any subgroups of $\mathbb{Z}^r$ and let $\eta_1, \ldots, \eta_k \in \mathrm{Tor}((\mathbb{C}^*)^r)$. Let $Q_1, \ldots, Q_k \subset (\mathbb{C}^*)^r$ be defined by*

$$Q_i = \eta_i V(\varepsilon_i), \qquad i = 1, \ldots, k.$$

Let $\varepsilon = \varepsilon_1 + \ldots + \varepsilon_k$ and $\eta = (\eta_1, \ldots, \eta_k)$. Let

$$\begin{array}{rcl} \rho : \varepsilon_1 \times \ldots \times \varepsilon_k & \to & \varepsilon \\ (\lambda_1, \ldots, \lambda_k) & \mapsto & \lambda_1 + \ldots + \lambda_k \end{array}$$

and let $\gamma : \varepsilon_1 \times \ldots \times \varepsilon_k \to (\mathbb{Z}^r)^k$ be the inclusion map. Then $Q_1 \cap \ldots \cap Q_k$ is nonempty if and only if $\gamma^*(\eta) \in \mathrm{im}(\rho^*)$ and for any connected component $Q \subset Q_1 \cap \ldots \cap Q_k$, we have

(i) Q is a translate of $V(\overline{\varepsilon})$,

(ii) $\dim(Q) = r - \mathrm{rank}(\overline{\varepsilon})$, and

(iii) if η has finite order, then

$$\mathrm{ord}(\eta) \mid \mathrm{ord}(Q) \mid \mathrm{ord}(\eta) D(\overline{\varepsilon}/\varepsilon).$$

Proof. Consider the commutative diagram

$$\begin{array}{ccc}
\mathbb{Z}^r/\varepsilon & \leftarrow & \mathbb{Z}^r/\varepsilon_1 \times \ldots \times \mathbb{Z}^r/\varepsilon_k \\
\uparrow & & \uparrow \\
\mathbb{Z}^r & \leftarrow & \mathbb{Z}^r \times \ldots \times \mathbb{Z}^r \\
\uparrow & & \uparrow \\
\varepsilon & \leftarrow & \varepsilon_1 \times \ldots \times \varepsilon_r
\end{array}$$

where the horizontal arrows are given by adding coordinates, the bottom vertical arrows are inclusions and the top vertical arrow are quotient maps. For $i = 1, \ldots, k$, let $P_i = V(\varepsilon_i)$. Then we have a commutative diagram of induced maps on the associated algebraic sets:

$$\begin{array}{ccc}
V(\varepsilon) & \longrightarrow & P_1 \times \ldots \times P_k \\
\downarrow & & \downarrow \\
(\mathbb{C}^*)^r & \xrightarrow{\alpha} & (\mathbb{C}^*)^r \times \ldots \times (\mathbb{C}^*)^r \\
\downarrow \beta & & \downarrow \gamma^* \\
\widehat{\varepsilon} & \xrightarrow{\rho^*} & \widehat{\varepsilon_1} \times \ldots \times \widehat{\varepsilon_k}.
\end{array}$$

The preimage $\alpha^{-1}(Q_1 \times \ldots \times Q_k)$ equals the intersection $Q_1 \cap \ldots \cap Q_k$. If $Q \subset Q_1 \cap \ldots \cap Q_k$ is a connected component, then it is a connected component of a fiber of β. The intersection is nonempty if and only if

$$\gamma^*(Q_1 \times \ldots \times Q_k) \cap \mathrm{im}(\rho^*) \neq \emptyset.$$

The claim now follows from Corollary 3.5.

$\blacksquare$

4 Formal $\mathbb{Q}$-linear relations

In this section, we describe $\mathbb{Q}$-linear relations between roots of unity and polar rational polygons following the work of Schoenberg [S] and Mann [M]. The aim is to give a constructive method for producing all $\mathbb{Q}$-linear relations and give a bound on the orders of roots of unity satisfying a linear equation in terms of the number of coefficients of the equation. Other work in this area can be found in [Le] and [C-J].

For any $n \in N$, let $\zeta_n = \exp(2\pi\sqrt{-1}/n)$. For $z \in \mathbb{C}^*$, let $\theta(z) = \arg(z)/2\pi$. Thus,

$$z = |z| \exp(2\pi\sqrt{-1}\ \theta(z)).$$

A *polar rational polygon*, or prp, is an oriented polygon in the complex plane with no parallel edges, such that each edge is a vector with rational length and with angle equal to a rational multiple of 2π.

Then prp's can be put into one-to-one correspondence with formal $\mathbb{Q}$-linear relations of the form

$$\sum_{i=1}^{k} a_i \epsilon_i = 0. \tag{2}$$

where $a_i \in \mathbb{Q}^*$ and

$$0 \leq \theta(\mathrm{sign}(a_1)\epsilon_1) < \ldots < \theta(\mathrm{sign}(a_k)\epsilon_k) < 1.$$

Given a prp T defined by (2), we will call $a_i\epsilon_i$ the sides of T, $|a_i|$ the *side lengths* and ϵ_i the *side angles.*

The *order* of T, written $\mathrm{ord}(T)$, is the least n such that, for some root of unity η, we have

$$\eta^n \epsilon^n = 1,$$

for all side angles ϵ of T. The length of T, written $\mathrm{len}(T)$ is k, the number of sides.

Any formal $\mathbb{Q}$-linear equation

$$\sum_{j=1}^{k} b_j \eta_j$$

can be put in the form (2) by the following:

(i) if $\theta(\eta_j) \pmod 1 \geq 1/2$, then replace a_j by $-a_j$ and η_j by $\zeta_2\eta_j$;

(ii) if $\theta(\eta_j) = \theta(\eta_\ell)$, then replace $b_j\eta_j + b_\ell\eta_\ell$ by $(b_j + b_\ell)\eta_j$;

(iii) remove any summand whose coefficient is zero; and

(iv) reorder the summands.

It is easy to see that to any formal $\mathbb{Q}$-linear equation there is a unique corresponding equation of the form (2), which can be obtained using the above steps, and hence a unique prp.

It follows that the set of prp's forms a commutative $\mathbb{Q}[\mathrm{Tor}(\mathbb{C}^*)]$-algebra, where $\mathrm{Tor}(\mathbb{C}^*)$ is the set of roots of unity. One just notes that formal $\mathbb{Q}$-linear equations are closed under addition, multiplication and scalar multiplication by elements of $\mathrm{Tor}(\mathbb{C}^*)$. The algebra operations on a prp will be the same as those for the corresponding formal $\mathbb{Q}$-linear equation. The resulting $\mathbb{Q}$-linear equation may not be of the form (2), but there is a unique prp associated to it which we take as the result of the operation.

The algebra operations have the following geometric interpretations. Multiplication by a positive rational $a \in \mathbb{Q}_+$ scales the corresponding polygon by a. Multiplication by any root of unity $\eta \in \mathrm{Tor}(\mathbb{C}^*)$ rotates the polygon by the argument of η. For example, multiplying the polygon in figure 1 by $\eta = -1$ yields the polygon rotated by 180 degrees shown in figure 2.

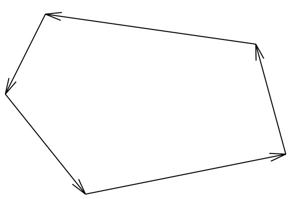

figure 1

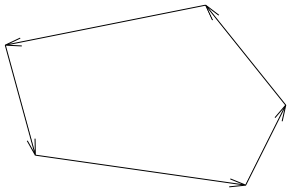

figure 2

Summing is like taking the union except that one needs to reorder the sides and get rid of redundancies.

