Publ. Mat. **48** (2004), 127–137

COUNTING FIXED POINTS OF A FINITELY GENERATED SUBGROUP OF Aff$[\mathbb{C}]$

F. Loray, M. van der Put and F. Recher

Abstract

Given a finitely generated subgroup G of the group of affine transformations acting on the complex line $\mathbb{C}$, we are interested in the quotient $\mathrm{Fix}(G)/G$. The purpose of this note is to establish when this quotient is finite and in this case its cardinality. We give an application to the qualitative study of polynomial planar vector fields at a neighborhood of a nilpotent singular point.

Introduction

Consider the group of affine transformations acting on the complex line $\mathbb{C}$

$$\mathrm{Aff}[\mathbb{C}] = \{aX + b;\ a, b \in \mathbb{C},\ a \neq 0\}.$$

For a finitely generated subgroup $G < \mathrm{Aff}[\mathbb{C}]$, we denote by $\mathrm{Fix}(G) \subset \mathbb{C}$ the set of all the points which are fixed by a non-trivial element of G (i.e. whose isotropy group $G^{\{c\}} = \{g \in G;\ g(c) = c\}$ is not reduced to the identity $\{X\}$)

$$\mathrm{Fix}(G) = \{c \in \mathbb{C};\ \exists\, g \in G,\ g(c) = c \text{ and } g \neq X\}.$$

The group G acts on this set and we denote by $\mathrm{Fix}(G)/G$ the set of G-orbits. The purpose of this note is to answer to the following two questions:

- When is $\mathrm{Fix}(G)/G$ finite?
- Suppose that $\mathrm{Fix}(G)/G$ is finite, what is its cardinality?

Motivations and application

More generally, these questions arise naturally for a finitely generated subgroup G of the group $\mathrm{Diff}(N)$ of diffeomorphisms of a smooth manifold N when one wants to study the topology of the leaves of a foliated manifold $(M, \mathcal{F})$ given by *suspension* of a representation

$$\rho\colon \pi_1(B, b) \longrightarrow \mathrm{Diff}(N)$$

2000 *Mathematics Subject Classification.* Primary: 34C; Secondary: 11A.
Key words. Limit cycles, singularities of vector fields, Riccati equation.

where $\pi_1(B,b)$ denotes the fundamental group of another manifold B (see also [**G**, Chapter I, 2.8]). Let us briefly recall the construction of the suspension $(M,\mathcal{F})$. Consider the canonical representation of the fundamental group $\sigma\colon \pi_1(B,b) \to \mathrm{Diff}(\widetilde{B})$ in the deck transformations of the universal covering $\widetilde{B}$. The image of the representation

$$\widetilde{\rho}\colon \left\{ \begin{array}{rcl} \pi_1(B,b) & \longrightarrow & \mathrm{Diff}(\widetilde{B}\times N) \\ \gamma & \longmapsto & (\sigma(\gamma),\rho(\gamma)) \end{array} \right.$$

acts properly and discontinuously on the product $\widetilde{B}\times N$. The quotient manifold $M = \widetilde{B}\times N/\widetilde{\rho}$ is the total space of a locally trivial bundle $\Pi\colon M \to B$ whose fibers are isomorphic to N. The horizontal foliation on $\widetilde{B}\times N$ whose leaves are $\widetilde{B}\times\{p\}$, $p\in N$, is invariant under the action of $\widetilde{\rho}$ and thus induces a regular foliation $\mathcal{F}$ on M. The leaves of $\mathcal{F}$ are transversal to the fibers and have the same dimension as the basis B. The projection Π induces by restriction a covering of each leaf $\Pi\big|_L\colon L\to B$ onto the basis. More precisely, if L_p denotes the leaf passing through $p\in\Pi^{-1}(b)\simeq N$, any loop $\gamma\in\pi_1(B,b)$ lifts-up at p as a path $\tilde{\gamma}\colon[0,1]\to L_p$ joining $\tilde{\gamma}(0)=p$ to $\tilde{\gamma}(1)=\rho(\gamma)(p)$. The fundamental group of L_p is given by the exact sequence

$$1\longrightarrow \ker(\rho)\longrightarrow \pi_1(L_p,p)\longrightarrow G^{\{p\}}\longrightarrow 1$$

