Remarks on J. Langer and D. A. Singer Decomposition Theorem for Diffeomorphisms of the Circle

R. de la Llave

Department of Mathematics, Fine Hall, Princeton University, Princeton, New Jersey 08544, USA

Abstract. We give a simple proof that all C^4 diffeomorphisms of the torus can be factorized into a finite number of diffeomorphisms commuting with reflection.

In one dimension, C^3 suffices and even C^2 can yield that the factors are almost diffeomorphisms. (The derivatives of the function and the inverse are in L^1 and are positive.)

In one dimension under C^∞ assumptions, this had been proved by J. Langer and D. A. Singer in their study of geodesic fields by different methods.

1. Introduction

J. Langer and D. A. Singer proved in [1] that $\mathrm{Diff}_+(S^1)$—the group of C^∞ orientation preserving diffeomorphisms of the circle—is generated by symmetric diffeomorphisms; that is, every C^∞ diffeomorphism is the composition of a finite number of diffeomorphisms that commute with reflections. (Taking $S = \mathbb{R}/\mathbb{Z}$, a reflection about θ is $R_\theta(x) = -(x - \theta) + \theta \pmod 1$, $f: S^1 \to S^1$ commutes with reflections if $f \circ R_\theta = R_\theta \circ f$.)

The interest of this theorem for the authors above was that, in the same paper, they showed it implies that given any orientation preserving C^∞ diffeomorphism f, there is a C^∞ gradient flow in the annulus that sends the point θ in the inner boundary to $f(\theta)$ in the outer boundary; this in turn, can be used to characterize which transformations in rays can be achieved through geodesic flows in conformal metrics; in more physical terms, they characterize the transformations that can be achieved by isotropic lenses (scalar index of refraction) in 2-*D*. Other applications are also possible. Since the conformal group in two dimensions (indefinite metric) is just the product of two diffeomorphism groups of the circle, it suffices to show invariance under changes that commute with reflections to show conformal invariance.

The object of this note is to provide a different and simpler proof of the result that works with weaker differentiability assumptions and obtains stronger differentiability in the factors.

   In distinction to the proof in [1] our proof is not based on rapidly convergent iterations but, rather, we reduce it to a sequence of steps that can be accomplished by a method of proof introduced by M. Herman [2, 3] to improve the differentiability conditions of the local Arnold theorem on conjugacy of diffeomorphisms to rotations and of J. Moser's twist mapping theorem. This method was also shown in [4] to yield good numerical values of the stability domains in C. Siegel center theorem.

   We first show that all diffeomorphisms close to the identity can be written as the composition of a rotation and two diffeomorphisms symmetric about two different axis. (We call this the reduction theorem.) Afterwards, we show that rotations can be also expressed as compositions of diffeomorphisms symmetric about the same axis. To show that rotations can be decomposed in this way we just apply a strong version of the reduction theorem—including uniqueness—to a carefully chosen family.

   For the first application of the reduction theorem, uniqueness plays no role and it is possible to give a proof that does not include uniqueness in the conclusions but which uses one derivative less. For the decomposition of rotations, derivatives in the hypothesis are no burden. Since the theorem including uniqueness is simpler to prove, we do it first.

   Both theorems can be proved by Herman's strategy: write a carefully chosen functional equation, take derivatives and logarithms—so that compositions become simpler—and treat the resulting equation as a fixed point problem; the version without uniqueness is obtained using Schauder fixed point theorem in the last stage and the one with uniqueness using the contraction mapping principle.

   One we have decomposition in a small ball, around the identity, extending it to all $\text{Diff}_+(S^1)$ is a simple argument in a point set topology.

   Notice that taking logarithms only makes sense in 1-dimension—and, besides, in setting up the fixed point theorem we will have to assume number theoretic properties which only hold for n-tuples when $n = 1$ (and then only in a set measure zero). So, this strategy is quite linked to 1-dimension. Nevertheless, we show that some multi-dimensional generalizations are possible by reducing the problem to a sequence of one dimensional problems. This requires use of the implicit function theorem in place of contraction mapping—so as to obtain smooth dependence on parameters in the previous results—and requires one derivative more.

   Unfortunately, those multidimensional results are not enough to derive analogues of Langer and Singer geometric results in higher dimensions; we prove them for T^d and, the geometric results would require S^d which, of course, is different when $d \neq 1$, but maybe it will be possible to remove this shortcoming.

   More precisely, the main theorem we want to prove is the following.

Main Theorem. *There exists a number ρ such that all C^r $r \geq 2$ orientation preserving diffeomorphisms of the circle can be written as composition of a finite number of factors that commute either with R_0 or R_ρ. When $r > 2$, the factors can be chosen among C^{r-2} diffeomorphisms, and when $r = 2$ they can be chosen so that they and their inverses have positive weak derivatives in L^p, all $1 \leq p < \infty$.*

2. Preliminaries and Notation

Since $S^1 = \mathbb{R}/\mathbb{Z}$, all maps of $\mathbb{R}$ to itself satisfying

$$f(x+1) = f(x) + 1 \tag{1}$$

can be thought of as maps of the circle to itself. Since we are going to be concerned mainly with maps close to the identity, we can decide unambiguously which map of the real line represents a map of the circle and we will, therefore, identify two such objects even without saying it explicitly.