Two prp's will be said to be *disjoint* if they do not share any sides angles. A prp T is *primitive* if there are no disjoint prp's S and U such that $T = S + U$. Geometrically, a prp is primitive if there is no way to rearrange the edges of the polygon to get a union of polygons joined at vertices. While any prp has a decomposition into a sum of disjoint primitives, this decomposition is not necessarily unique.

For example, consider the $\mathbb{Q}$-linear equation given by expanding out

$$(1 + \zeta_3 + \zeta_3^2)(1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4) = 0. \tag{3}$$

The associated prp is given in figure 3.

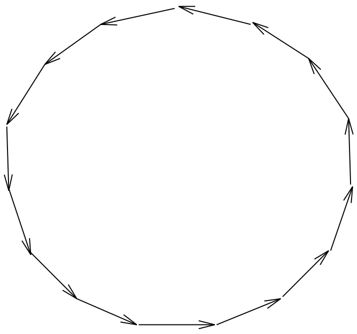

figure 3

The prp defined by (3) can be decomposed into primitive prp's as in figure 4 and figure 5.

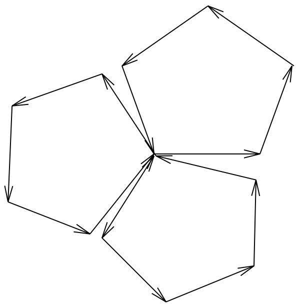

figure 4

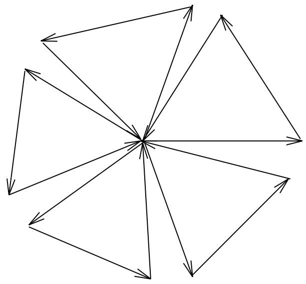

figure 5

The decomposition in figure 4 comes from writing (3) as

$$\sum_{i=1}^{2} \zeta_3^i \, [1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4] = 0$$

and figure 5 comes from writing (3) as

$$\sum_{i=1}^{4} \zeta_5^i \, [1 + \zeta_3 + \zeta_3^2] = 0.$$

The sum of nondisjoint prp's could have smaller length than the sum of the total as we see in the next example. Let A be the prp defined by

$$\zeta_6 + \zeta_6^2 + (-1) = 0$$

and T_5 is the prp defined by

$$1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0.$$

Then $\zeta_5 \, A + T_5$ is the prp (see figure 6) given by the following $\mathbb{Q}$-linear equation

$$1 + (\zeta_6 + \zeta_6^5)\zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$$

or

$$1 + \zeta_{30} + \zeta_{30}^{11} + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0.$$

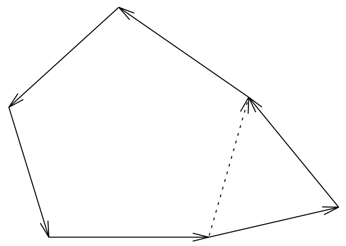

figure 6

In general we have the following.

Lemma 4.1 *The lengths of sums satisfies the following inequalities*

$$\max \{\mathrm{len}(T_1), \mathrm{len}(T_2)\} \leq \mathrm{len}(T_1 + T_2) \leq \mathrm{len}(T_1) + \mathrm{len}(T_2),$$

with equality on the right hand side if T_1 and T_2 are disjoint and equality on the left hand side if the set of side angles of one prp is contained in the other's.

We will make use of the following types of prp's. For any prime p, let $\sigma_p(x)$ be the cyclotomic polynomial

$$\sigma_p(x) = 1 + x + \ldots + x^{p-1}.$$

Let T_p be the prp defined by $\sigma_p(\zeta_p) = 0$.

Let $n = mp$, where p is a prime not dividing m. (For example, if n is prime then $m = 1$.) Then the minimal polynomial $\sigma_{n,p}$ for ζ_n over $\mathbb{Q}[\zeta_m]$ is given by

$$\sigma_{n,p}(x) = \zeta_m^{a(p-1)} + \zeta_m^{a(p-2)} x + \ldots + x^{p-1},$$

where a is the integer $0 \leq a < m$, such that $ap \equiv 1 \pmod{m}$. Let $T_{n,p}$ be the prp defined by $\sigma_{n,p}(\zeta_n) = 0$. That is, the prp corresponding to the formal $\mathbb{Q}$-linear relation

$$\sum_{i=0}^{p-1} \zeta_n^{ap(p-1-i)+i} = 0.$$

Lemma 4.2 *Let n be an integer, p a prime dividing n, such that p^2 doesn't divide n. The prp $T_{n,p}$ is a multiple of T_p by some element of $\mathbb{Q}[\mathrm{Tor}(\mathbb{C}^*)]$.*

Proof. Let $m = n/p$ and let a be such that $ap \equiv 1 \pmod{m}$. Let r be any integer such that $ap = 1 + mr$. Then, since $\zeta_n^m = \zeta_p$, we have

$$\begin{aligned} \zeta_n^{ap(p-1-i)+i} &= \zeta_n^{mr(p-1-i)+(p-1)} \\ &= \zeta_p^{r(p-1-i)} \zeta_n^{p-1}. \end{aligned}$$

Thus, $T_{n,p}$ is defined by the formal linear relation

$$\zeta_n^{p-1} \sum_{i=0}^{p-1} \zeta_p^{r(p-1-i)} = 0.$$

Since p doesn't divide r, $r(p-1-i)$ ranges in $0, \ldots, p-1$ as i ranges in $0, \ldots, p-1$. Therefore,

$$T_{n,p} = \zeta_n^{p-1} T_p.$$

■

Our proof of the following result uses essentially the same ideas as Mann uses in ([M], Theorem 1), except that we take more advantage of the structure of prp's as a $\mathbb{Q}[\mathrm{Tor}(\mathbb{C}^*)]$-algebra.

Proposition 4.3 *Let T be a primitive prp of length r and order n. Then we have*

(i) n is square free;

(ii) for any prime p dividing n, $p \leq r$;

(iii) for any prime p dividing n, T is a $\mathbb{Q}[\mathrm{Tor}(\mathbb{C}^*)]$-linear combination of $T_{n,p}$ and prp's of order n/p.

Proof. Let

$$\sum_{i=1}^{r} a_i \epsilon_i = 0 \tag{4}$$

be the $\mathbb{Q}$-linear relation corresponding to T of the form (2). If T has order n, then by multiplying T by an element of $\mathrm{Tor}(\mathbb{C}^*)$, if necessary, we can assume that all the ϵ_i in (4) have order n. We will show that n is square free and for any prime p dividing n, $p \leq r$.

Let p be a prime dividing n and let $m = n/p$. Since $\zeta_n^p = \zeta_m$, we can write

$$\epsilon_i = \eta_i \zeta_n^{\alpha_i},$$

for $i = 1, \ldots, r$, where $\eta_i \in \mathbb{Q}[\zeta_m]$ and $0 \leq \alpha_i \leq p-1$. Define

$$q_{T,n,p}(x) = \sum_{i=1}^{r} a_i \eta_i x^{\alpha_i}.$$

This is a polynomial with coefficients in $\mathbb{Q}[\zeta_m]$ satisfied by ζ_n and hence the minimal polynomial $\sigma_{n,p}(x)$ for ζ_n over $\mathbb{Q}[\zeta_m]$ divides $q_{T,n,p}(x)$. If p^2 divides n then $\deg(\sigma_{n,p}) = p$ which is strictly greater than the degree of $q_{T,n,p}(x)$, and hence $q_{T,n,p}(x)$ is identically zero. Since T is primitive, this means that all the α_i are the same, but then we can multiply T by ζ_p^{-1} to get a prp of order m which is a contradiction, since the order of a prp is preserved under multiplication by roots of unity.