where $G<\mathrm{Diff}(N)$ denotes the image of ρ and $G^{\{p\}}=\{g\in G;\, g(p)=p\}<G$, the isotropy subgroup associated to p. In other words, the fundamental group $\pi_1(L_p,p)$ of L_p is isomorphic to $\rho^{-1}(G^{\{p\}})=\{\gamma\in\pi_1(B,b);\,\rho(\gamma)(p)=p\}$. Therefore, the leaves L_p passing through generic points p (having trivial isotropy group) are pairwise diffeomorphic (universal property of coverings) with same fundamental group $\pi_1(L_p,p)\simeq\ker(\rho)$. Finally, the two questions above are related to counting the non-generic leaves, i.e. those leaves having more topology (or having non-trivial holonomy). The number of them is then given by $\mathrm{Fix}(G)/G$ and their fundamental group is increased by $G^{\{p\}}$.

Such foliations naturally appear for instance in the phase portrait of a differential equation of Riccati type $y' = a(x)y^2+b(x)y+c(x)$ where a, b and c denote rational functions of x. Denote by $\Omega\subset\mathbb{C}$ the complement of the polar set of a, b and c. The regular foliation induced in variables (x,y) on $\Omega\times\mathbb{C}$ extends as a regular foliation $\mathcal{F}$ on $\Omega\times P^1(\mathbb{C})$ transversal to the vertical fibration and is actually the suspension of the monodromy representation $\rho\colon\pi_1(\Omega,x_0)\to PGL(2,\mathbb{C})$ (see [**H**]). The case $N=\mathbb{C}$ and $\mathrm{Diff}(N)=\mathrm{Aff}[\mathbb{C}]$ considered in the present note occurs when the Riccati equation has a rational solution.

The monodromy group G is therefore affine in a convenient projective coordinate. It would be interesting to answer to the same questions in the more general case of $PGL(2,\mathbb{C})$ acting on the projective sphere. This note underlines the surprising complexity of this simple problem even in the affine case and suggests that the projective case will be difficult. Already, the affine case naturally arises when we study the topology of complex trajectories of a singular analytic vector field in the plane having a Liouvillian first integral. For instance, the trajectories of the nilpotent Hamiltonian vector field $V_0 := y\partial_x + nx^{2n-1}\partial_y$, $n \geq 2$, are completely understood by means of the first integral $f_0(x,y) = y^2 - x^{2n}$: all trajectories apart from the singular fiber $\{y^2 - x^{2n} = 0\}$ have the same topology at a neighborhood of $(x,y) = (0,0) \in \mathbb{C}^2$. Now, consider a perturbation V of V_0 having the form:

$$V = (y\partial_x + nx^{2n-1}\partial_y) + (\alpha + x)x^{n-1}(x\partial_x + ny\partial_y)$$

for a complex number $\alpha \in \mathbb{C}$. As a direct application of the results of this note, we obtain the:

Corollary 1. *When $\alpha \in \mathbb{C} - \mathbb{Q}$ and $n \geq 3$, the polynomial vector field V above has infinitely many complex trajectories having non-periodic holonomy in any neighborhood of the singular point $(x,y) = (0,0)$. When $\alpha \in \mathbb{Q}$, then V has finitely many trajectories having non-trivial holonomy, the number of which depends on the arithmetic of n and α. For instance, when $\alpha = 0$ and $n = p$ is an odd prime number, there are $1 + \frac{p-1}{2} + \frac{2^{p-1}-1}{p}$ such trajectories.*

In particular, this corollary provides explicit examples of polynomial planar vector fields having infinitely many complex limit cycles at the neighborhood of a nilpotent singular point.

Proof: The phase portrait of the vector field V is defined by the equation $\omega = 0$ where ω is the holomorphic 1-form

$$\omega = (y\,dy - nx^{2n-1}\,dx) + (\alpha + x)x^{n-1}(x\,dy - ny\,dx).$$

In coordinates $t = y/x^n$ and $z = 1/x$, we obtain the Fuchsian Riccati equation

$$\frac{dz}{dt} = \frac{(t+\alpha)z + 1}{n(t^2-1)} = \frac{(1+\alpha)z+1}{2n(t-1)} + \frac{(1-\alpha)z-1}{2n(t+1)}.$$

The monodromy group of this equation is affine, generated by the monodromy maps around 1 and -1

$$g_1(z) = e^{2i\pi\frac{(1+\alpha)}{2n}}z + c_1 \quad \text{and} \quad g_{-1}(z) = e^{2i\pi\frac{(1-\alpha)}{2n}}z + c_{-1}$$

for some constants $c_1, c_{-1} \in \mathbb{C}$.