The space of maps satisfying 1 can also be thought of as the affine space obtained adding to the identity a space of periodic functions. We will find useful the following spaces of periodic functions. (We will systematically use the notation $\hat{f} = f - \text{Id}$.)

$$H^r = \{f \mid \|f\|_r^2 = |f_0|^2 + \sum_{k \in \mathbb{Z}} |f_k|^2 (2\pi k)^{2r} < \infty\},$$

where f_k is the k-th Fourier coefficient of f, $f(x) = \sum_{k \in \mathbb{Z}} f_k e^{2\pi i k x}$. When r is an integer — the only case we are going to consider —

$$\|f\|_r^2 = \left| \int_0^1 f \right|^2 + \|f^r\|_{L^2},$$

where f^r is the r-th distribution derivative of f.

All H^r are Hilbert spaces with the obvious scalar product.

We will repeatedly use the following facts:

i) H^r is embedded in C^{r-1} for $r \geq 1$. This embedding is compact. On the unit ball of H^r the weak topology of H^r and the topology induced by C^{r-1} coincide.

ii) If $f, g \in H^r$, $r \geq$, then $f \cdot g \in H^r$ and

$$\|f \cdot g\|_r < K_r \|f\|_r \|g\|_r.$$

iii) If $f, g \in H^r$, $r \geq 2$, $\|g\|_r \leq 1/2$

$$\|f \circ (g + \text{Id})\| \leq K'_r \|f\|_r.$$

We give the proof of iii) for $r = 2$. The other cases are similar,

$$f \circ (g + \text{Id})'' = f'' \circ (g + \text{Id})(g' + 1)^2 + f' \circ (g + \text{Id})g'',$$

$$\|f'' \circ (g + \text{Id})(g' + 1)^2\|_{L^2}^2 = \int_0^1 |f'' \circ (g + \text{Id})|^2 (g' + 1)(g' + 1)^3$$

$$\leq \sup |(g' + 1)|^3 \int_{\text{range}(g + \text{Id})} |f''|^2,$$

$$\|f' \circ (g + \text{Id})g''\|_{L^2} \leq \|g''\|_{L^2} \sup |f'|,$$

and these terms can all be bounded uniformly by a constant times $\|f\|_r$. The other terms with the integrals are easier.

This inequality is one of the elements of the proof that are not known in higher dimensions even if there are some weaker forms.   □

(See [9] p. 67 ff and references there for a survey of results on composition of diffeomorphisms with Sobolev regularity.)

iv) If $r \geqq 2$, there is an H^r neighborhood U of the identity such that all functions in it are invertible and, moreover, the H^r norm of all the inverses of functions in U is bounded.

Proof of iv). We construct the inverse of a function by integrating the derivatives $(f^{-1})' = 1/f' \circ f$. Since f' is bounded away from zero uniformly for $f \in U$, we can see by the same argument used for diffeomorphisms that the r-th derivatives of f^{-1} exists and its L^2 norm is bounded.

Unfortunately, it is not true that an H^1 neighborhood of the identity has only invertible elements, as can easily be seen.

v) If $m \in C^{r+l+1}$, r, $l \in \mathbb{N}$ the map $\tau: H^r \to H^r$ defined by $h \to m \circ h$ is of class C^l. Moreover, when h ranges in a bounded set

$$\| D\tau(h) \| \leqq \| m \|_{C^{r+1}} K.$$

Proof of v). We will prove the statement for $l = 1$ and that the derivative is multiplication by $m' \circ h$. Hence, the full result follows by induction in l.

It suffices to show that

$$\| m \circ (h + \Delta) - m(h) - (m' \circ h) \Delta \|_{H_r} \leqq K \| m \|_{C^{r+1}} (\| \Delta \|_{H^r})^2.$$

For $r = 1$, taking the derivatives

$$m' \circ (h + \Delta)(h + \Delta)' - m' \circ hh' - m'' \circ hh' \Delta - (m' \circ h) \Delta'$$
$$= h'(m' \circ (h + \Delta) - m' \circ h - m'' \circ h\Delta) + \Delta'(m' \circ (h + \Delta) - m' \circ h),$$

and it suffices to bound the L^2 norm of this by $(\| \Delta \|_{H^r})$. Now, the second factor in the first term is bounded in C^0 by $2 \| m \|_{C^2} (\| \Delta \|_{H^0})$ in turn is bounded by $\| \Delta \|_{H^1}$. The second factor in the second term is bounded in the supremum norm and Δ' is bounded in the L^2 norm both by $\| \Delta \|_{H^2}$.

By induction in r we can show that, taking the r-th derivative, the only term containing Δ^r is

$$\Delta^{(r}(m' \circ (h + \Delta) - m' \circ h)$$

whose L^2 norm can be bounded.

Since we are in 1 dimension, we can bound the supremum norm of all other derivatives by $\| \Delta \|_{H^r}$, and all the other terms appearing are bounded in the same way as when one wants to prove this theorem by C^r rather than H^r.