Thus, n is square free (proving (i)) and $\sigma_{n,p}(x)$ divides $q_{T,n,p}(x)$. Set

$$A_\alpha = \sum_{\alpha_i = \alpha} a_i \eta_i$$

and write $q_{T,n,p}(x)$ as

$$q_{T,n,p}(x) = \sum_{\alpha=0}^{p-1} A_\alpha x^\alpha.$$

Since $q_{T,n,p}(x)$ is not identically zero and has degree less than or equal to $p-1$, we have

$$q_{T,n,p}(x) = B\sigma_{n,p}(x) \tag{5}$$

for some invertible $B \in \mathbb{Q}[\zeta_m]$.

By (5), evaluating $B^{-1}\ A_\alpha$ as a complex number gives the αth coefficient of $\sigma_{n,p}(x)$. Thus, the formal $\mathbb{Q}$-linear equation

$$B^{-1}\ A_\alpha - \zeta_m^{a(p-1-\alpha)} = 0$$

defines a prp, which we'll call T_α. Then T has the following decomposition into a sum of prp's

$$T = B\ \sum_{\alpha=0}^{p-1} T_\alpha + B\ T_{n,p}.$$

Since $\mathrm{ord}(T_\alpha) = m$, we have proved (iii).

By Lemma 4.1, $\mathrm{len}(T) \geq \mathrm{len}(T_{n,p}) = p$, so $p \leq r$ which proves (ii).

■

Proposition 4.3 leads to a geometric method for generating all prps as we see in the following result, originally proved by Schoenberg in [S].

Corollary 4.4 *The set of prp's, considered as a $\mathbb{Q}[\mathrm{Tor}(\mathbb{C}^*)]$-module, is generated by the set of T_p, where p ranges over all primes.*

Proof. By Lemma 4.2, $T_{n,p}$ is a multiple of T_p by an element of $\mathbb{Q}[\zeta_{n/p}]$. The rest follows from Proposition 4.3 and induction on the number of primes dividing n.

■

It follows that geometrically one can construct all prp's by starting with regular p-gons, for primes p, and doing the operations of rotation, stretching and "adding", where "adding" means taking the union of sides, grouping like side angles, getting rid of sides of zero length and reordering the sides, as described above.

5 Behavior of torsion points

We start in this section with a review of the proof of Theorem 1. Then, using the relation between finitely generated groups and rational planes developed in section 3, we study the degree and period of p_V. Finally, we give a proof of Theorem 2.

5.1 Proof of Theorem 1.

Let $V = V(f_1, \ldots, f_r) \subset (\mathbb{C}^*)^r$ be any algebraic subset. We want to find a finite number of rational planes $Q_1, \ldots, Q_\ell$ contained in V so that

$$\overline{Tor(V)}^{\mathrm{Zar}} = \bigcup_{i=1}^{\ell} Q_i.$$

Step 1. We can reduce to the case of hypersurfaces, since $V = V(f_1) \cap \ldots \cap V(f_r)$ and, by Proposition 3.6, a finite intersection of rational planes is a finite union of rational planes.

Step 2. Let $V = V(f)$, where $f \in \Lambda_r$ defined by

$$f = \sum_{\lambda \in \mathcal{L}(f)} a_\lambda t^\lambda, \quad a_\lambda \in \mathbb{C}^*,$$

for $\mathcal{L}(f) \subset \mathbb{Z}^r$ is a finite subset. We'll show that

$$\overline{\mathrm{Tor}(V)}^{\mathrm{Zar}} = \bigcup_{i=1}^{k} \psi_i^{-1}(S_i),$$

for some finite collection of monomial maps $\psi_i : (\mathbb{C}^*)^r \to \widehat{G_i}$, for some character groups $\widehat{G_i}$, and some finite sets of torsion elements $S_i \subset \mathrm{Tor}(\widehat{G_i})$. It then follows from Corollary 3.5 that $\overline{\mathrm{Tor}(V)}^{\mathrm{Zar}}$ is a finite union of rational planes.

Let $\mathcal{L} = \mathcal{L}(f)$ and let $\ell(f)$ be the linear polynomial

$$\ell(f) = \sum_{\lambda \in \mathcal{L}} a_\lambda x_\lambda$$

where x_λ are independent variables, for λ ranging in $\mathcal{L}$. Then

$$V(f) = \alpha_f^{-1}(V(\ell(f))),$$

where $\alpha_f : (\mathbb{C}^*)^r \to (\mathbb{C}^*)^{\mathcal{L}}$ is the monomial map induced by

$$\begin{array}{ccc} \mathbb{Z}^{\mathcal{L}} & \to & \mathbb{Z}^r \\ e_\lambda & \mapsto & \lambda. \end{array}$$

Step 3. Let Π_f be the set of partitions of $\mathcal{L}$, where for all $\nu \in \mathcal{P} \in \Pi_f$, ν has at least 2 elements. Fix $\mathcal{P} \in \Pi_f$. Let $L_{\mathcal{P}}$ be the system of linear equations

$$\ell_\nu(f) = \sum_{\lambda \in \nu} a_\lambda t_\lambda,$$

for each $\nu \in \mathcal{P}$. This defines a system of linear equations defined on

$$W(\mathcal{P}) = \prod_{\nu \in \mathcal{P}} (\mathbb{C}^*)^{\nu}.$$

Let $\mathcal{T}(\mathcal{P}, f)$ be the set of elements $(\epsilon_\lambda)_{\lambda \in \nu, \nu \in \mathcal{P}} \in W(\mathcal{P})$ satisfying the system $L_{\mathcal{P}}$:

$$\sum_{\lambda \in \nu} a_\lambda \varepsilon_\lambda = 0, \qquad \text{forall } \nu \in \mathcal{P}.$$

Then

$$V(\ell(f)) = \bigcup_{\mathcal{P} \in \Pi_f} \mathcal{T}(\mathcal{P}, f).$$

For each $\nu \in \mathcal{P}$, choose $\lambda_\nu \in \nu$ and let $\nu^* = \nu \setminus \{\lambda_\nu\}$. Define

$$W(\mathcal{P})^* = \prod_{\nu \in \mathcal{P}} (\mathbb{C}^*)^{\nu^*}.$$

Let

$$\beta_\nu : (\mathbb{C}^*)^{\nu} \to (\mathbb{C}^*)^{\nu^*}$$

be the map defined by

$$\begin{array}{ccc} \mathbb{Z}^{\nu^*} & \to & \mathbb{Z}^{\nu} \\ e_\lambda & \mapsto & e_\lambda - e_{\lambda_\nu}. \end{array}$$

Let

$$\beta_{\mathcal{P}} : W(\mathcal{P}) \to W(\mathcal{P})^*$$

be the product of the maps β_ν. Let $\mathcal{V}(\mathcal{P}, f)$ be the set of solutions $(\varepsilon_\lambda)_{\lambda \in \nu^*, \nu \in \mathcal{P}} \in W(\mathcal{P})^*$ to the inhomogeneous equations

$$\sum_{\lambda \in \nu^*} (-a_\lambda / a_{\lambda_\nu}) t_\lambda = 1, \qquad \nu \in \mathcal{P}.$$