We claim that g_1 and g_{-1} commute if, and only if, $\frac{(1+\alpha)}{2n}$ or $\frac{(1-\alpha)}{2n}$ belongs to $\mathbb{Z}-\{0\}$. Indeed, when $\alpha \neq -1$, the Riccati equation has two singular points over the singular point $t=1$, namely $z=\frac{-1}{1+\alpha}$ and $z=\infty$. Therefore, the corresponding monodromy map is conjugated to its linear part (which is the identity) if, and only if, $\frac{(1+\alpha)}{2n} \in \mathbb{Z}$. If $\alpha=-1$, the Riccati equation has a double singular point at $z=\infty$ and g_1 is a translation which obviously does not commute with g_{-1}. Finally, when g_1 and g_{-1} both have a non-trivial linear part, then they commute, if, and only if, they share a common fixed point in $\mathbb{C}$ corresponding to a rational solution $z(t)$ of the Riccati equation. One can see from the phase portrait of this equation in $(t,z) \in \mathbb{P}^1 \times \mathbb{P}^1$ that the graph of $z(t)$ cannot intersect the invariant line $z=\infty$, but must intersect the lines $t=1,-1,\infty$ respectively at the singular points $z=\frac{-1}{1+\alpha}, \frac{1}{1-\alpha}, 0$. In other words, the rational function $z(t)$ has no pole on the Riemann sphere and satisfies $z(1) \neq z(-1)$. This contradicts Liouville Theorem and proves the claim.

When α is irrational, g_1 and g_{-1} have non-periodic linear parts and do not commute. Lemma 3 provides infinitely many trajectories having non-trivial holonomy. Moreover, the holonomy groups of those special trajectories are infinite, and contain contractions as soon as $\alpha \notin \mathbb{R}$.

When α is rational, g_1 and g_{-1} have periodic linear parts and the Riccati equation has finitely many trajectories having non-trivial holonomy by Theorem 2. For instance, when $\alpha=0$, we have after conjugacy

$$g_1 = \zeta_{2n} z \quad \text{and} \quad g_{-1} = \zeta_{2n} z + 1.$$

Therefore, the monodromy group G is also generated by

$$g_1 = \zeta_{2n} X \quad \text{and} \quad g_{-1} \circ (g_1)^{-1} = X + 1$$

and the number of exceptional trajectories is given by Theorem 4 with $m=2n$ and $r=1$.

Finally, assume that G is not abelian, and its linear part is not real. For instance, this is the case when $n \geq 3$ and α is zero or irrational. Then we claim that any complex trajectory of the Riccati equation having at least one non-trivial holonomy map actually contains loops arbitrary close to $z=\infty$ with t bounded providing this holonomy. Therefore, this holonomy will occur in any neighborhood of $(x,y)=(0,0)$ as holonomy of a trajectory of the vector field V. In order to prove the claim, it suffices to show that given a point $z \in \mathbb{C}$ fixed by a non trivial element $g \in G$, and given arbitrary large constant $T \gg 0$, one can find a conjugate $g' = \tilde{g}^{-1} \circ g \circ \tilde{g}$, $\tilde{g} \in G$, with a word decomposition

$$g' = (g_{\varepsilon_1})^{k_1} \circ (g_{\varepsilon_2})^{k_2} \circ \cdots \circ (g_{\varepsilon_M})^{k_M} \in G,$$

where $\varepsilon_m = \pm 1$ and $k_m \in \mathbb{Z}$ for $m = 1, 2, \ldots, M$, having the following property: the new fixed point $z' = \tilde{g}^{-1}(z)$ and all intermediate iterates

$$(g_{\varepsilon_m})^l \circ (g_{\varepsilon_{m+1}})^{k_{m+1}} \circ \cdots \circ (g_{\varepsilon_M})^{k_M}(z'), \quad \begin{cases} m = 0, \ldots, M, \\ l = 0, \ldots, k_m \end{cases}$$

remain T-far from 0. Obviously, the corresponding loop is in the same leaf ($\tilde{g} \in G$) and may be thought, in the fundamental group of the leaf, as a product of the initial one with another loop having trivial holonomy; they are even not cohomologous in general. The new word g' may be obtained as follows.