Remark. When h ranges over a bounded set in H^r this implies uniform bounds for $|h|$. The norms of m need only be taken over that set.

Remark. From this, it also follows that if f ranges over a bounded H^{r+1} neighborhood, the application Inv: $H^r \to H^r$ sending $f \to f^{-1}$ is differentiable. Indeed, the differential is

$$[(D \operatorname{Inv})_F] \alpha = - \frac{\alpha \circ \operatorname{Inv} F}{F' \circ \operatorname{Inv} F} = - \left(\frac{\alpha}{F'} \right) \circ \operatorname{Inv} F.$$

If a diffeomorphism of the circle commutes with reflections about 0, the function representing it should be odd about zero, that is: $f(x) = -f(-x)$.

In Fourier coefficients, this means $\hat{f}_k = -\hat{f}_{-k}$ for all k. More generally, if a diffeomorphism commutes with a reflection about an axis going through ρ, the Fourier coefficients would satisfy

$$a^k \hat{f}_k = -a^{-k}\hat{f}_{-k} \quad \text{for all } k,$$

where $a = \exp(2\pi i\rho)$.

We denote by O_ρ^r the space of functions odd about ρ which are in H^r. It is a closed subspace.

The Fourier coefficients of even functions about ρ satisfy

$$a^k \hat{f}_k = a^{-k}\hat{f}_{-k}.$$

We will denote by E_ρ^r the space of functions even about ρ which are in H^r. It is also a closed subspace.

The derivative of an odd function is even and the derivative of an even function is odd. All primitives of odd functions are even and each even function has one and only one primitive which is odd. Any function of an even function is even.

The other ingredient of this proof is—as in [1]—the fact that the separation of the two axis which we make reflections is not well approximated by rationals.

The separations we can use in our proof are those given by numbers of constant type. That is, those numbers ρ satisfying

$$|\rho - p/q|^{-1} \leqq \gamma q^2 \quad \text{for all} \quad p, q \in \mathbb{Z} \text{ and some } \gamma > 0.$$

An immediate consequence of this is that, when

$a = \exp(2\pi i\rho)$ and ρ is of constant type, we have
$|a^{2k} - 1|^{-1} \leqq Ck.$

More delicate is the following estimate that we will use in Theorem 3,

$$\left(\sum_{N \leqq |k| \leqq 2N} \frac{1}{|k(1 - a^{2k})|^p} \right)^{1/p} \leqq C_p \quad \begin{array}{l} \text{for all } p > 1 \\ \text{and all } N > 0. \end{array}$$

Notice that this is much stronger than what one could hope if the inequalities defining a number of constant type were saturated all the time. However, using the pigeon-hole principle one realizes that these inequalities are saturated very rarely. We refer to [2] and [5] to find a proof.

This condition of separation from rationals is extremely strong. In contrast to the conditions used in [1], which hold for a set of numbers of full measure, it holds only for a set of numbers of measure zero. However, for the present purposes, this is no restriction. In [5] it is possible to find a discussion of properties of these constant type numbers including their abundance.

3. The Reduction Theorem

As was said in the introduction we start by proving a version of the theorem that includes uniqueness among its conclusions.

Theorem 1 (Reduction theorem; first version). *Let $r \geq 2$ be fixed and ρ be a number of constant type, let also A_1 and A_2 be two diameters of the circle forming an angle of $2\pi\rho$ radians. (We will give the circle a system of coordinates so that A_1 goes through 0 and A_2 through ρ).*

If $f: \mathbb{R} \to \mathbb{R}$ is a C^{r+2} function satisfying

$$f(x+1) = f(x) + 1, \quad \| \hat{f} \|_{C^{r+2}} < \varepsilon_0,$$

ε_0 *a number to be determined later.*

Then, there exist two diffeomorphisms u, v of the circle of class H^r and a real number θ so that
(*)
$$u \circ v \circ f(x) = x + \theta,$$

$$u, v \quad \text{commute with reflections about } A_1, A_2 \text{ respectively.}$$

Moreover,

– There exists a B so that u, v can be chosen

$$\| \hat{u} \|_{H^r} \leq B\varepsilon, \quad \| \hat{v} \|_{H^r} \leq B\varepsilon.$$

– u, v, θ are determined uniquely by the preceding properties.
– In case $f \in C^{r+l+2}$, the function that associates to each f, (u, v, θ) is of class C^l.

Remark. Notice that if we were to use an iteration method, it would be much more convenient to try to solve

$$u \circ f \circ v(x) = x + \theta$$

which, however is unsuitable for this strategy.

Proof of Theorem 1. We observe that satisfying (*) is the same thing as satisfying (notice that the derivatives exist pointwise, but this formula is also right if the derivatives exist in weak sense)

$$u' \circ v \circ f(x) v' \circ f(x) f'(x) = 1.$$

Taking logarithms, this becomes

$$(\log u') \circ v \circ f(x) + (\log v') \circ f(x) + \log f'(x) = 0.$$

Writing $x = f^{-1} \circ v^{-1}(y)$, this becomes

$$\log u'(y) - \log(v^{-1})'(y) = \log(f^{-1})' \circ v^{-1}(y). \tag{2}$$

A moment's reflection will show that, a solution of (2) is a solution of (*) and that, since all diffeomorphisms of the circle have derivative strictly bigger than 0, taking logarithms is allowed on all solutions of (*) and so, (*) and (2) are actually equivalent.