Then $\mathcal{T}(\mathcal{P}, f) = \beta_{\mathcal{P}}^{-1}(\mathcal{V}(\mathcal{P}, f))$, so we have

$$V(f) = \bigcup_{\mathcal{P} \in \Pi_f} \alpha_f^{-1} \beta_{\mathcal{P}}^{-1}(\mathcal{V}(\mathcal{P}, f)). \tag{6}$$

Step 4. Let

$$\psi_{\mathcal{P},f} : (\mathbb{C}^*)^r \to W(\mathcal{P})^*$$

be the composition $\psi_{\mathcal{P},f} = \beta_{\mathcal{P}} \circ \alpha_f$. Then $\psi_{\mathcal{P},f}$ is induced by the maps

$$\begin{array}{cccl} \bigoplus_{\nu \in \mathcal{P}} \mathbb{Z}^{\nu^*} & \to & \mathbb{Z}^r & \\ e_\lambda & \mapsto & \lambda - \lambda_\nu & \text{if } \lambda \in \nu. \end{array}$$

Equation (6) now becomes

$$V(f) = \bigcup_{\mathcal{P} \in \Pi_f} \psi_{\mathcal{P},f}^{-1}(\mathcal{V}(\mathcal{P}, f)). \tag{7}$$

Since monomial maps take torsion points to torsion points, (7) implies

$$\overline{\mathrm{Tor}(V(f))}^{\mathrm{Zar}} = \bigcup_{\mathcal{P} \in \Pi_f} \psi_{\mathcal{P},f}^{-1}(\mathrm{Tor}(\mathcal{V}(\mathcal{P}, f)))$$

If $\mathcal{P}$ and $\mathcal{P}'$ are two elements in Π_f, $\mathcal{P}'$ is a *refinement* of $\mathcal{P}$ if for any $\nu' \in \mathcal{P}'$, there is a $\nu \in \mathcal{P}$ such that $\nu' \subset \nu$. A refinement $\mathcal{P}'$ of $\mathcal{P}$ is *proper* if $\mathcal{P}'$ is not equal to $\mathcal{P}$. If $\mathcal{P}'$ is a refinement of $\mathcal{P}$, then

$$\mathcal{V}(\mathcal{P}', f) \subset \mathcal{V}(\mathcal{P}, f).$$

Let $\mathcal{V}_m(\mathcal{P}, f)$ be the set of elements of $\mathcal{V}(\mathcal{P}, f)$ which are not in $\mathcal{V}(\mathcal{P}', f)$ for any proper refinement $\mathcal{P}'$ of $\mathcal{P}$. Let $S(\mathcal{P}, f) = \mathrm{Tor}(\mathcal{V}_m(\mathcal{P}, f))$. Then we have

$$\overline{\mathrm{Tor}(V(f))}^{\mathrm{Zar}} = \bigcup_{\mathcal{P} \in \Pi_f} \psi_{\mathcal{P},f}^{-1}(S(\mathcal{P}, f)). \tag{8}$$

Thus, the proof of Theorem 1 is completed by the following lemma.

Lemma 5.1 *(Laurent, Sarnak) The set $S(\mathcal{P}, f)$ is finite.*

This follows from ([Lau], Theorem 1) and ([A-S], Lemma 3.1).

■

When f is defined over $\mathbb{Q}$, Mann's Theorem (see Prop. 5.4) gives an explicit bound on the order of points in $S(\mathcal{P}, f))$. The rational planes inside a given algebraic subset of $(\mathbb{C}^*)^r$ can now be described in the following way.

Proposition 5.2 *Let $V \subset (\mathbb{C}^*)^r$ be any algebraic subset defined by Laurent polynomials $\mathcal{F} = \{f_1, \ldots, f_k\} \subset \Lambda_r$. Let $\Pi_{\mathcal{F}} = \Pi_{f_1} \times \ldots \times \Pi_{f_k}$. Then*

$$\overline{\mathrm{Tor}(V)}^{\mathrm{Zar}} = \bigcup_{\mathcal{P}_1 \times \ldots \times \mathcal{P}_k \in \Pi_{\mathcal{F}}} \bigcap_{i=1}^{k} \psi_{\mathcal{P}_i,f_i}^{-1}(S(\mathcal{P}_i, f)). \tag{9}$$

Proof. We have

$$\overline{\mathrm{Tor}(V)}^{\mathrm{Zar}} = \bigcap_{i=1}^{k} \overline{\mathrm{Tor}(V(f_i))}^{\mathrm{Zar}}$$

so the statement follows from (8).

■

5.2 Degree and Periodicity.

We will now give some results concerning the degree and period of p_V.

First let $f \in \Lambda_r$ be a Laurent polynomial. We will begin by studying the hypersurface $V(f) \subset (\mathbb{C}^*)^r$ defined by f. For a partition $\mathcal{P} \in \Pi_f$, define

$$\delta_{\mathcal{P},f} = \begin{cases} 1 & \text{if } S(\mathcal{P},f) \neq \emptyset, \\ 0 & \text{otherwise.} \end{cases}$$

For $\mathcal{P} \in \Pi_f$, let $\varepsilon(\mathcal{P},f) \subset \mathbb{Z}^r$ be the subset generated by

$$\{\lambda - \mu : \exists \nu \in \mathcal{P}, \lambda, \mu \in \nu\}$$

Then $\varepsilon(\mathcal{P},f) = \varepsilon(\psi_{\mathcal{P},f})$, where $\psi_{\mathcal{P},f}$ is the map defined in the previous section, so by Corollary 3.5, any connected component of a fiber of $\psi_{\mathcal{P},f}$ is a translate of $V(\overline{\varepsilon(\mathcal{P},f)})$.

For any subset $\mathcal{U} \subset \Pi_f$, let $\varepsilon(\mathcal{U},f) \subset \mathbb{Z}^r$ be the subgroup generated by

$$\bigcup_{\mathcal{P} \in \mathcal{U}} \varepsilon(\mathcal{P},f).$$

Then by Proposition 3.6 any rational plane Q in the intersection

$$\bigcap_{\mathcal{P} \in \mathcal{U}} F_{\mathcal{P}}$$

where each $F_{\mathcal{P}}$ is a fiber of $\psi_{\mathcal{P},f}$, is a translate of $V(\overline{\varepsilon(\mathcal{U},f)})$.