Start with a word decomposition of g like above. Denote by $h, h' \in G$ two translations that are $\mathbb{R}$-independant in G (the linear part of G is not real) together with a word decomposition. Consider also $\tilde{h} = g \circ h \circ g^{-1}$. Since $z = \infty$ is fixed by the generators g_1 and g_{-1}, there is a sequence $\cdots > T_n > \cdots > T_1 > T_0 = T$ such that any point z' outside the T_{n+1}-ball remains T_n-far from 0 after one iteration of g_1, g_{-1}, g_1^{-1} or g_{-1}^{-1}. Choose $T' := T_n$ for a n bounding the length of the words g, h, h' and $\tilde{h}$. Therefore, if z' is T'-far from 0, then its orbit under iteration or g, h, h' and $\tilde{h}$ (or one of the inverses) does not intersect the T-ball.

Now, we choose a large translation h^N such that $z' = h^N(z)$ and its image $z'' = g(z')$ are T'-far from 0. Notice that the new transformation $g' = h^{-N} \circ g \circ h^N$ fixes z' and admits the word decomposition $g' = h^{-N} \circ \tilde{h}^N \circ g$. By construction, the iteration of word g on z' remains T-far from 0. Also, if the sequence

$$z'', \tilde{h}(z''), \ldots, \tilde{h}^N(z''), h^{-1} \circ \tilde{h}^N(z''), \ldots, h^{-N} \circ \tilde{h}^N(z'') = z'$$

does not intersect the T'-ball, then the *full orbit of z'' under $h^{-N} \circ \tilde{h}^N$ viewed as a word in g_1 and g_{-1}* will stay T-far from 0.

If not, then we can use the commutativity of h, h' or $\tilde{h}$ to re-arrange the word $h^{-N} \circ \tilde{h}^N$. For instance, when h and $\tilde{h}$ are $\mathbb{R}$-independant, this follows from the fact that the T'-ball cannot disconnect the "lattice"

$$L = (z'' + \mathbb{R} \cdot h + \mathbb{Z} \cdot \tilde{h}) \cup (z'' + \mathbb{Z} \cdot h + \mathbb{R} \cdot \tilde{h}) \in \mathbb{C}.$$

The word $h^{-N} \circ \tilde{h}^N$ corresponds to a path in L joining z'' to its image $z' = h^{-N} \circ \tilde{h}^N(z'')$. If this path crosses the T'-ball, then it can be replaced by another path in L avoiding this ball. When h and $\tilde{h}$ are $\mathbb{R}$-dependant, then we introduce h' and use the lattice generated by h and h'. This ends the proof of the last claim, as well as the corollary. □

Acknowledgement. We would like to thank the referee who carefully read our paper and motivated us to provide Corollary 1 as a concrete application (with a full proof).

The answer to the first question

Consider a subgroup $G < \mathrm{Aff}(\mathbb{C})$ given by generators

$$G = \langle a_i X + b_i;\ i = 1, \dots, s \rangle.$$

Let $\lambda\colon \mathrm{Aff}(\mathbb{C}) \to \mathbb{C}^*;\ aX + b \mapsto a$ be the group homomorphism giving the linear part. Denote by $\Lambda := \lambda(G)$ the linear part of G and by $T := \ker(\lambda\colon G \to \Lambda)$ its translation part. We have

$$\Lambda = \langle a_i;\ i = 1, \dots, s \rangle \subset \mathbb{C}^*.$$

One can identify T to a subgroup of $\mathbb{C}$ (still denoted by T):

$$T = \{b;\ X + b \in G\} \subset \mathbb{C}.$$

From the action of G by conjugacy on its normal subgroup T, we see that T is stable under multiplication by elements of Λ and therefore inherits a structure of module over the ring $\mathbb{Z}[\Lambda]$. In the sequel we will suppose that both Λ and T are non-trivial, otherwise the two questions we are concerned with become trivial.