To simplify the notation we will call $\log(f^{-1})'$ just m. What we want to do is to check that, under suitable assumptions of smallness in m (which are implied by closeness of f to the identity) (2) has a solution, unique in a certain region, and all the other conclusions.

The way of solving Eq. 2 is to introduce the operator $\mathcal{T}$ that, given a function $h \in I + E_0^r$ produces the only function (we will prove the appropriate uniqueness statement) $l \in I + E_0^r$, satisfying

$$\log(l')(x) + m \circ h(x) = s(x) \in E_\rho^{r-1}.$$

We will show that this operator is a contraction and, therefore has a fixed point v. From this fixed point (and the corresponding s) we can construct a solution of (∗). The other properties will follow from a careful reading of the proof.

$\mathcal{T}$ will be constructed step by step, keeping good track of the constants. In this construction we will need the following

Lemma 1. *Let ρ be a number of constant type.*

If f is a function belonging to H^r, $r \geq 1$, then there are two functions u, v belonging to E_ρ^{r-1}, E_0^{r-1} satisfying $u + v = f$.

Moreover, these functions are unique up to constants (which obviously have the constraint $\int u + \int v = \int f$), and we have

$$\| u - \textstyle\int u \|_{H^{r-1}} \leqq C \| f \|_{H^r}, \quad \| v - \textstyle\int v \|_{H^{r-1}} \leqq C \| f \|_{H^r}.$$

For convenience, we will denote the map sending f to $v - \int v$ by P_0.

Proof of Lemma 1. If we take Fourier coefficients, the equation is just $u_k + v_k = f_k$.

When k is not equal to zero, the equation for $-k$ is different, but, using the symmetry relations, it contains the same unknowns, $a^{2k} u_k + v_k = f_{-k}$. These two equations can be solved to give

$$u_k = (-f_k + f_{-k})/(1 - a^{2k}), \quad v_k = (-a^{2k} f_k + f_{-k})/(1 - a^{2k}).$$

Using the inequalities for the rational approximations of ρ we get,

$$|u_k| \leqq (|f_k| + |f_{-k}|) Ck, \quad |v_k| \leqq (|f_k| + |f_{-k}|) Ck.$$

From which all the conclusions of the lemma follow.   □

It is clear now, how to construct $\mathcal{T}$. Given h, we compose it with m. Then, apply Lemma 1 to produce $\log l'$ (up to a constant), exponentiate to obtain l' up to a factor and then, find the only primitive of this function which is odd. The "miracle" is that this last step restores the derivative we had lost in applying Lemma 1. We fix uniquely the arbitrary factor in such a way that the result is a diffeomorphism of the circle (that is, l' should integrate to 1).

The reason why this operator should be a contraction under smallness assumptions in m is because the last three steps have well defined Lipschitz constants (provided that we only consider bounded sets) and the Lipschitz constant of the first can be made arbitrarily small by imposing smallness conditions in m.

More precisely, we have:

$$\mathcal{T}_1 : V \subset I + O_0^r \to H^r; \quad \mathcal{T}_1 h = m \circ h,$$

$$\mathcal{T}_2 : H^r \to E_0^{r-1} : \mathcal{T}_2 = P_0 \text{ as in Lemma 1,}$$

$$\mathcal{T}_3 : E_0^{r-1} \to E_0^{r-1} : \mathcal{T}_3 h(x) = \exp h(x),$$

$$\mathcal{T}_4 : E_0^{r-1} \to I + O_0^r : \mathcal{T}_4 h(x) = \frac{\int\limits_0^x h(y)\, dy}{\int\limits_0^1 h(y)\, dy}.$$

What we proved in v) is that, by making $|m|_{C^{r+1}}$ sufficiently small, we can get T_1 to have a derivative of norm as small as we want.

$\mathscr{T}_2$ is linear and we showed it is bounded. By the same type of C^r bounds, $\mathscr{T}_3$ is Lipschitz on bounded sets. Moreover, it sends E_0^{r-1} bounded sets to sets of functions uniformly bounded away from zero. For these functions, normalizing to integral 1 is a C^∞ operation and, integration is linear and bounded in the spaces considered.

The function v^{-1} solving (2) is obtained applying the contracting mapping principle. Looking at the right-hand side we obtain $\log(u')$. Therefore we obtain u up to a factor that is fixed uniquely by requiring it to be a diffeomorphism of the circle. Once one is convinced that u, v are unique in a ball, there is no difficulty in obtaining the same for θ.

To prove the bound for $\|\hat{v}\|$, it suffices to observe that $\|\mathscr{T}\text{Id} - \text{Id}\|_r \leq B_1 \|\|m\|\|$. Then, the contraction mapping principle gives

$$\|\hat{v}^{-1} - \text{Id}\|_r \leq \frac{E \|\|m\|\|}{1 - \text{Lip}(\mathscr{T})}.$$

But smallness conditions in m imply uniform bounds in $\text{Lip}(\mathscr{T})$.