Let

$$D(\mathcal{U},f) = D(\overline{\varepsilon(\mathcal{U},f)}/\varepsilon(\mathcal{U},f))$$

and let

$$D(f) = \operatorname{lcm}\,\{D(\mathcal{U},f) : \mathcal{U} \subset \Pi_f\}.$$

Let

$$M(\mathcal{P},f) = \max\,(\{\operatorname{ord}(x) : x \in S(\mathcal{P},f)\} \cup \{1\})$$

and let

$$M(f) = \operatorname*{lcm}_{\mathcal{P} \in \Pi_f} M(\mathcal{P},f).$$

Proposition 5.3 *Let $f \in \Lambda_r$ any Laurent polynomial and $V = V(f)$. Then any rational plane $Q \subset V(f)$ is a translate of $V(\overline{\varepsilon(\mathcal{P},f)})$, for some partition $\mathcal{P} \in \Pi_f$. Furthermore,*

$$\deg(p_{V(f)}) = \max_{\mathcal{P} \in \Pi_f} (r - \operatorname{rank}(\overline{\varepsilon(\mathcal{P},f)})\delta_{\mathcal{P},f}$$

and

$$\operatorname{per}(p_{V(f)}) \quad | \quad M(f)D(f).$$

Proof. Recall that

$$\overline{\mathrm{Tor}(V(f))}^{\mathrm{Zar}} = \bigcup_{\mathcal{P}\in\Pi_f} \psi^{-1}_{\mathcal{P},f}(S(\mathcal{P},f)).$$

Thus, the degree of $p_{V(f)}$ is the maximum dimension of rational planes in $\psi^{-1}_{\mathcal{P},f}(S(\mathcal{P},f))$. Since $\varepsilon(\psi_{\mathcal{P},f}) = \varepsilon(\mathcal{P},f)$, by Corollary 3.5, if $S(\mathcal{P},f)$ is not empty, then for any rational plane $Q \subset \psi^{-1}_{\mathcal{P},f}(S(\mathcal{P},f))$, we have

$$\dim(Q) = r - \mathrm{rank}(\overline{\varepsilon(\mathcal{P},f)}).$$

This gives the formula for $\deg(p_{V(f)})$. The period of p_V depends on the orders of rational planes in intersections of fibers of $\psi^{-1}_{\mathcal{P},f}$ over $S(\mathcal{P},f)$. Any such intersection is empty if it involves more than one fiber of $\psi_{\mathcal{P},f}$, for some $\mathcal{P}$. Let $\mathcal{U} \subset \Pi_f$ be any subset such that, for any $\mathcal{P}\in\mathcal{U}$, $\delta_{\mathcal{P},f} = 1$. Choose a connected component $Q_{\mathcal{P}} \subset \psi^{-1}_{\mathcal{P},f}(S(\mathcal{P},f))$ for each $\mathcal{P}\in\mathcal{U}$. Let

$$M = \operatorname*{lcm}_{\mathcal{P}\in\mathcal{U}} \mathrm{ord}(\psi_{\mathcal{P}}(Q_{\mathcal{P}})).$$

Then, by Proposition 3.6, for any rational plane Q in the intersection

$$\bigcap_{\mathcal{P}\in\mathcal{U}} Q_{\mathcal{P}},$$

we have

$$\mathrm{ord}(Q) \mid M\ D(\mathcal{U},f).$$

Taking the least common multiple of both sides, the claim follows.

∎

While the various groups denoted by $\varepsilon(-)$ can be computed routinely, the sets $S(\mathcal{P},f)$ need to be studied in a case by case manner. When f is defined over $\mathbb{Q}$ the results described in section 4 are aids to computation.

In particular, we have the following result of Mann [M] (cf. Proposition 4.3).

Proposition 5.4 *(Mann) Let $\epsilon = (\epsilon_1,\ldots,\epsilon_r)$ be any finite order maximal solution to a linear equation*

$$\sum_{i=1}^{r} a_i\epsilon_i = 1,$$

with $a_i \in \mathbb{Q}$ for all $i = 1,\ldots,r$. Let n be the order of ϵ as an element of $(\mathbb{C}^*)^r$. Then n is square free and, if $n = p_1 \ldots p_k$ is a factorization, then $p_i \le r+1$ for $i = 1,\ldots,k$.

As a consequence of Proposition 5.4, we have the following bound on $M(\mathcal{P},f)$. For any partition $\mathcal{P}$, let

$$R(\mathcal{P}) = \max\ \{|\nu| : \nu \in \mathcal{P}\}.$$

For any positive integer R, let $N[R]$ be the product of distinct primes less than or equal to R.

Corollary 5.5 *If $f \in \Lambda_r$ is defined over $\mathbb{Q}$ and has R coefficients, then*

$$M(\mathcal{P}, f) \mid N[R(\mathcal{P})]$$

for any partition $\mathcal{P} \in \Pi_f$.

We will now give bounds on $p_{V(\mathcal{F})}$, where $\mathcal{F} = \{f_1, \ldots, f_k\} \subset \Lambda_r$ is any finite subset. For any $\pi = (\mathcal{P}_1, \ldots, \mathcal{P}_k) \in \Pi_{\mathcal{F}}$, let

$$\begin{aligned} \varepsilon(\pi, \mathcal{F}) &= \varepsilon(\mathcal{P}_1, f_1) + \ldots + \varepsilon(\mathcal{P}_k, f_k), \\ S(\pi, \mathcal{F}) &= S(\mathcal{P}_1, f_1) \times \ldots \times S(\mathcal{P}_k, f_k), \\ R(\pi) &= \max \{R(\mathcal{P}_i) : i = 1, \ldots, k\}, \\ M(\pi, \mathcal{F}) &= \operatorname{lcm} \{\operatorname{ord}(x) : x \in S(\pi, \mathcal{F})\}, \text{ and} \\ M(\mathcal{F}) &= \operatorname{lcm} \{M(\pi, \mathcal{F}) : \pi \in \Pi_{\mathcal{F}}\}. \end{aligned}$$

For any subset $\mathcal{U} \subset \Pi_{\mathcal{F}}$, define $\varepsilon(\mathcal{U}, \mathcal{F}) \subset \mathbb{Z}^r$ to be the subgroup generated by

$$\bigcup_{\pi \in \mathcal{U}} \varepsilon(\pi, \mathcal{F}).$$

Let

$$\begin{aligned} D(\mathcal{U}, \mathcal{F}) &= D(\overline{\varepsilon(\mathcal{U}, \mathcal{F})}/\varepsilon(\mathcal{U}, \mathcal{F})) \\ D(\mathcal{F}) &= \operatorname{lcm} \{D(\mathcal{U}, \mathcal{F}) : \mathcal{U} \subset \Pi_{\mathcal{F}}\}. \end{aligned}$$

Thus, for any $\lambda \in \overline{\varepsilon(\mathcal{U}, \mathcal{F})}/\varepsilon(\mathcal{U}, \mathcal{F})$, we have $\operatorname{ord}(\lambda) \mid D(\mathcal{F})$.

Let ρ be defined by

$$\begin{aligned} \rho : \varepsilon(\mathcal{P}_1, f_1) \times \ldots \times \varepsilon(\mathcal{P}_k, f_k) &\to \varepsilon(\mathcal{P}_1, f_1) + \ldots + \varepsilon(\mathcal{P}_k, f_k) \\ (\lambda_1, \ldots, \lambda_k) &\mapsto \lambda_1 + \ldots + \lambda_k \end{aligned}$$

and let

$$\gamma : \varepsilon(\mathcal{P}_1, f_1) \times \ldots \times \varepsilon(\mathcal{P}_k, f_k) \hookrightarrow Z^r \times \ldots \times \mathbb{Z}^r$$

be the inclusion map. Let

$$\delta_{\pi, \mathcal{F}} = \begin{cases} 1 & \text{if } \gamma^*(S(\pi, \mathcal{F})) \cap \operatorname{im}(\rho^*) \neq \emptyset, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 5.3 extends to arbitrary algebraic subsets as follows.