We take care that, in general, T is not a finitely generated subgroup of G, but we note that it is finitely generated as a normal subgroup of G. In other words, we claim that T is a finitely generated module over $\mathbb{Z}[\Lambda]$ (having rank $\leq \frac{s(s+1)}{2}$). Indeed, the commutator subgroup $G' = [G, G]$ of G is the subgroup of T generated by all conjugates of the elementary commutators $[a_i X + b_i, a_j X + b_j]$, $i, j = 1, \dots, s$, $i \neq j$ in G. The group G' is thus generated as normal subgroup of G (or, equivalently, as a module over $\mathbb{Z}[\Lambda]$) by those $\frac{s(s-1)}{2}$ elements. In order to generate T, it suffices to add a set of generators for the quotient T/G'. Since G/G' is a commutative group of rank $\leq s$, its subgroup T/G' has also rank $\leq s$.

We observe that the map $c \in \mathbb{C} \to G^{\{c\}} = \{g \in G;\ g(c) = c\}$ induces a bijection between $\mathrm{Fix}(G)$ and the set of the maximal commutative subgroups H of G with $H \neq T$. Since $G^{\{g(c)\}} = gG^{\{c\}}g^{-1}$, one obtain a bijective correspondance

$$\mathrm{Fix}(G)/G \longleftrightarrow \{H < G \text{ maximal commutative subgroup},\ H \neq T\}/G$$

with the G-conjugacy classes of such subgroups H. The image $\lambda(H) \subset \Lambda$ depends only on the G-conjugacy class of H.

Theorem 2. *With notations above, the set* $\mathrm{Fix}(G)/G$ *is finite if, and only if, the linear part* Λ *of* G *is a finite subgroup of* $\mathbb{C}^*$.

Proof: Suppose that Λ is finite. Then $\Lambda = \langle \zeta_n \rangle$ where ζ_n denotes a primitive n^{th} root of unity and $\mathbb{Z}[\Lambda]$ is equal to the ring of integers $\mathbb{Z}[\zeta_n]$ in $\mathbb{C}$. Given a generator $g \in G$ for Λ, $g = \zeta_n X + t$, one may linearize it by a translation and assume without loss of generality that Λ is contained as a linear subgroup in G. Therefore, any element of G writes $g = \zeta_n^i X + t$, $t \in T$ and we have

$$\mathrm{Fix}(G) = \bigcup_{i=1}^{n-1} \frac{1}{1-\zeta_n^i} T.$$

The set of T-orbits of $\frac{1}{1-\zeta_n^i}T$ is equal to the finitely generated module $T/(1-\zeta_n^i)T$ over the finite ring $\mathbb{Z}[\zeta_n]/(1-\zeta_n^i)$. Thus $\mathrm{Fix}(G)/G$ is finite. The other implication of Theorem 2 follows from the next lemma. □

Lemma 3. *Suppose that* Λ *is infinite. Then there are infinitely many subgroups of* Λ *of the form* $\lambda(H)$, *where* $H \neq T$ *is a maximal commutative subgroup of* G.

Proof: Let $a \in \Lambda$ be an element of infinite order. After conjugation of G by an element of $\mathrm{Aff}(\mathbb{C})$, we may suppose that aX lies in G. Choose an integer $m > 1$. In fact, we prove that, for any integer $m > 1$, there exists a maximal commutative subgroup $H \neq T$ of G such that $\lambda(H)$ contains some power of a but $a^i \notin \lambda(H)$ for $i = 1, \ldots, m$. The lemma will follow from this.

The ring $\mathbb{Z}[\Lambda, \frac{1}{(a-1)(a^2-1)\cdots(a^m-1)}]$ is finitely generated over $\mathbb{Z}$. Therefore there exists a surjective homomorphism ϕ to a finite field $\mathbb{F}_q$. Set $\alpha := \phi(a)$. Then $\alpha^i \neq 1$ for $i = 1, \ldots, m$ and $\alpha^{q-1} = 1$. Let $I \subset \mathbb{Z}[\Lambda]$ denote the ideal generated by the elements $\frac{a^{q-1}-1}{a^d-1}$ for $d \mid q-1$ and $1 \leq d \leq m$. This is a proper ideal of $\mathbb{Z}[\Lambda]$: $a^d - 1 \notin I$ since $\phi(a^d - 1) \neq 0$ and ϕ sends I to 0 ($\phi(a^{q-1} - 1) = 0$). There exists an element $t \in T \setminus IT$. Indeed, suppose that $IT = T$. Let $\underline{m}$ be a maximal ideal of $R := \mathbb{Z}[\Lambda]$ containing I, so $\underline{m}T = T$. After localization with respect to $S := R \setminus \underline{m}$, one finds that $B := S^{-1}T$ is a finitely generated module over the noetherian local ring $S^{-1}R$ such that $\underline{m}B = B$. This implies that $B = 0$ (Nakayama's lemma) [**La**]. Since the elements of S are not zero divisors on T, one obtains the contradiction that $T = 0$.