The continuity of the fixed point with respect to m (given the topology of $\|\|m\|\|$) comes from the fact that $\mathscr{T}_1$ is linear in m. So that, when we have two m's $\|\mathscr{T}_{1(m)}h - \mathscr{T}_{1(m')}h\|_{H^r} \leq \|\|m - m'\|\|$ uniformly in $h \in V$, so that there is a constant D such that $\|\mathscr{T}_{(m)}h - \mathscr{T}_{(m')}h\|_r \leq D \|\|m - m'\|\|$ uniformly in $h \in V$.

If $\hat{v}^{-1}$ is a fixed point for $\mathscr{T}(m)$ it follows that

$$\|\mathscr{T}_{m'}\hat{v}^{-1} - \hat{v}^{-1}\|_r \leq D \|\|m - m'\|\|.$$

And thus, the fixed point of $\mathscr{T}_{m'}$ is not far away from v^{-1}.

Now, as remarked in the introduction when $r \geq 2$, then the inversion is a bounded operation in a neighborhood of the identity and all the bounds for v^{-1} carry over to v itself. $\square$

To obtain that (u, v, θ) depends differentiably on f, we just recall that since exponentials etc. are C^∞, $\mathscr{T}(f, u, v)$ is a C^l function and we showed its derivative is bounded away from 1. So that we can apply the implicit function theorem in Banach spaces.

Corollary 1. *In the conditions of Theorem 1, there exists a constant B_3 so that*

$$\left| \theta - \int_0^1 \hat{f} \right| \leq B_3 \varepsilon^2.$$

Proof. (∗) can be rewritten as:

$$x + \hat{u} \circ v \circ f(x) + \hat{v}(f(x)) + \hat{f}(x) = x + \theta,$$

so

$$\left| \theta - \int_0^1 \hat{f} \right| \leq |\int \hat{u} \circ v \circ f| + |\int \hat{v} \circ f(x)|.$$

Remember that both $\hat{u}$ and $\hat{v}$ are odd functions and that, therefore they integrate to zero over a whole period so that $|\int \hat{v} \circ f(x)| = |\int \hat{v} \circ f(x) - \hat{v}(x)|$. However

$$|\hat{v} \circ f(x) - \hat{v}(x)| \leq \sup_{x \in [0,1]} |\hat{v}'(x)| \sup_{x \in [0,1]} |f(x) - x|,$$

and each of the factors can be bounded by something proportional to ε. The first term, involving $\hat{u}$, can be bounded in a similar fashion. $\qquad\square$

Corollary 2. *All small enough rotations can be written as products of diffeomorphisms commuting with reflections.*

Proof. We construct a continuous family of g_λ, $\lambda \in [-\lambda_0, \lambda_0]$ of diffeomorphisms with the following properties:

i) g_λ is well into inside the domain of applicability of Theorem 1 (so that θ is a well defined continuous function of λ).

ii) All g_λ are products of diffeomorphisms commuting with reflections.

iii) $\theta(g_\lambda)$ changes sign in $[-\lambda_0, \lambda_0]$.

It follows that, for all diffeomorphisms f close enough to the identity, (in particular small rotations) $\theta(g_\lambda \circ f)$ changes sign so that there is one λ^*, $\theta(g_\lambda * \circ f) = 0$, which means that f can be written as a product of diffeomorphisms commuting with reflections. In view of Corollary 1, iii) can be substituted by:

iv) g_λ is differentiable with respect to λ,

v) $\theta(g_0) = \int \hat{g}_0 = 0$,

vi) $\dfrac{d}{d\lambda} \int \hat{g}|_{\lambda=0} \neq 0$.

Such a family can be constructed in the following way: Call $h_\lambda(x) = x + \lambda \sin 2\pi x$.

If k, l are diffeomorphisms commuting with reflections about 0 and ρ respectively, $g_\lambda = h_\lambda \circ k \circ l$ is an acceptable family provided $\int \sin(k \circ l(x)) \neq 0$, and k, l are suitably close to the identity. (Notice that we obtain $\theta_{(g_0)} = 0$ by just observing that $l^{-1} \circ k^{-1} \circ g_0(x) = x$.) k and l can be obtained by adding to the identity antisymmetric functions centered at 0 and ρ respectively, which are small and which "live" in a small interval.

This can be done, e.g. using the Poisson kernel (or rather a trigonometric polynomial truncation of it),

$$k = x + \varepsilon_1 \sin(2\pi x) P(x, \rho/100),$$
$$l = x + \varepsilon_2 \sin(2\pi x - 2\pi\rho) P(x - \rho, \rho/100).$$

One can get easily convinced that, by choosing ε_1 and ε_2 all the condition are satisfied. (If we take $\varepsilon_2 = 2\varepsilon_1 = \varepsilon$, $\int \sin(k \circ l(x))$ is an analytic function of ε and one only has to check that it is not identically zero to conclude that in any small neighborhood there are points where it is not zero. The derivative with respect to ε can be seen to be nonzero. So, by getting to a small enough ε we can adjust any smallness condition.) Depending on how small we have to choose ε, we have to impose more severe smallness restrictions for λ_0, but there is still a strictly positive number that will work.