Theorem 3 *Let $\mathcal{F} \subset \Lambda_r$ be a finite subset let and $V = V(\mathcal{F})$. Then any rational plane $Q \subset V$ is a translate of $V(\overline{\varepsilon(\pi, \mathcal{F})})$ for some partition $\pi \in \Pi_{\mathcal{F}}$. Furthermore,*

$$\deg(p_V) = \max_{\pi \in \Pi_{\mathcal{F}}} (r - \operatorname{rank}(\overline{\varepsilon(\pi, \mathcal{F})}))\delta_{\mathcal{P}, \mathcal{F}}$$

and

$$\operatorname{per}(p_V) \mid M(\mathcal{F}) \; D(\mathcal{F}).$$

Proof. From (9), we know that $\overline{\mathrm{Tor}(V(\mathcal{F}))}^{\mathrm{Zar}}$ is the union over $\pi \in \Pi_{\mathcal{F}}$ of

$$Q(\pi, \mathcal{F}) = \bigcap_{i=1}^{k} \psi^{-1}_{\mathcal{P}_i, f}(S(\mathcal{P}_i, f)).$$

Hence $\deg(p_V)$ is the maximum dimension of any rational plane $Q \subset Q(\pi, \mathcal{F})$. By Proposition 3.6, $Q(\pi, \mathcal{F})$ is nonempty if and only if $\delta_{\pi, \mathcal{F}} = 1$. Also by Proposition 3.6, any rational plane $Q \subset Q(\pi, \mathcal{F})$ is a translate of $V(\overline{\varepsilon(\pi, \mathcal{F})})$ and its dimension equals $r - \mathrm{rank}(\overline{\varepsilon(\pi, \mathcal{F})})$. This gives the formula for the degree of p_V.

The period $\mathrm{per}(p_V)$ is the lcm of $\mathrm{ord}(Q)$, where Q is a rational plane in the intersection $\bigcap_{\pi \in \mathcal{U}} Q_\pi$, where $Q_\pi \subset Q(\pi, \mathcal{F})$, is some choice of rational planes and π ranges in a subset $\mathcal{U} \subset \Pi_{\mathcal{F}}$. Note that

$$M(\mathcal{U}, \mathcal{F}) = \mathrm{lcm}\ \{M(\pi, \mathcal{F}) : \pi \in \mathcal{U}\}$$

divides $M(\mathcal{F})$. By Proposition 3.6, we have

$$\mathrm{ord}(Q) \mid M(\mathcal{U}, \mathcal{F})\ D(\mathcal{U}, \mathcal{F})$$

and taking the least common multiple of both sides, we get the bound for the period of $p_{V(f)}$.

■

5.3 Proof of Theorem 2.

Theorem 2 follows easily from Theorem 3 and Corollary 5.5. To prove (i), we need to find polynomials defining the rational planes in V. Since by Theorem 3, any rational plane Q in V is of the form $Q = \eta V(\varepsilon)$, where $\varepsilon = \overline{\varepsilon(\pi, \mathcal{F})}$ and η is a finite order element of $(\mathbb{C}^*)^r$. By Lemma 3.1, $V(\varepsilon)$ is defined by I_ε and (i) follows. The bound for $\deg(p_V)$ in (ii) comes from ignoring the $\delta_{\mathcal{P}, V}$ in Theorem 3. By Corollary 5.5, we have the inequality

$$M(\mathcal{F}) \mid N[R(\mathcal{F})],$$

where $R(\mathcal{F})$ is the maximum number of coefficients of a Laurent polynomial $f \in \mathcal{F}$. This implies the bound for $\mathrm{per}(p_V)$ in (iii).

■

6 Examples

In this section we consider some algebraic subsets $V \subset (\mathbb{C}^*)^r$ defined by a finite set of Laurent polynomials $\mathcal{F} \subset \Lambda_r$ and study the torsion points on V in terms of $\mathcal{F}$. We start with some notation. For any $m \in \mathbb{N}$, let $\mathcal{C}_m : \mathbb{N} \to \mathbb{N}$ be the periodic function defined by

$$\mathcal{C}_m(n) = \begin{cases} 1 & \text{if } m \text{ divides } n, \\ 0 & \text{otherwise} \end{cases}$$

For any root of unity ϵ, let $\theta(\epsilon) \in \mathbb{Q}/\mathbb{Z}$ be such that

$$\epsilon = \exp(2\pi\sqrt{-1}\,\theta(\epsilon)).$$

For any positive integer n, denote by ζ_n the primitive nth root of unity such that $\theta(\zeta_n) = 1/n$. For any $\theta \in (\mathbb{Q}/\mathbb{Z})^r$, let $\mathrm{ord}(\theta)$ be the least positive integer n, such that $n\theta = 0 (\mathrm{mod}\ 1)$.

For any torsion point $\epsilon = (\epsilon_1, \ldots, \epsilon_r)$ in $(\mathbb{C}^*)^r$ define

$$\theta(\epsilon) = (\theta(\epsilon_1), \ldots, \theta(\epsilon_r)) \ \in \ (\mathbb{Q}/\mathbb{Z})^r.$$

Then

$$\mathrm{ord}(\epsilon) = \mathrm{ord}(\theta(\epsilon)).$$

A binomial equation

$$t^\lambda - \zeta = 0 \tag{10}$$

where $\lambda = (\lambda_1, \ldots, \lambda_r) \in \mathbb{Z}^r$ and ζ is a root of unity $\zeta = \zeta_n^k$, $0 \le k \le n-1$, corresponds to a linear equation

$$\lambda_1\theta_1 + \ldots + \lambda_r\theta_r = k/n \ (\mathrm{mod}\ 1), \tag{11}$$

in the sense that ϵ satisfies (10) if and only if $\theta(\epsilon)$ is a solution to (11). We'll call equation (11) the *exponential form* of equation (10).

We'll use the following simplification of Theorem 3 in Examples 2 and 3.

Proposition 6.1 *Suppose $\Pi_{\mathcal{F}}$ contains only one element π. Let*

$$M(\mathcal{F}) = \mathrm{lcm}\ \{\mathrm{ord}(x) : x \in S(\pi, \mathcal{F})\} \cup \{1\}$$

and let

$$D(\mathcal{F}) = D(\overline{\varepsilon(\pi, \mathcal{F})}/\varepsilon(\pi, \mathcal{F})).$$

If $S(\pi, \mathcal{F}) = \emptyset$, then $p_{V(\mathcal{F})} = 0$. Otherwise,

$$\deg(p_{V(\mathcal{F})}) = r - \mathrm{rank}(\overline{\varepsilon(\pi, \mathcal{F})}).$$

and

$$M(\mathcal{F}) \mid \mathrm{per}(p_{V(\mathcal{F})}) \mid M(\mathcal{F})\ D(\mathcal{F}).$$

Proof. We have

$$\overline{\mathrm{Tor}(V)}^{\mathrm{Zar}} = \psi_{\pi,\mathcal{F}}^{-1}(S(\pi, \mathcal{F})),$$

which is a union of disjoint rational planes contained in fibers over the points in $S(\pi, \mathcal{F})$. Since $\varepsilon(\pi, \mathcal{F}) = \varepsilon(\psi_{\pi,\mathcal{F}})$, the rest follows from Corollary 3.5.

■

Example 1. We begin with a set of examples where the degree bound in Theorem 2 is attained. Let r be an even number, $r = 2k$. Let

$$f = \sum_{i=1}^{r} (-1)^i t_i \in \Lambda_r$$

and $V = V(f)$.