Finally, let H be a maximal commutative subgroup containing $h := a^{q-1}X + t$. Let $d \geq 1$ be minimal such that $a^d \in \lambda(H)$. Since we have also $a^{q-1} \in \lambda(H)$, then $d \mid q-1$. It follows that H contains an element

of the form $k := a^d X + b$ with $b \in T$ since $aX \in G$. Now $k^{\frac{q-1}{d}} = h$ (if not, there exists a non-trivial translation in H which is a contradiction since H is commutative) and thus $t = \frac{a^{q-1}-1}{a^d-1} b$. This implies that $d > m$ and H has the required properties. □

The answer to the second question

We have to consider a group G generated by a finite linear subgroup $\langle \zeta_n X \rangle$ of order n and by a translation subgroup $\{X + t;\, t \in T\}$ where $T \subset \mathbb{C}$ is a finitely generated $\mathbb{Z}[\zeta_n]$-module of rank r. We note that the module T has no torsion and thus T is a projective $\mathbb{Z}[\zeta_n]$-module. For the computation of $\#\operatorname{Fix}(G)/G$, we start with two examples.

Example 1. *Assume that $n = p^{k+1}$ with p prime and $k \geq 0$.* As in the beginning of the proof of Theorem 2, one may assume without loss of generality that any element of G writes $g = \zeta_n^i X + t$, $t \in T$. If $g \in G$ has a fixed point ($g \notin T$), then a convenient iterate $g \circ g \circ \cdots \circ g$ has linear part ζ_p with the same fixed point. Therefore, we have

$$\operatorname{Fix}(G) = \frac{1}{1-\zeta_p} \cdot T$$

and we may consider

$$\operatorname{Fix}(G)/T \simeq T/(1-\zeta_p)T$$

as a module over the ring $\mathbb{Z}[\zeta_{p^{k+1}}]/(1-\zeta_p)$. We have to count the number of Λ-orbits on $T/(1-\zeta_p)T$, where $\Lambda = \langle \zeta_{p^{k+1}} \rangle$. First, we have

$$\mathbb{Z}[\zeta_{p^{k+1}}]/(1-\zeta_p) \simeq \mathbb{Z}[X]/(\Phi_{p^{k+1}}(X), X^{p^k} - 1),$$

where $\Phi_n = \frac{X^{p^{k+1}}-1}{X^{p^k}-1} = X^{(p-1)p^k} + \cdots + X^p + 1$ denotes the n^{th} cyclotomic polynomial. The ideal is also generated by p and $X^{p^k} - 1$. After substitution $X = 1 + Y$, one finds that

$$\mathbb{Z}[\zeta_{p^{k+1}}]/(1-\zeta_p) \simeq \mathbb{F}_p[Y]/(Y^{p^k}).$$

In particular, the ideal $(1-\zeta_p)$ is contained in only one maximal ideal, say $\underline{m}$. Let S be the multiplicative system $S := \mathbb{Z}[\zeta_{p^{k+1}}] \setminus \underline{m}$. Then $S^{-1}T$ is a free module of rank r over the local ring $S^{-1}\mathbb{Z}[\zeta_{p^{k+1}}]$. Since $T/(1-\zeta_p)T$ is isomorphic to $S^{-1}T/(1-\zeta_p)S^{-1}T$, one has that $T/(1-\zeta_p)T$ is a free module of rank r over $\mathbb{Z}[\zeta_{p^{k+1}}]/(1-\zeta_p)$ and we can identify

$$T/(1-\zeta_p)T \simeq \left(\mathbb{F}_p[Y]/(Y^{p^k})\right)^r.$$

We have to count the number of Λ-orbits on $\left(\mathbb{F}_p[Y]/(Y^{p^k})\right)^r$ where Λ is the cyclic group of order p^k generated by $(1+Y)$ modulo (Y^{p^k}).