Theorem 2 (Reduction theorem, second version). *Let $r \geq 2$ be fixed and ρ be a number of constant type. Let also A_1 and A_2 be two diameters of the circle forming an angle of $2\pi\rho$ radians.*

Then there exists an $\varepsilon_0 > 0$ (ε_0 depends on r) such that, when $f \in C^{r+1}$ and $\|\hat{f}\|_r = \varepsilon \leq \varepsilon_0$, then there exist two diffeomorphisms u, $v \in \mathrm{Id} + H^r$ so that

$$u \circ v \circ f(x) = x + \theta. \tag{*}$$

$$u, v \text{ commute with reflections about } A_1, A_2. \tag{**}$$

$$\theta \text{ is arbitrarily small when } \varepsilon \text{ is sufficiently small.} \tag{***}$$

Proof of Theorem 2. Again, we start by remarking that if we find a solution of (2) we can find a solution of the problem and again, we find a solution of (2) by treating it as a fixed point problem for $\mathscr{T}$. The difference with the previous proof is that we do not involve the contraction mapping principle but rather, Schauder–Tychonoff fixed point theorem. Even if we do not obtain uniqueness this way, we only have to control where the image under $\mathscr{T}$ lies and not the Lipschitz constants; this allows the use of one derivative less in the hypothesis.

We start by fixing K_r small enough in such a way that in

$$V = \{v \in \mathrm{Id} + H^r \mid \|\hat{v}\|_r \leqq K_r\}$$

we can perform inversion and it is a bounded operation.

We see, using iii) that, by imposing sufficiently strong smallness conditions in $\|m\|_r$, we can make $\mathscr{T}_1 V$ to be contained in an arbitrarily small ball around zero.

By carrying the argument the same way as we did in the previous version we can obtain that $\mathscr{T}V$ is contained in a ball as small as we please around the identity. In particular it can be made to be contained in V.

Since V is clearly convex, the only hypothesis of Schauder–Tychonoff theorem which remains to check, is that $\mathscr{T}$ is continuous in a topology in which V is compact. However, for maps between Hausdorff compact spaces, continuity is the same as the closeness of the graph. So, it suffices to find a topology in which V is compact and (2) is a closed relation.

The C^1 topology is acceptable. Compactness of V comes from the compactness of Sobolev's embedding and closeness of the graph is most easily established looking at the extended operator $\mathscr{T}^* : \mathscr{T}^* h = (s, l)$ (The same notations as in (2)), so that (h, s, l) in the graph of $\mathscr{T}^*$ is the same as those satisfying (2) which is a property clearly preserved under C^1 limits. Since $\mathscr{T}^*$ also maps a compact set into a compact set, it is continuous, and since $\mathscr{T}$ is obtained by projecting, it is also continuous.

To finish the proof we only have to remark that the smallness conditions for $\|m\|_r$ can be obtained by imposing smallness to $\|f - \mathrm{Id}\|_{r+1}$.

Remark. Observe that by using this method in the proof we only "lose one derivative" whereas Nash–Moser methods would lose more.

The proof is, however, not optimal in the differentiability assumptions. The next proof deals with the borderline case of assuming only two derivatives.

Other modifications are also possible. One could e.g. use fractional order, Sobolev spaces or spaces of Hölder spaces for which all the ingredients of this proof—characterization by decay rates of Fourier coefficients and inequalities for the composition—are available [6, 3]. However, the next version seems to be close to optimal in the differentiability requirements and we have not explored in this paper the other possibilities.

Theorem 3 (Reduction theorem, third version). *Let ρ be a number of constant type, and A_1 and A_2 be two diameters of the circle forming an angle of $2\pi\rho$ radians.*

Then there exists an $\varepsilon_0 > 0$ such that when $\| \hat{f} \|_{C^2} = \varepsilon \leqq \varepsilon_0$, then there are two homeomorphisms u, v, and a number θ such that the same conclusions of the previous theorem hold except uniqueness.

Proof of Theorem 3. Again, we solve (2) instead of (∗) by constructing the operator $\mathscr{T}$, but we try to optimize differentiable assumptions.

The intuition is that the most delicate step is the exponentiation because it is the one which is done in a space with less regularity. Probably the less regular space in which exponentiation can be controlled with today's technology is B.M.O. (The functions of bounded mean oscillations) and this fits wonderfully with a remarkable theorem by Yves Meyer which characterizes which functions, through the application of Lemma 1, yield functions in B.M.O. The regularity properties required of m are chosen in such a way that everything fits together. All this remarkable strategy comes straight from [2] and what follows, after having found the right formulation, is very similar to what is in this paper. As a matter of fact, imitating the proof in [2], one can see that it suffices to use L^p, $p > 1$ bounds in the second derivative of f instead of the C^2 smallness conditions. For simplicity we just check the later case. Notice that, already a C^2 proof is beyond Nash–Moser techniques. Besides that, for our applications, we are only interested in topologies compatible with the group structure of diffeomorphisms.