We can see immediately that $V(f)$ contains the affine subtorus

$$P = V(\{t_i t_{i+1}^{-1} - 1 : i = 2j-1, j = 1, \ldots, k\}).$$

The dimension of P equals the dimension of solutions $\theta = (\theta_1, \ldots, \theta_r) \in (\mathbb{Q}/\mathbb{Z})^r$ such that

$$\theta_{2j-1} - \theta_{2j} = 0 \pmod 1, \qquad \text{for all } j = 1, \ldots, k.$$

The dimension is clearly $r - k = k$, so $\deg(p_{V(f)}) \geq k$.

Now take any partition $\mathcal{P} \in \Pi_f$. Then $\varepsilon(\mathcal{P}, f) = \overline{\varepsilon(\mathcal{P}, f)}$ and

$$\operatorname{rank}(\varepsilon(\mathcal{P}, f)) = \sum_{\nu \in \mathcal{P}} (|\nu| - 1) \geq k.$$

Therefore,

$$\deg(p_{V(f)}) \leq n - k = k$$

and we have equality.

Example 2. Let $V(f) \in (\mathbb{C}^*)^r$ be defined by

$$f = a_1 t^{\lambda_1} + a_2 t^{\lambda_2} + a_3 t^{\lambda_3}, \qquad a_i \in \mathbb{Q}^*$$

Since there are only three coefficients there is only one parition in Π_f, namely $\mathcal{P} = \{1, 2, 3\}$.

We have

$$\varepsilon = \varepsilon(\mathcal{P}, f) = \{\lambda_1 - \lambda_3, \lambda_2 - \lambda_3\}$$
$$L_{\mathcal{P},f} : \frac{-a_1}{a_3} x + \frac{-a_1}{a_2} y - 1$$

The following is a table of all possible values for $a = -a_1/a_3$ and $b = -a_2/a_3$ which give nonempty $S(\mathcal{P}, f)$.

(a, b)	$S(\mathcal{P}, f)$
$(1, 1)$	$(\zeta_6, \zeta_6^{-1}), (\zeta_6^{-1}, \zeta_6)$
$(1, -1)$	$(\zeta_6, \zeta_3), (\zeta_6^{-1}, \zeta_3^{-1})$
$(-1, 1)$	$(\zeta_3, \zeta_6), (\zeta_3^{-1}, \zeta_6^{-1})$
$(-1, -1)$	$(\zeta_3, \zeta_3^{-1}), (\zeta_3^{-1}, \zeta_3)$
$(1/2, 1/2)$	$(1, 1)$
$(1/2, -1/2)$	$(1, -1)$
$(-1/2, 1/2)$	$(-1, 1)$
$(-1/2, -1/2)$	$(-1, -1)$

Thus, for example, if $f = t_1 + t_2 + t_3$, then

$$p_{V(f)}(n) = 2n\ \mathcal{C}_3(n).$$

If $\mathcal{F} \subset \Lambda_r$ is any finite collection of Laurent polynomials with three coefficients, then $\Pi_{\mathcal{F}}$ contains a single element π so we can use Proposition 6.1.

Let $V = V(\mathcal{F})$, $\mathcal{F} = \{f_1, f_2\} \subset \Lambda_r$, where

$$\begin{aligned} f_1 &= t_1 t_3 + t_4 + \alpha \\ f_2 &= t_1 + t_2 + \beta t_3 \end{aligned}$$

where $\alpha, \beta \in \{\pm 1\}$.

Then $\Pi_{\mathcal{F}}$ has a single element $\pi = (\mathcal{P}, \mathcal{P})$, where $\mathcal{P} = \{1, 2, 3\}$. Since

$$\begin{aligned} &\varepsilon = \varepsilon(\pi, \mathcal{F}) = \varepsilon(\mathcal{P}, f_1) + \varepsilon(\mathcal{P}, f_2) \\ &\quad = \{(1,0,1,0), (0,0,0,1), (1,0,-1,0), (0,1,-1,0)\} \\ &\overline{\varepsilon} = \mathbb{Z}^4, \\ &D(\mathcal{F}) = D(\overline{\varepsilon}/\varepsilon) = D(\mathbb{Z}/2\mathbb{Z}) = 2, \end{aligned}$$

by Proposition 6.1, the bounds on the degree and period of p_V are

$$0 \le \deg(p_V) \le r - \operatorname{rank}(\overline{\varepsilon}) = 4 - 4 = 0$$

which implies $\deg(p_V) = 0$ and

$$M(\mathcal{F}) \mid \operatorname{per}(p_V) \mid 2M(\mathcal{F}).$$

For any α and β, the exponential form of equations defining

$$\overline{\operatorname{Tor}(V)}^{\mathrm{Zar}} = \psi_{\pi,\mathcal{F}}^{-1}(S(\pi, \mathcal{F})),$$

are the linear equations

$$\begin{aligned} \theta_1 + \theta_3 &= c \pmod 1 \\ \theta_4 &= -c \pmod 1 \\ \theta_1 - \theta_3 &= d \pmod 1 \\ \theta_2 - \theta_3 &= -d \pmod 1. \end{aligned}$$

where c and d range in $A \times B$, and depend on α and β. The following table shows the p_V corresponding to the different choices of α and β.

(α, β)	A	B	$M(\mathcal{F})$	p_V	$\operatorname{per}(p_V)$
$(1, 1)$	$\{1/3, 2/3\}$	$\{1/3, 2/3\}$	3	$4\,\mathcal{C}_3 + 4\,\mathcal{C}_6$	6
$(1, -1)$	$\{1/3, 2/3\}$	$\{1/6, 5/6\}$	6	$8\,\mathcal{C}_{12}$	12
$(-1, 1)$	$\{1/6, 5/6\}$	$\{1/3, 2/3\}$	6	$8\,\mathcal{C}_{12}$	12
$(-1, -1)$	$\{1/6, 5/6\}$	$\{1/6, 5/6\}$	6	$8\,\mathcal{C}_6$	6

Note that in the last example where $(\alpha, \beta) = (-1, -1)$ is the period of p_V strictly less than $M(\mathcal{F})\ D(\mathcal{F})$.

We will now justify the entries in the column under p_V in the table.

If $\alpha = \beta = 1$, we have solutions

(c, d)	solutions $(\theta_1, \theta_2, \theta_3, \theta_4)$
$(1/3, 1/3)$	$(1/3, 2/3, 0, 2/3), (5/6, 1/6, 1/2, 2/3)$
$(1/3, 2/3)$	$(0, 2/3, 1/3, 2/3), (1/2, 1/6, 5/6, 2/3)$
$(2/3, 1/3)$	$(0, 1/3, 2/3, 1/3), (1/2, 5/6, 1/6, 1/3)$
$(2/3, 2/3)$	$(2/3, 1/3, 0, 1/3), (1/6, 5/6, 1/2, 1/3)$

There are four solutions with order 3 and four with order 6, thus,

$$p_V(n) = \begin{cases} 8 & \text{if } 6 \mid n, \\ 4 & \text{if } 3 \mid n \text{ and } 6 \nmid n \\ 0 & \text{otherwise} \end{cases}$$

and hence $p_V(n) = 4\ \mathcal{C}_6(n) + 4\ \mathcal{C}_3(n)$.

If $\alpha = 1$ and $\beta = -1$, we have the solutions:

(c, d)	solutions $(\theta_1, \theta_2, \theta_3, \theta_4)$
$(1/3, 1/6)$	$(1/4, 11/12, 1/12, 2/3), (3/4, 5/12, 7/12, 2/3)$
$(1/3, 5/6)$	$(1/12, 5/12, 1/4, 2/3), (7/12, 11/12, 3/4, 2/3)$
$(2/3, 1/6)$	$(11/12, 7/12, 3/4, 1/3), (5/12, 1/12, 1/4, 1/3)$
$(2/3, 5/6)$	$(3/4, 1/12, 11/12, 1/3), (1/4, 7/12, 5/12, 1/3)$

All solutions have order 12 so we have $p_V(n) = 8\ \mathcal{C}_{12}(n)$.