The set $\mathrm{Fix}(G)/T \simeq \left(\mathbb{F}_p[Y]/(Y^{p^k})\right)^r$ splits into the disjoint union of

$$C(p^s) = \left\{c \in \left(\mathbb{F}_p[Y]/(Y^{p^k})\right)^r ;\ \text{the } \Lambda\text{-orbit of } c \text{ has length } p^s\right\}$$

for $s = 0, \ldots, k$. On the other hand, one observes that the set of orbits having length at most p^s is given by $\sqcup_{i=0}^{s} C(p^i) = \left(Y^{p^{k-s}}\mathbb{F}_p[Y]/(Y^{p^k})\right)^r$ and thus

$$\sum_{i=0}^{s} \#C(p^i) = \#\left(Y^{p^{k-s}}\mathbb{F}_p[Y]/(Y^{p^k})\right)^r = p^{rp^s}.$$

One concludes that $C(p^s)$ contains exactly p^r orbits if $s = 0$ and $\frac{p^{rp^s} - p^{rp^{s-1}}}{p^s}$ orbits for $s = 1, \ldots, k$. This leads to the formula

$$\#\,\mathrm{Fix}(G)/G = p^r + \sum_{s=1}^{k} \frac{p^{rp^s} - p^{rp^{s-1}}}{p^s}.$$

Example 2. *Assume that $n = p^{k+1}q^{l+1}$ with distinct primes p, q and $k, l \geq 1$.* Let $T \subset \mathbb{C}$ be a finitely generated $\mathbb{Z}[\zeta_{p^{k+1}q^{l+1}}]$-module of rank r and let $G \subset \mathrm{Aff}(\mathbb{C})$ be the group generated by $\zeta_{p^{k+1}q^{l+1}}X$ and $\{X+t;\ t \in T\}$. As in Example 1, the fixed point of a non-trivial element $g \in G \setminus T$ is also the fixed point of a convenient iterate of g having ζ_p or ζ_q as linear part. Therefore,

$$\mathrm{Fix}(G) = \frac{1}{1-\zeta_p}T \bigcup \frac{1}{1-\zeta_q}T.$$

The intersection of these two sets is T. Indeed, $\frac{a}{1-\zeta_p} = \frac{b}{1-\zeta_q}$ implies $(1-\zeta_p)b = (1-\zeta_q)a$. Since the image of $(1-\zeta_q)$ in $\mathbb{Z}[\zeta_{p^{k+1}q^{l+1}}]/(1-\zeta_p)$ is invertible, one has that a is divisible in T by $(1-\zeta_p)$. Let N_p, N_q denote the respective numbers of Λ-orbits on the set of the non-zero elements of $\frac{1}{1-\zeta_p}T/T$ and $\frac{1}{1-\zeta_q}T/T$. Then

$$\#\,\mathrm{Fix}(G)/G = 1 + N_p + N_q.$$

Now we concentrate on the counting of N_p. The natural homomorphism

$$\mathbb{Z}[\zeta_{p^{k+1}}] \otimes \mathbb{Z}[\zeta_{q^{l+1}}] \longrightarrow \mathbb{Z}[\zeta_{p^{k+1}q^{l+1}}]$$

is an isomorphism. The same arguments as in Example 1 yield

$$\mathbb{Z}[\zeta_{p^{k+1}q^{l+1}}]/(1-\zeta_p) \simeq \mathbb{F}_p[Y]/(Y^{p^k}) \otimes \mathbb{F}_p[X]/(\Phi_{q^{l+1}}).$$

It is known [**LN**] that the ring $\mathbb{F}_p[X]/(\Phi_{q^{l+1}})$ is a product of copies of the field $\mathbb{F}_{p^m}$ where $m \geq 1$ is minimal such that $q^{l+1} \mid p^m - 1$. In particular, the image of $1-\zeta^i_{q^{l+1}}$ in $\mathbb{Z}[\zeta_{p^{k+1}q^{l+1}}]/(1-\zeta_p)$ is invertible for $i = 1, \ldots, q^{l+1}-1$. As before

$$\frac{1}{1-\zeta_p} T/T \simeq \left(\mathbb{F}_p[Y]/(Y^{p^k}) \otimes \mathbb{F}_p[X]/(\Phi_{q^{l+1}})\right)^r.$$