The critical lemmas are the following:

Lemma 2 (John and Nirenberg). *Given a real function h over the real line, we call*

$$h_I = \frac{1}{|I|} \int_I h(x) dx,$$

where $|I|$ is the measure of the interval I and also

$$\| h \|_{B.M.O.} = \sup_I \frac{1}{|I|} \int_I |h - h_I|.$$

(Notice that strictly speaking $\| \ \|_{B.M.O.}$ is not a norm, since it takes the value zero on all constant functions).

We say that a function h is in B.M.O. when $\| h \|_{B.M.O.} < \infty$.

Then, there exist two constants $b > 0$, $B > 0$, so that, when $h \in B.M.O.$, $\int h = 0$ and b' is a real number so that

$$b' < b / \| h \|_{B.M.O.}.$$

We have

$$\int_0^1 e^{b'|h|} dx \leqq 1 + \frac{Bb' \| h \|_{B.M.O.}}{b - \| h \|_{B.M.O.} b'}.$$

Proof. It can be found in [7].

The consequence we want to deduce from this lemma is that, by controlling the B.M.O. norm, we can control the L^2 norm of the exponential and we will also need

lower bounds on the normalizing factor. The latter can be deduced applying Jensen's inequality.

$$\left(\int e^{h'}\right)^{-1} \geqq \left(\int e^{|h|}\right)^{-1} \geqq 1/\int e^{-|h|} \geqq \left(1 - \frac{B\|h\|_{\text{B.M.O.}}}{b + \|h\|_{\text{B.M.O.}}}\right)^{-1}.$$

Lemma 3 (Yves Meyer). *Let P_0 be defined as in Lemma 1 (that is, the projection on the space of even functions about θ with respect to the even functions about ρ, where ρ is a fixed number of constant type). Then, given any $p > 1$, there is a constant depending only on p such that*

$$\|P_0 f\|_{\text{B.M.O.}} \leqq C_p \|f^1\|_{L^p}.$$

Proof of Lemma 3. This lemma is not quite the same as the one enunciated in paper [8], but its proof applies without any modification. The key step in his proof is Lemma 3 of [8] and, using the Fourier representation of the operator P_0 that we gave in Lemma 1 and the estimates for constant type numbers mentioned in the introduction, we can prove very easily the estimates needed to apply it.   □

The proof has to be slightly more careful than before, since we do not have as many properties to control the spaces. The choice of V for example has to include the positivity of the derivative to guarantee that there is an inverse

$$V = \{f(x) \mid f(x) \in \text{Id} + 0_0^r, \|f'\|_{L^2} \leqq \varepsilon, f'(x) > 0\}.$$

Notice that the oddness of f about 0 implies that it should vanish at zero, giving therefore a one-to-one correspondence between functions and their derivatives. Under C^1 smallness conditions in m we can obtain

$$\|(m \circ f)'\|_{L^2} = \|m' \circ f f'\|_{L^2} \leqq \|m\|_{C^1} \|f'\|_{L^2}.$$

So, we have controlled where $\mathcal{T}_1 V$ lies. Using Meyer Lemma, we have controlled $\|\log l'\|_{\text{B.M.O.}}$, and using John and Nirenberg lemma we can bound $\|l'\|_{L^2}$ and we can also bound the normalizing factor.

The upshot of all this is that, under C^1 smallness conditions in m, V is sent into V and in order to apply Schauder–Tychonoff theorem we just need a topology in which V is compact so that $\mathcal{T}$ has a closed graph. Such a topology is the weak L^2 topology for the derivatives (remember that for odd functions the derivative determines the functions). (This topology, as a matter of fact is the topology of Hölder norms of order 1/2).

We just observe that when three functions l, s, h satisfy (2), then they satisfy

$$l' f' \circ h = s',$$

and the only thing we have to show is that when $l'_i \to l'$, $h'_i \to h$ in the weak L^2 sense, the left-hand side converges in the weak L^2 sense to the value of the limits.

This is true because weak L^2 in the derivatives of h_i implies convergence in the supremum norm for $f' \circ h_i$ and convergence in the supremum norm for one factor and weak convergence for the other, implies weak convergence for the product.

Remark. Observe that the last step of the supremum convergence also follows from L^p $p > 1$ boundedness for f''. The arguments which are necessary for proving that under such conditions, $\mathcal{T}$ maps a suitable V into itself, do not need modification from those in [2].

As remarked before, the fact that the derivative is positive guarantees that the map is invertible. Moreover, since our map does not send sets of positive measure into sets of measure zero (this also follows from positivity of the derivative), then the inverse is absolutely continuous and has an L^1 derivative.

So, given two C^2 diffeomorphisms that can be factored into homeomorphisms with strictly positive L^1 derivative and symmetry properties, their product and their inverses have similar properties.

We hence proved that, indeed, there is a C^2 ball around the identity all of whose members enjoy this property. The C^2 topology is compatible with the group structure under composition.

4. The Decomposition Theorem

Any of the versions of the reduction theorem we have proved tells that all functions which are in a sufficiently small neighborhood of the identity can be reduced to rotations by composing with symmetric ones and, in view of Corollary 2, all functions which are close to the identity can be written as a product of a finite number of functions commuting with reflections.

The C^r topologies when r is an integer are compatible with the group structure under composition.