If $\alpha = -1$ and $\beta = 1$, we have the solutions:

(c, d)	solutions $(\theta_1, \theta_2, \theta_3, \theta_4)$
$(1/6, 1/3)$	$(1/4, 7/12, 11/12, 5/6), (3/4, 1/12, 5/12, 5/6)$
$(1/6, 2/3)$	$(5/12, 1/12, 3/4, 5/6), (11/12, 7/12, 1/4, 5/6)$
$(5/6, 1/3)$	$(7/12, 11/12, 1/4, 1/6), (1/12, 5/12, 3/4, 1/6)$
$(5/6, 2/3)$	$(3/4, 5/12, 1/12, 1/6), (1/4, 11/12, 7/12, 1/6)$

All solutions have order 12 so $p_V(n) = 8\ \mathcal{C}_{12}(n)$.

If $a = b = -1$, we have solutions

(c, d)	solutions $(\theta_1, \theta_2, \theta_3, \theta_4)$
$(1/6, 1/6)$	$(1/6, 5/6, 0, 5/6), (2/3, 1/3, 1/2, 5/6)$
$(1/6, 5/6)$	$(0, 1/3, 1/6, 5/6), (1/2, 5/6, 2/3, 5/6)$
$(5/6, 1/6)$	$(0, 2/3, 5/6, 1/6), (1/2, 1/6, 1/3, 1/6)$
$(5/6, 5/6)$	$(5/6, 1/6, 0, 1/6), (1/3, 2/3, 1/2, 1/6)$

All solutions have order 6, so $p_V(n) = 8\ \mathcal{C}_6(n)$.

Example 3. We now study the Fermat curve $V(f)$, defined by

$$f(t_1, t_2) = t_1^m + t_2^m - 1.$$

Then

$$\begin{aligned}
&\overline{\mathrm{Tor}(V(f))}^{\mathrm{Zar}} = \phi^{-1}_{\mathcal{P},f}(S(\mathcal{P}, f)) \\
&S(\mathcal{P}, f) = \{\mu_1, \mu_2\} \qquad \mu_1 = (\zeta_6, \zeta_6^{-1}), \quad \mu_2 = (\zeta_6^{-1}, \zeta_6), \\
&M(f) = 6, \\
&\varepsilon = \varepsilon(\mathcal{P}, f) = \{(m, 0), (0, m)\}, \\
&\overline{\varepsilon} = \{(1, 0), (0, 1)\} = \mathbb{Z}^2, \\
&\overline{\varepsilon}/\varepsilon = (\mathbb{Z}/m\mathbb{Z})^2, \\
&D(f) = D((\mathbb{Z}/m\mathbb{Z})^2) = m
\end{aligned}$$

We thus have

$$\deg(p_{V(f)}) = 0$$

and

$$6 = M(f) \mid \mathrm{per}(p_{V(f)}) \mid M(f)\ D(f) = 6m.$$

For integers $a, b \in \mathbb{Z}$, let (a, b) denote their greatest common divisor. We'll show that

$$p_V(f) = \begin{cases} 2(m, n)^2 & \text{if } 6 \mid \frac{n}{(n,m)}, \\ 0 & \text{otherwise.} \end{cases}$$

and hence $p_{V(f)}$ has period $6m$.

For instance, if $m = 3$, $p_V(n) = 18\ C_{18}(n)$.

The exponential linear equations associated to $\phi_{\mathcal{P},f}$ are

$$\begin{cases} m\theta_1 &= 1/6 \pmod 1 \\ m\theta_2 &= 5/6 \pmod 1 \end{cases} \qquad \begin{cases} m\theta_1 &= 5/6 \pmod 1 \\ m\theta_2 &= 1/6 \pmod 1 \end{cases} \tag{12}$$

Consider the first equation and suppose there is a solution

$$(\theta_1, \theta_2) = (a/n, b/n) \in (\mathbb{Q}/\mathbb{Z})^2.$$

We will show that 6 divides $n/(m, n)$. The equations in (12) imply that

$$ma/n - 1/6 \in \mathbb{Z}$$

so $6n$ divides $6ma - n$ and hence 6 divides n. Setting $n_1 = n/6$, we have n divides $ma - n_1$. Set $m_1 = m/(m, n)$. Then

$$m_1(m, n)a = n_1 \pmod{n}.$$

Since $(m_1, n) = 1$, m_1 is invertible modulo n and there is some $m_2 \in \mathbb{Z}$ such that $m_2 m_1 = 1 (\mathrm{mod}\ n)$. Thus,

$$(m, n)a = m_2 n_1 \pmod{n}$$

and hence

$$(m, n)a = m_2 n_1 + nr,$$

for some integer r. Since n is relatively prime to m_1 and m_2, so is (m, n). Thus, (m, n) divides n_1 and hence 6 divides $n/(m, n)$.

Conversely, suppose 6 divides $n/(m, n)$. Let m_1 be a representative for the multiplicative inverse of $m/(m, n)$ modulo n. Then

$$a = \frac{n}{6(m, n)} m_1 \qquad b = \frac{-n}{6(m, n)} m_1$$

is a solution to the first system and (b, a) is a solution to the second.

To find the number of solutions of order n. We need to look at the homogeneous equations

$$m(r/n) = 0 \pmod{1} \qquad m(s/n) = 0 \pmod{1}.$$

These have solutions $r, s \in \mathbb{Q}/\mathbb{Z}$ given by

$$r = kn/(m, n), \quad s = \ell n/(m, n)$$

for $k, \ell = 0, \ldots, (m, n) - 1$. Thus, in total, there are $2(m, n)^2$ possible solutions to (12) of order n when 6 divides $n/(m, n)$.

∎

References

[A-S] S. Adams and P. Sarnak. Betti numbers of congruence groups. *Israel J. of Math.* **88** (1994), 31–72.

[C-J] J.H. Conway and A.J. Jones. Trigonometric diophantine equations. Acta Arithmetica. **30** (1976), 229-240.

[H] E. Hironaka. Alexander stratifications of character varieties Annales de l'Institut Fourier. (to appear)

[Lan] S. Lang. Fundamentals of diophantine geometry. Berlin-Heidelberg-New York : Springer. (1983).

[Lau] M. Laurent. Equations diophantine exponentielles. *Invent. Math.* **78** (1984), 299-327.

[Le] H.W. Lenstra, Jr. Vanishing sums of roots of unity. Proc. Bicentennial Congress Wiskundig Genootschap, Math. Centre Tracts. **101**, Amsterdam (1979), 249-268.

[M] H.B. Mann. On linear relations between roots of unity. *Mathematika* **12**, London (1965), 107-117.

[R] W. Ruppert. Solving algebraic equations in roots of unity. J. reine u. angw. Math. **435** (1993), 119-156.

[S] I.J. Schoenberg. A note on the cyclotomic polynomial. Mathematika. **11** (1964), 131-136.

M.S.R.I., 1000 Centennial Drive, Berkeley, CA 94720
eko@msri.org

Department of Mathematics, University of Toronto,
100 St George St., Toronto, ON M5S 3G3
eko@math.toronto.edu