The orbit of any non-zero element in this set has length $p^s q^{l+1}$ with $s \in \{0, \ldots, k\}$. Indeed, the image of $\zeta^i_{q^{l+1}} - 1$ in $\mathbb{Z}[\zeta_{p^{k+1}q^{l+1}}]/(1-\zeta_p)$ is invertible for all $i = 1, \ldots, q^{l+1}-1$. Let $C(p^s q^{l+1})$ denote the set of the elements having an orbit of length $p^s q^{l+1}$. Then one has, like before,

$$\sum_{s=0}^{m} \#C(p^s q^{l+1}) = p^{r\varphi(q^{l+1})p^m} - 1 \quad \text{for} \quad m = 0, \ldots, k$$

where φ denotes the Euler function.

Note that the -1 is due to omitting 0 in $\frac{1}{1-\zeta_p} T/T$. This implies that the number of Λ-orbits of length $p^s q^{l+1}$ is

$$\frac{p^{r\varphi(q^{l+1})} - 1}{q^{l+1}} \quad \text{if} \quad s = 0$$

and

$$\frac{p^{r\varphi(q^{l+1})p^s} - p^{r\varphi(q^{l+1})p^{s-1}}}{p^s q^{l+1}} \quad \text{for} \quad s = 1, \ldots, k.$$

From this one derives a formula for N_p. The case N_q is similar and one arrives at

$$\begin{aligned} \#\operatorname{Fix}(G)/G = 1 &+ \frac{p^{r\varphi(q^{l+1})} - 1}{q^{l+1}} + \sum_{s=1}^{k} \frac{p^{r\varphi(q^{l+1})p^s} - p^{r\varphi(q^{l+1})p^{s-1}}}{p^s q^{l+1}} \\ &+ \frac{q^{r\varphi(p^{k+1})} - 1}{p^{k+1}} + \sum_{s=1}^{l} \frac{q^{r\varphi(p^{k+1})q^s} - q^{r\varphi(p^{k+1})q^{s-1}}}{q^s p^{k+1}}. \end{aligned}$$

The general case is done in a similar way and one obtains the formula:

Theorem 4. *With notations above, let the group $G < \operatorname{Aff}[\mathbb{C}]$ be generated by a finite linear group $\Lambda = \langle \zeta_m X \rangle$ of order m and a translation group $\{X + t;\, t \in T\}$ where T is a $\mathbb{Z}[\zeta_m]$-module of rank r. Then*

$$\#\operatorname{Fix}(G)/G = 1 + \sum_{j=1}^{t} \left\{ \frac{p_j^{r\varphi(m_j)} - 1}{m_j} + \sum_{s=1}^{k_j} \frac{p_j^{r\varphi(m_j)p_j^s} - p_j^{r\varphi(m_j)p_j^{s-1}}}{p_j^s m_j} \right\}$$

where m has prime decomposition $m = p_1^{k_1+1} \cdots p_t^{k_t+1}$ and $m_j := m/p_j^{k_j+1}$.

References

[G] C. Godbillon, *"Feuilletages. Études géométriques"*, with a preface by G. Reeb, Progress in Mathematics **98**, Birkhäuser Verlag, Basel, 1991.

[H] E. Hille, *"Ordinary differential equations in the complex domain"*, reprint of the 1976 original, Dover Publications, Inc., Mineola, NY, 1997.

[La] S. Lang, *"Algebra"*, second edition, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1984.

[LN] R. Lidl and H. Niederreiter, *"Finite fields"*, with a foreword by P. M. Cohn, second edition, Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press, Cambridge, 1997.

F. Loray:
(C.N.R.S.) I.R.M.A.R.
Université de Rennes 1
Campus de Beaulieu
35042 Rennes Cedex
France
E-mail address: frank.loray@univ-rennes1.fr

M. van der Put:
Vakgroep Wiskunde
Rijksuniversiteit Groningen
Postbus 800
9700 Av Groningen
Nederland
E-mail address: M.van.der.Put@math.rug.nl

F. Recher:
Laboratoire A.G.A.T.
U.F.R. de Mathématiques
Université de Lille 1
Cité Scientifique
59655 Villeneuve d'Ascq Cedex
France
E-mail address: recher@univ-lille1.fr

Primera versió rebuda el 21 de març de 2003,
darrera versió rebuda el 29 d'octubre de 2003.