Since the set of diffeomorphisms that can be written as a finite product of symmetric ones is clearly a group, it is open and, since the complement is the union of cosets, it should be open too.

However, the group of orientation preserving diffeomorphisms of the circle is connected and, therefore the set should be the whole group. This finishes the proof of the main theorem.

Remark. A corollary of the proof is that all small enough rotations can be written as $u \circ v \circ g_{\lambda_0}$. Looking at the symmetries of the factor, it is easy to establish that the decomposition we constructed of a small rotation and its inverse are not just the inverse.

It follows that there is a non-trivial factorization of the identity. Hence, the solution of the inverse scattering problem of making a lense given its action is not unique.

5. Multidimensional Generalizations

We want to prove the following:

Theorem 4. *Let* $F \in T^d \to T^d$ *be a diffeomorphism of class* C^r *($r \geqq 4$) in the connected component of the identity in this group, then* F *can be written as a finite product of diffeomorphisms commuting with reflections across planes* $\{x_i = a\}$.

Proof. Again, it suffices to prove a local version of the theorem.

All diffeomorphisms of class C^r, $r \geqq 1$ sufficiently close to Id, can be factorized in the following way:

$$F = g_1 \circ \cdots \circ g_d,$$

where

$$g_i = \text{Id} + (0, \ldots, 0, \underset{i}{\hat{g}}, 0, \ldots, 0),$$

and the factors are also C^r. Therefore, it suffices to factorize diffeomorphisms of the form

$$(x_1, \ldots, x_d) \rightarrow (x_1 + \hat{g}(x_1 \cdots x_d), x_2, \ldots, x_d).$$

We may try to do this also using diffeomorphisms of the same form u, v commuting with reflections across $\{x_1 = 0\}$, $\{x_1 = \rho\}$ respectively and translations. That is, we try to find u, v such that

$$u \circ v \circ f(x) = (x_1 + \theta(x_2 \cdots x_d), x_2, \ldots, x_d). \tag{2}$$

If we succeed, it is very easy to factorize the right-hand side into diffeomorphisms commuting with reflections.

In effect, for functions of the form $(x_1, \ldots, x_d) \rightarrow (x_1 + \hat{u}(x_2, \ldots, x_d), x_2, \ldots, x_d)$, compositions are the same as addition of the $\hat{u}$, and it suffices to show that all periodic functions can be written as sums of functions commuting with reflections.

In effect, applying Lemma 3, we can write

$$\theta(x_2, \ldots, x_d) = \hat{u}(x_2, \ldots, x_d) + \hat{v}(x_2, \ldots, x_d) + \int \theta(x_2, \ldots, x_d) dx_2$$

and, if $\theta \in H^r$, $\hat{u}, \hat{v} \in H^{r-1}$ (clearly $\int \theta dx_2 \in H^r$). So that we can apply the induction until we get to a constant rotation. But we already proved that constant rotations can be decomposed.

So, we are only left with showing we can choose u, v as in (2).

If we fix $(x_2, \ldots, x_d)$ this is precisely the problem we solved in the one dimensional version and we can consider (2) as solving a $d - 1$ family of one dimensional problems.

By the corollaries on smoothness, the solutions (u, v^{-1}, θ) are in H^{r-2} and depend in a C^1 fashion on the parameters.

Now, if $v^{-1} \in H^{r-1}$, then v depends in a C^1 fashion when topoligized in the H^{r-2} norm.

Hence, when considered as a function $(x_1, \ldots, x_d)$ it is a diffeomorphism.

Higher differentiability in f will yield higher differentiability in u, v^{-1}, and hence higher differentiability of the function $v \rightarrow v^{-1}$ (in the spaces with less differentiability).

References

1. Langer, J., Singer, D. A.: Diffeomorphisms of the circle and geodesic fields on Riemann surfaces of genus one. Inv. Mat. **69**, 229–242 (1982)
2. Herman, M. R.: Sur les diffeomorphismes du cercle de nombre de rotation de type constant. In: Conference on harmonic analysis in honor of Zygmund, A. Becker W. et al., (eds.) Belmont: Wadsworth 1983
3. Herman, M.: a) Lectures in Les Houches (1981), unpublished; b) Sur les courbes invariates par les diffeomorphisms de l'anneau. Asterisque **103–104** (1981)
4. de la Llave, R.: A simple proof of a particular case of C. L. Siegel center theorem. J. Math. Phys. **24**, (8) 2118–2121 (1983)
5. M. R.: Herman, Sur la conjugation différentiable des difféomorphismes du cercle a des rotations. Pub. Mat. I.H.E.S. **44**, 5–233 (1979)
6. Hörmander, L.: Implicit function theorems. Stanford preprint 1977
7. John, F., Nirenberg, L.: On functions of bounded mean oscillation. Commun. Pure Appl. Math. **14**, 415–426 (1961)
8. Meyer, Y.: Sur un problème de Michel Herman. In: Conference on harmonic analysis in honor of Zygmund, A., Becker, W. et al. (eds.). Belmont: Wadsworth 1983
9. Marsden, J.: Applications of global analysis in mathematical physics. Boston: Publish or Perish 1974